Uma visão abrangente da computação

Organizadores:
Mirian Nunes de Carvalho Nunes
Carolina Gomes Araújo Garreto

2023

Pascal Editora

2 volume

MIRIAN NUNES DE CARVALHO NUNES
CAROLINA GOMES ARAÚJO GARRETO
(Organizadoras)

UMA VISÃO ABRANGENTE DA COMPUTAÇÃO

VOLUME 2

EDITORA PASCAL
2023

Editor Chefe: Prof. Dr. Patrício Moreira de Araújo Filho

Edição e Diagramação: Eduardo Mendonça Pinheiro

Edição de Arte: Marcos Clyver dos Santos Oliveira

Bibliotecária: Rayssa Cristhália Viana da Silva – CRB-13/904

Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)

B578u

Coletânea Uma visão abrangente da computação / Mirian Nunes de Carvalho Nunes e Carolina Gomes Araújo Garreto (Org). São Luís - Editora Pascal, 2023.

378 f. : il.: (Uma visão abrangente da computação; v. 2)

Formato: PDF

Modo de acesso: World Wide Web

ISBN: 978-65-80751-83-9

D.O.I.: 10.29327/5280411

1. Computação. 2. Inteligência artificial. 3. Computação forense. 4. Proteção de dados. I. Nunes, Mirian Nunes de Caravalho. II. Garreto, Carolina Gomes Araújo. III. Título.

CDU: 004::343.98

2023

www.editorapascal.com.br

contato@editorapascal.com.br

APRESENTAÇÃO

Esta edição da série “Uma visão abrangente da computação” é o resultado da seleção de vários artigos científicos publicados sobre a temática central da obra. Nesta edição são abordados temas como a influência e aplicações em Inteligência Artificial (IA), o uso da computação forense em crimes cibernéticos, uma abordagem sobre a importância da segurança da informação em banco de dados onde se encontram armazenadas diversas informações e uma análise sobre a implementação da lei geral de proteção de dados pessoais, assunto este bastante atual e em evidência em ambientes empresariais devido a sua grande importância. As áreas abordadas como a IA, segurança da informação e a lei geral de proteção de dados, a LGPD, os organizadores ressaltam a sua importância devido a sua grande relevância para a solução de problemas encontrados atualmente em ambientes empresariais. Os autores desta série científica confirmam o valor dessas áreas da engenharia e ciência da computação e as soluções encontradas, mas principalmente vem reforçar a importância do tema de vanguarda e sua aplicabilidade, contribuindo para que as empresas e centros de pesquisa possam identificar projetos com o potencial de desenvolvimento de novas tecnologias e inovação para o futuro de novas aplicações e soluções de problemas empresariais.

Wagner Elvio de Loiola Costa

Mestre em engenharia elétrica

ORGANIZADORES

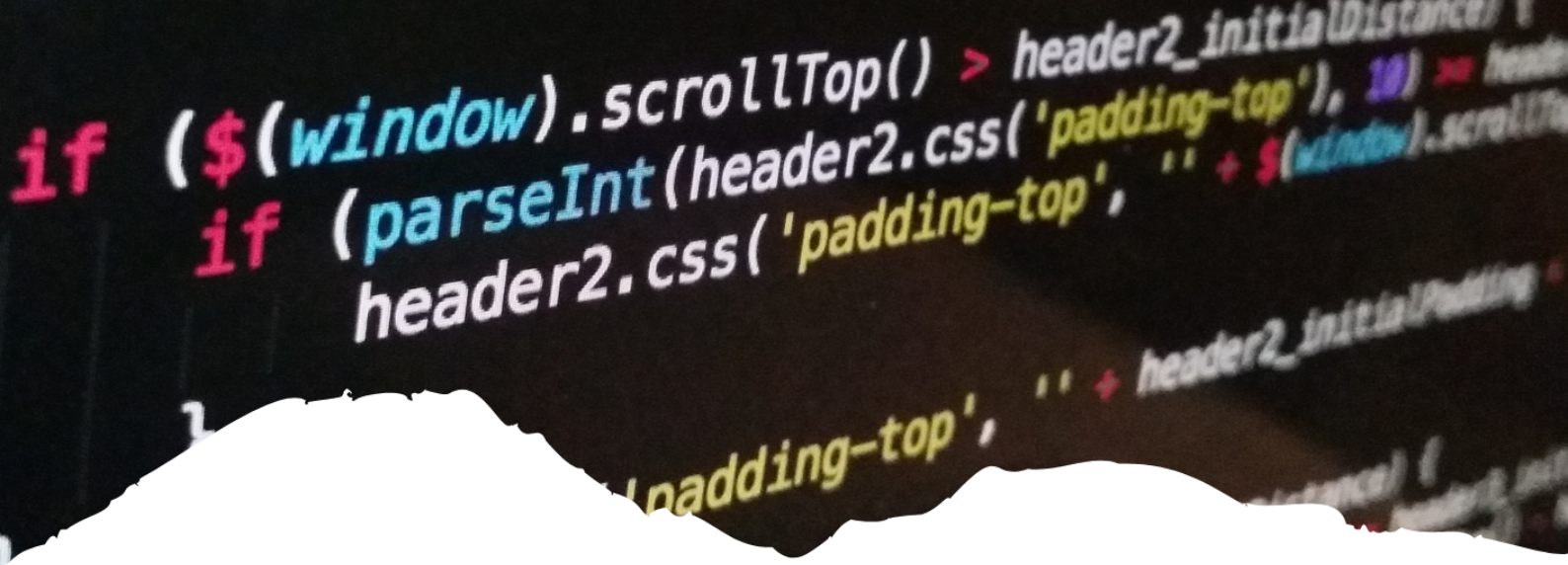
Mirian Nunes de Carvalho Nunes

Graduada em Desenho Industrial pela Universidade Federal do Maranhão - UFMA. Graduada em Formação Pedagógica de Docentes para as áreas do Ensino Médio e Profissionalizante pela Universidade Estadual do Maranhão - UEMA. Pós-Graduada Gestão Educacional pela Faculdades Integradas Potencial - FIP - Cotias - SP; em Arte, Educação e Tecnologias Contemporâneas pela Universidade de Brasília - UnB e em Docência do Ensino Superior pela Universidade Candido Mendes RJ. Exerce cargo de Professora na Universidade Pitágoras São Luís - MA, ministrando as disciplinas de Desenho Técnico, Desenho Técnico Mecânico no programa computacional Inventor da Autodesk, Desenho Técnico Projetivo no programa computacional AutoCAD da Autodesk e Orientação de TCC. Atuou como Professora EaD da disciplina de Desenho Técnico de 2013 a 2020 no Curso de Segurança do Trabalho pela UEMANET.

Carolina Gomes Araujo Garreto

Doutoranda em Segurança e Saúde Ocupacionais, pela Universidade do Porto. Possui mestrado em Engenharia de Segurança e Higiene Ocupacionais, pela Universidade do Porto (2019), Especialização em Engenharia de segurança do trabalho, pela Universidade Estácio de Sá - Laboro (2015), Especialização em engenharia ferroviária, pela UnDB (2012) e graduação em Engenharia Elétrica Industrial pelo IFMA (2011).

SUMÁRIO



1

SEGURANÇA DE REDES

NETWORK SECURITY

Evinerison Silva Avelar
Iago Emanuel Fernandes Moreira
Rafael Costa Santana
Roberto Max Louzeiro Pimentel
Robson Mateus Santana do Lago
Thamyres Mikaelly dos Santos Conceição

Resumo

Com o desenvolvimento tecnológico que tem se apresentado na computação, a Computação em Nuvem surgiu e tem sido cada vez mais utilizada por empresas e organizações de diferentes setores, com o objetivo de assegurar a proteção e a segurança dos dados, de modo a garantir a integridade e a privacidade das informações armazenadas. O principal objetivo desta pesquisa é identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem. Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Como resultado, verificou-se que a computação em nuvem, do inglês *Cloud Computing*, é uma expressão utilizada para definir um modelo de computação em que os recursos e serviços são disponibilizados em uma rede de servidores e utilizados de forma compartilhada através da internet. Muito empregada nas empresas, a Computação em Nuvem proporciona diversos benefícios, como a escalabilidade, otimização, controle de acesso, disponibilidade e segurança. Como desvantagens, pode-se mencionar o tempo de inatividade, a falta de atenção dos usuários e o fato de que dados criptografados na nuvem podem sofrer ataques cibernéticos. Dentre as estratégias de segurança para a proteção de informações e dados armazenados na nuvem destacam-se a segurança, gestão de riscos, identidade do usuário, proteção de dados e informações, prestação da privacidade em nuvem, dentre outras.

Palavras-chave: Computação em Nuvem, Tecnologia, Dados, Segurança de Rede.

Abstract

With the technological development that has been presented in computing, Cloud Computing has emerged and has been increasingly used by companies and organizations from different sectors, in order to ensure the protection and security of data, in order to guarantee the integrity and the privacy of the information stored. The main objective of this research is to identify information security issues for the protection and privacy of data in services that use cloud computing. To carry out this work, the methodology used was a Bibliographic Review Research. As a result, it was found that cloud computing is an expression used to define a computing model in which resources and services are made available on a network of servers and used in a shared way over the internet. Widely used in companies, Cloud Computing provides several benefits, such as scalability, optimization, access control, availability and security. As disadvantages, one can mention the downtime, the lack of attention of the users and the fact that data encrypted in the cloud can suffer from cyber attacks. Among the security strategies for protecting information and data stored in the cloud, there are security, risk management, user identity, data and information protection, provision of privacy in the cloud, among others.

Keywords: Cloud computing, Technology, Data, Network Security.

1. INTRODUÇÃO

Com a tecnologia no geral se desenvolvendo cada vez mais rápido e o mundo como um todo tornando-se mais conectado a cada dia, várias soluções são criadas para facilitar e baratear custos, tanto para os fornecedores de serviço quanto para os consumidores.

A computação em nuvem surgiu como uma tecnologia que possibilita o armazenamento e processamento de forma remota, não havendo a necessidade de máquinas fortes o suficiente para essas funções na empresa que utiliza esses serviços, com isso qualquer máquina conectada na nuvem poderia acessar as ferramentas oferecidas visto que as mesmas estariam sendo disponibilizadas remotamente, e sendo processadas em uma outra máquina.

A tecnologia começou a ser amplamente utilizada sendo mais barata para a empresa do que a forma tradicional que seria possuir todas as máquinas necessárias de forma física, com isso dados e mais dados são armazenados na nuvem, dados esses com informações sigilosas, tanto informações pessoais quanto empresarias. Com isso ataques são feitos a todo momento com o intuito de roubar informações, surge então a grande necessidade de proteger esses dados, utilizando métodos e boas práticas de proteção tanto para enviar golpes e fraldes quanto para manter a credibilidade e confiança com a empresa.

Com a tecnologia da computação em nuvem (*Cloud Computing*) tornando-se cada vez mais utilizada por bancos, lojas e Grandes Empresas é necessário assegurar a proteção e segurança dos dados, garantindo assim a integridade e privacidade das informações armazenadas. Sem essa segurança as empresas sofreriam ainda mais com ataques, os dados poderiam ser vazados ou roubados criando assim uma brecha para fraudes, golpes bancários, falsidade ideológica dentre outros crimes e também uma queda na credibilidade e confiança com a instituição atacada, justificando essa pesquisa.

A segurança e proteção de redes se faz cada vez mais importante visto que com os avanços tecnológicos e o mundo cada vez mais conectado surgem também novos casos de invasões e violações em redes por conta de hackers, vírus, malwares e outros fatores de risco. Diante disso, questiona-se: Qual a importância da proteção de redes para serviços que utilizam computação em nuvem?

O principal objetivo desta pesquisa é identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem. Especificamente, pretende-se: Analisar os conceitos e características da Computação em Nuvem; demonstrar as vantagens e desvantagens ao usar computação em nuvem; apontar as estratégias de segurança para a proteção de informações e dados armazenados na nuvem.

Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Para tanto, buscou-se auxílio em livros, revistas e artigos das bases de dados Google Acadêmico e Sciello, que pudessem oferecer referenciais teóricos condizentes com o tema apresentando, dando subsídio para a construção do trabalho. Foram utilizados os materiais acadêmicos publicados nos últimos cinco anos (2017 a 2022). As palavras-chaves na utilizadas na pesquisa foram: Computação em nuvem; Tecnologia; Dados; e Segurança de Rede.

2. A COMPUTAÇÃO EM NUVEM

A computação em nuvem é uma tecnologia que disponibiliza recursos computacionais de forma remota e compartilhada por todos que estão conectados. Como citado por Camboim e Alencar (2018, p.21):

> A computação em nuvem, do inglês *Cloud Computing* ou apenas cloud, é o termo utilizado para definir um modelo de computação em que os recursos e serviços são disponibilizados em uma rede de servidores e utilizados de forma compartilhada através da internet.

Historicamente, o termo nuvem vem sendo utilizado como sinônimo de internet. Esse uso inicialmente derivou-se da sua estrutura representativa em diagramas de rede, esboçando uma nuvem, utilizado para demonstrar a movimentação de dados por meio de *backbones* que pertenciam à nuvem (FERREIRA; CARVALHO, 2020).

O conceito de nuvem surgiu em 1961, quando o professor John McCarthy propôs que a tecnologia teria o poder de levar a um futuro em que a computação poderia ser comercializada por meio de um modelo de negócio utilitário. Com a virada do milênio, o conceito foi revitalizado e a expressão computação em nuvem passou a ser utilizada nos ambientes e cenários tecnológicos (PEREIRA, 2019).

Nascida na década de 90, a expressão computação em nuvem diz respeito à disponibilidade sob demanda de recursos computacionais como armazenamento e processamento, sem o gerenciamento nem o gasto de recursos direto do utilizador. Após o surgimento da internet a computação em nuvem surgiu, mas foi só depois de 1995 que ela deixa de ser unicamente de uso acadêmico e começa a ser explorada por empresas de forma comercial (SILVA NETO; BONACELLI; PACHECO, 2021). Com o custo de utilização de serviços sendo mais baixo que o de uma montagem e gerenciamento de uma infraestrutura completa, a computação em nuvem começou a ser explorada comercialmente.

Com os avanços tecnológicos e econômicos em diversas áreas, a forma de consumo de determinados produtos e serviços foi se moldando com essa evolução. Alguns serviços básicos como eletricidade, gás e água são utilizados de forma muito simples, mas, toda infraestrutura por trás de tais serviços é gerenciada por uma empresa que faz a cobrança desse serviço de acordo com a demanda do mesmo e não pelo valor que seria gasto por uma pessoa comum em toda a infraestrutura responsável pelo fornecimento de tal produto. “Computação em nuvem é uma tendência recente de tecnologia cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso.” (TAMANAHA, 2020). Portanto, seguindo a mesma ideia dos outros serviços, a computação em nuvem é um serviço oferecido que é cobrado pela demanda de seus usuários.

Segundo De Paula e Oliveira (2021, p.12), atualmente, o conceito de computação em nuvem possui uma outra denotação, como destaca:

> Hoje, com a Computação em Nuvem, a imagem da nuvem representa outra coisa. Aplicações podem usar recursos computacionais da nuvem ou elas mesmas podem executar de lá. A nuvem não é mais algo intangível, mas o cerne da computação.

Já nas palavras de Oliveira (2020, p.15), no que se refere ao conceito de computação em nuvem:

> Ainda existe muito desconhecimento, desinformação e até mesmo mitos são criados em torno do assunto. Mas é inegável que a computação em nuvem vai transformar a maneira de como as empresas operam sua TI, bem como vai transformar a maneira como os provedores irão oferecer seus serviços de TI.

A Figura 1 expõe o exemplo de uma organização contratante que não custeia os investimentos em equipamentos e sua manutenção, tendo em vista que a empresa contratada disponibiliza a manutenção dos equipamentos e os compartilha com demais usuários.

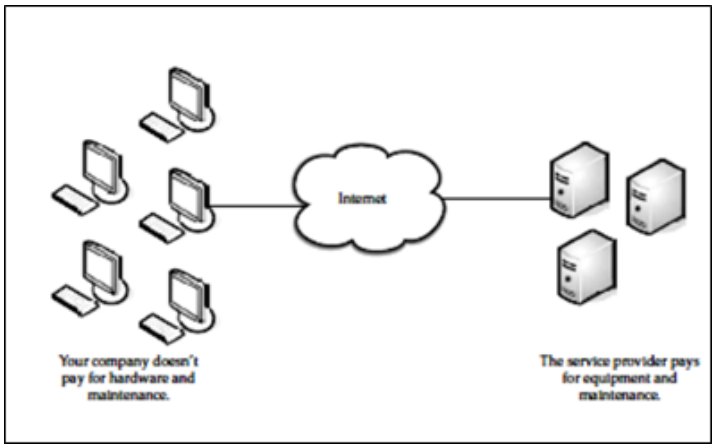


Figura 1: Como a computação em nuvem hospeda aplicações

Fonte: Martins (2019).

Sendo assim, entende-se que a computação em nuvem diz respeito ao fornecimento sob demanda de recursos da Tecnologia da Informação por meio da internet. Ao invés de utilizar hardwares ou softwares que estão no local, a tecnologia utilizada é aquela disponível em um banco de dados remoto. Mesmo que, muitas vezes sejam gratuitos, a maior parte dos serviços de computação em nuvem são pagos (ARNOLD; ZANELLA, 2022).

Segundo as palavras de Avinte, Nascimento e Nascimento (2019), a computação em nuvem pode ser também conceituada como a entrega de recursos de TI sob demanda através da internet, cujo uso estabelece um preço de pagamento. Sendo assim, ao invés de comprar e ter que manter servidores, o usuário tem a possibilidade de acessar os serviços por meio de banco de dados, de acordo com a sua necessidade, usando provedores.

Nesse sentido, Souza e Oliveira (2019, p.14) destacam que:

> Como um novo estilo de computação em que os recursos dinamicamente escaláveis e muitas vezes virtualizados são fornecidos como serviços através da Internet. Computação em nuvem se tornou uma tendência tecnológica significativa, e muitos especialistas esperam que a computação em nuvem irá reformular a tecnologia da informação (TI) os processos e o mercado de TI. Com a tecnologia de computação em nuvem, os usuários usam uma variedade de dispositivos, incluindo PCs, laptops, smartphones e PDAs para acessar programas, armazenamento e aplicação de desenvolvimento de plataformas pela Internet, através de serviços oferecidos por provedores de computação em nuvem.

Sendo assim, a computação em nuvem é vista por muitos autores como uma evolução natural dos sistemas de computação atual e a sua exploração leva à um novo patamar de criação de aplicativos (CARVALHO; ARAÚJO, 2021). Desse modo, uma empresa pode tanto contratar um servidor de serviços em nuvem como utilizar seu data e realizar esse serviço.

Neste sentido, a Figura 2 apresenta as origens da Computação em Nuvem:

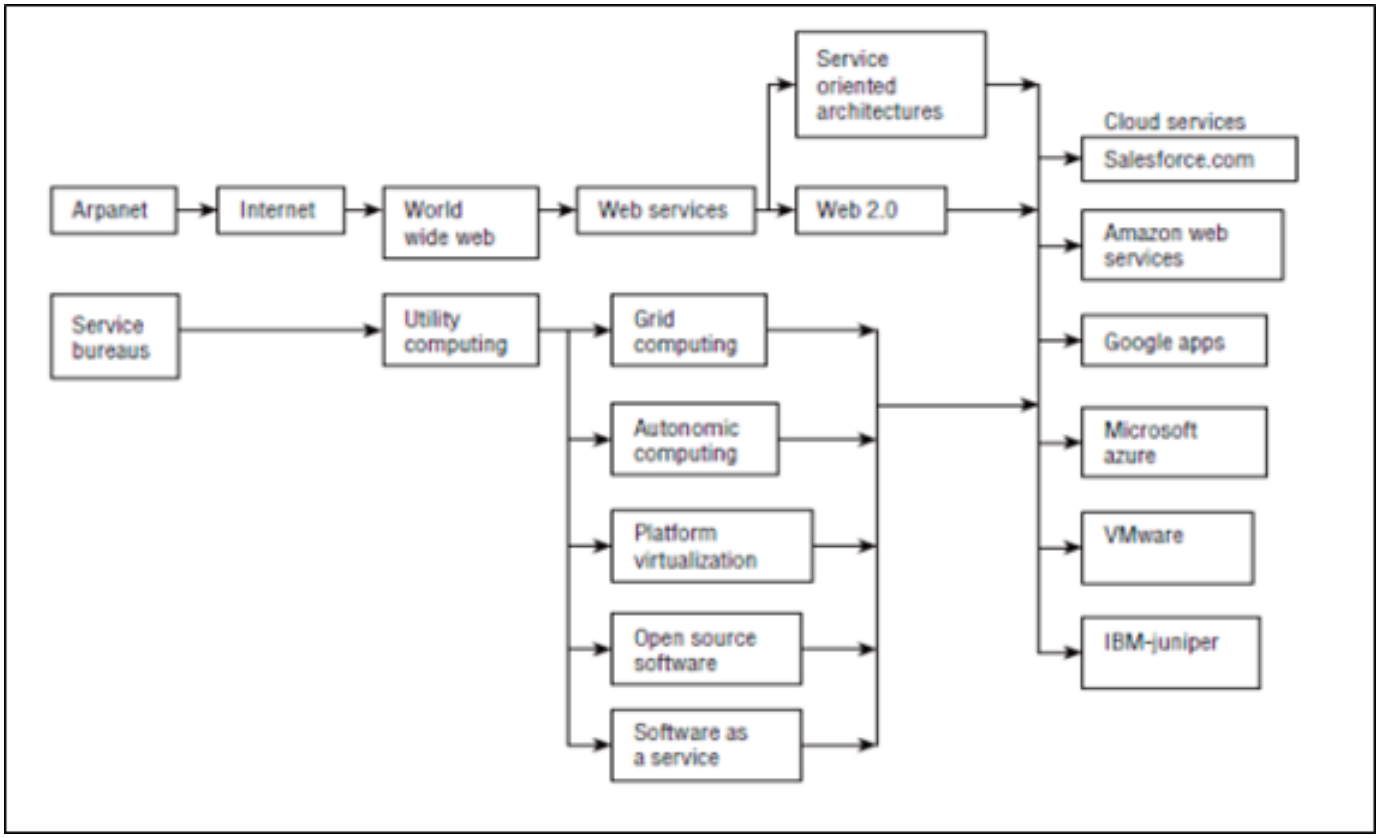


Figura 2: Origens da computação em nuvem

Fonte: Martins (2019).

Diante disso, alguns elementos merecem destaque na origem da computação em nuvem, sendo eles:

- *Utility Computing* – Corresponde à entrega de recursos de computação a um determinado cliente que paga por essa demanda quando há necessidade. O seu objetivo é utilizar os serviços de maneira eficiente, reduzindo assim os custos. Esse termo é comumente empregado na comparação do uso deste tipo de recurso computacional com os fornecedores de energia elétrica, por exemplo (CARVALHO; ARAÚJO, 2021).
- *Grid Computing* – Refere-se à aplicação do poder de processar diversos recursos computacional em rede, a fim de resolver especificamente um problema. Representa uma maneira de processamento paralelo executado em uma rede de computadores. Nesse sistema, os servidores, as redes e o armazenamento combinam-se, a fim de formar nós fortes e poderosos, correspondendo a um recurso que pode ser configurado de modo dinâmico, de acordo com a necessidade do usuário (ARNOLD; ZANELLA, 2022).
- *Autonomic Computing* – Diz respeito ao funcionamento de um sistema de computadores, sem a necessidade de controles externos. Esse termo baseia-se no siste-

ma nervoso autônomo do corpo humano, que controla as suas diferentes funções. Assim, o seu objetivo é fazer com que o computador execute complexas funções, sem necessidade de intervenções relevantes do usuário (FRANCO et al., 2021).

- *Platform Virtualization* – Esse elemento corresponde à repartição logica dos recursos computacionais em ambientes de múltipla execução, onde se incluem servidores, sistemas operacionais e aplicativos. A virtualização baseia-se no conceito de uma máquina virtual que é executada sobre uma plataforma física. A virtualização da plataforma é controlada através de um Monitor de Máquina Virtual (VMM), também conhecido como Hypervisor Xen. Este, é um dos recursos computacionais mais utilizados na computação em nuvem.
- *Software as a Service* (SaaS) – Este elemento refere-se à distribuição de software e modelo de implementação onde as aplicações são disponibilizadas aos usuários como um serviço. Sendo assim, eles podem ser adequadamente executados em sistemas dos usuários ou ainda, em servidores do seu provedor, prevendo a eficácia no gerenciamento de patches, bem como a colaboração (NETO et al., 2020).
- *Service Oriented Architecture* (SOA) – Esse recurso compreende um conjunto de serviços que comunicam-se entre si, tendo suas interfaces descritas e seu uso pode ser empregado em diversas organizações. A interface desses serviços é especificada em XML (Extensible Markup Language) (FRANCO et al., 2021).

Portanto, observa-se que esses elementos possuem significativa relevância para a computação em nuvem, representando recursos que podem ser utilizados e que contribuem para seu o bom funcionamento.

Com a popularização das redes wireless, e a grande quantidade de dispositivos conectados como smartphones, tablets e notebooks a computação em nuvem cresce a cada dia, por conta do seu processamento e baixo custo de utilização. “A computação na nuvem ou *Cloud Computing* é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independentemente da plataforma, bastando para isso ter um terminal conectado à “nuvem” (PICOTO; CRESPO; CARVALHO, 2021). Com a facilidade de acesso a arquivos e aplicações e a comodidade de utilização dos serviços a tendência é que essa tecnologia se desenvolva ainda mais com o passar dos anos.

3. VANTAGENS E DESVANTAGENS DA COMPUTAÇÃO EM NUVEM

Dentre as principais questões organizacionais abordadas ao se tratar sobre a computação em nuvem, destacam-se os benefícios e riscos provenientes do uso dessa tecnologia. Quando uma empresa resolve por adotar esse modelo para implantar seus recursos operacionais, ou ainda, aumentar a gama de serviços oferecidos aos seus consumidores, os seus gestores devem considerar o custo-benefício de se transferir a sua capacidade funcional para terceiros (ARNOLD; ZANELLA, 2022).

Sendo assim, de acordo com Avinte e Nascimento (2019), pode-se mencionar como principais benefícios da computação em nuvem para as empresas:

- Escalabilidade – Uma das características principais da computação em nuvem é a possibilidade de reduzir ou aumentar recursos, conforme a demanda operacional de cada empresa.
- Otimização – Por ser um ambiente virtual, é possível alterar procedimentos, sem a

necessidade de estabelecer novos recursos e equipes, e notificar todos os colaboradores sobre quem fez a alteração automaticamente.

- Controle de acesso – A ferramenta de controle de acesso de usuários cria permissões de acordo com as tarefas de cada colaborador. Assim, os gestores têm visibilidade de quem acessa as aplicações da empresa.
- Disponibilidade- A computação em nuvem permite retirar qualquer elemento ou sistema dos serviços da empresa para reparo, manutenção ou substituição, sem afetar os processos de TI.
- Segurança – O armazenamento na nuvem utiliza computação avançada, além de ser capaz de fazer backup e identificar vulnerabilidades.

Uma das principais vantagens da Computação em Nuvem é que o usuário só paga pelo que usa. Algum tempo atrás, se uma empresa decidisse utilizar um software de gestão mais robusto, como um ERP ou um sistema de Planejamento e Orçamento, tinha que comprar os próprios servidores para instalá-lo. Também tinha que adquirir licenças de bancos de dados, além de precisar possuir pessoal especializado para configurar tudo. E isso não era nada barato (CAMBOIM; ALENCAR, 2018).

Era comum, ainda, a empresa ter que comprar uma máquina poderosa para atender um período de pico no processamento. Isso fazia que a organização ficasse com capacidade ociosa ou que precisasse renovar esses equipamentos em pouco tempo por ficarem ultrapassados. Uma alternativa para essa questão é a Computação em Nuvem. Aqui, as empresas que utilizam *Cloud Computing* "alugam" a capacidade de hardware que desejam durante um determinado o período, pagando apenas pelos recursos de que precisa durante o tempo de uso (CARVALHO; ARAÚJO, 2021).

Isso também vale para os softwares que a empresa precisa. Ao invés de comprar uma licença de uso do sistema e adquirir servidores para instalá-lo, agora o usuário paga apenas uma mensalidade para quem fornece o sistema. E já tem tudo funcionando na hora, com custos que chegam a ser milhares de vezes menores em alguns casos (CAMBOIM; ALENCAR, 2018).

Outra das grandes vantagens da computação em nuvem que fica claro analisando o processo descrito acima é a flexibilidade. Ou seja, o cliente pode decidir aumentar ou diminuir sua infraestrutura de tecnologia na hora que quiser, de forma extremamente rápida e ágil. Se a empresa está crescendo rápido, não é preciso fazer grandes investimentos e perder tempo planejando a compra de um novo servidor, por exemplo. O cliente simplesmente "aperta um botão" e tem mais recursos à disposição, automaticamente, ampliando o espaço em seu banco de dados nas nuvens (FERREIRA; CARVALHO, 2020).

Quando o cliente utiliza um software na nuvem (Saas), o próprio fornecedor se encarrega disso. Tudo por meio de métodos automatizados que garantem que sempre haverá disponibilidade, não importa o número de pessoas que estão acessando o sistema naquele momento, o processamento do software em nuvem acontecerá normalmente. Essa função é especialmente útil para quem lida com negócios sazonais, que tem picos e quedas de movimento (PEREIRA, 2019).

Mais uma das vantagens da computação em nuvem é que o *Cloud Computing* permite que mesmo empresas pequenas tenham acesso a recursos de tecnologia de ponta. Antes, comprar um sistema de gestão sofisticado provavelmente estaria fora de cogitação para uma empresa de poucos funcionários. Hoje, da maneira como funciona a Computação em Nuvem, vê-se pequenas empresas utilizando os mesmos sistemas de gestão utilizados por grandes companhias. E isso só é possível porque cada empresa paga apenas pelo

que usa. Logo, os preços acabam se ajustam naturalmente de acordo com o tamanho da organização e principalmente de acordo com sua necessidade de uso (SILVA NETO; BONACELLI; PACHECO, 2021).

Cloud Computing é a área, mas o cliente pode utilizar este conceito em software ou hardware. Existem vários tipos serviços de Computação em Nuvem. Por exemplo, o cliente pode "alugar" um espaço num servidor e utilizar como precisar, ou pode alugar um software para atender uma ou mais áreas de sua empresa, com tudo já pronto, sem ter que configurar nada. Além de ser mais acessível e flexível, o modelo de software como serviço (Empresas SaaS) tem outras vantagens (FERREIRA; CARVALHO, 2020).

O modelo *Cloud Computing* vem mudando completamente a relação entre vendedor e cliente, uma vez que a excelência do serviço prestado deve ser contínua. Se não estiver satisfeito com o serviço prestado, o usuário pode simplesmente trocar de fornecedor sem grandes impactos para o seu negócio. Isso requer atenção especial de quem fornece o serviço para conquistar e manter o cliente sempre satisfeito, o que novamente é muito bom para todas as partes. É claro que *Cloud Computing* tem vantagens e desvantagens, Contudo, cada vez mais, as vantagens da implantação do sistema de Computação em Nuvem têm ficado claro para todos (OLIVEIRA, 2020).

Em relação às desvantagens da Computação em Nuvem, Pereira (2019) destaca o custo: para cada ação realizada pela empresa, existe um custo a ser adicionado no orçamento e no caso da computação em nuvem não seria diferente, já que você terá de contratar um servidor para atender especificamente às necessidades de seus colaboradores. Isso inclui a obtenção de um serviço mais robusto ou maior espaço de armazenamento. Além disso, é necessário ter uma internet de qualidade, confiável e consistente para aproveitar os benefícios da tecnologia em nuvem.

De acordo com Oliveira (2020), uma das maiores desvantagens da tecnologia em nuvem. Seus provedores podem enfrentar interrupções técnicas devido a motivos como perda de energia, baixa conectividade da internet, entre outros. Quando a conexão com a internet cai, significa que o acesso aos servidores fica indisponível, prejudicando o andamento do trabalho. Também é preciso garantir que a falta de energia não prejudique o acesso à internet. Então, geradores e planos de internet móvel devem ser considerados para evitar essa desvantagem.

Ainda que existam opções gratuitas, empresas e empresários que criam e acessam grande volume de arquivos podem precisar de planos pagos para atender às suas necessidades. Apesar dos arquivos serem criptografados, a partir do momento em que são armazenados na nuvem, seus dados podem sofrer ataques de cibercriminosos e ter logins e senhas capturados, o que pode gerar um grande transtorno para a empresa no futuro. Por isso é necessário buscar um serviço seguro e confiável (CARVALHO; ARAÚJO, 2021).

Segundo Martins (2019), os fornecedores de serviços na nuvem podem entrar em falência. Sendo assim, há sempre a possibilidade de uma nova empresa poder falir ou alterar o seu serviço. Quando avalia os fornecedores de serviços na nuvem descubra como pode obter os seus dados de volta se alguma vez decidir descontinuar a utilização de um serviço. Os melhores serviços permitem que descarregue os seus dados num formato padrão e não-exclusivo.

Oliveira (2020) ressalta também que as organizações irão necessitar de mais largura de banda e de uma conexão à Internet mais fiável para usarem as ferramentas sedeadas na nuvem. Se o acesso consistente à Internet, a velocidade da conexão ou a largura de banda são problemas para a sua organização, os serviços na nuvem podem não ser a escolha certa para si de momento.

4. ESTRATÉGIAS DE SEGURANÇA PARA A PROTEÇÃO DE INFORMAÇÕES E DADOS ARMAZENADOS NA NUVEM

Em lugares onde há ambientes computacionais é comum vermos que vários requisitos de segurança são ignorados comparados aos requisitos necessários dos sistemas. Isso resulta em desenvolvimento de sistemas e ambientes com grande vulnerabilidade a ataques e segurança falha. Quando falamos em vulnerabilidade em Computação em Nuvem, logo relacionamos modelos de entrega e sistemas hospedados em fornecedores terceiros, onde o geralmente engloba-se milhares de questões relacionadas à privacidade e segurança das informações residentes neste servidor na nuvem (CARVALHO; ARAÚJO, 2021).

Apesar das preocupações citadas acima, como privacidade e segurança, o assunto sobre segurança na nuvem muitas vezes esquece-se da importância de criar planos de contingência e Acordo de Níveis de Serviço (ANS) (em inglês SLA – *Service Level Agreement*), designados a prover confiabilidade e a certeza de que os negócios não sofrerão grandes impactos no caso de um desgaste (ARNOLD; ZANELLA, 2022).

Na computação tradicional, ambientes *in-house*, os usuários têm total controle sobre seus dados, processos e seu computador. Por outro lado, na Computação em Nuvem todos os serviços e manutenção são fornecidos por um provedor de nuvem. Sendo assim, o cliente (usuário) muitas das vezes, desconhece onde exatamente os dados estão armazenados devido ao dinamismo da nuvem. Desta maneira, o cliente não tem controle sobre todas as atividades dos seus dados (FRANCO et al., 2021).

De acordo com Pereira (2019, p.21), “ainda é preciso trabalhar muito antes que a indústria entenda de onde vêm os furos de segurança em Computação em Nuvem”. Isso impulsiona diversas equipes de pesquisas a buscar melhores práticas em segurança, caso empresas queiram ou pretendam desfrutar dos benefícios da Computação em Nuvem. A implantação e consumo de nuvem devem ser pensadas não só no contexto do ‘interno’ versus ‘externo’, como em relação à localização física dos ativos, recursos e informações, mas também no contexto de quem são os seus consumidores e de quem é o responsável pela sua governança, segurança e conformidade com políticas e padrões.

Isto não é sugerir que a localização da nuvem seja dentro ou fora da empresa de um ativo, um recurso ou uma informação não afete a condição de segurança e de risco de uma organização porque elas são afetadas, mas sim para ressaltar que esse risco também depende dos tipos de ativos, recursos e informações sendo gerenciadas, de quem as gerencia e como as gerencia, de quais controles estão selecionados e como eles estão integrados e questões de conformidade (NETO et al., 2020).

4.1 Segurança, governação, gestão de riscos e conformidade

As organizações utilizadoras da tecnologia *Cloud Computing* precisam ter visibilidade da segurança aplicada na nuvem. Isso inclui ampla transparência no processo de mudança, falhas ocorridas, gerenciamento de incidentes, assim como emissão de relatórios aos inquilinos da nuvem com as logs de auditoria. Quando falamos em Cloud Computing podemos afirmar que para a nuvem ser segura, a visibilidade do cliente é um ponto chave para que a segurança seja eficaz.

De acordo com Pereira (2019), a Lei Sarbanes-Oxley, exige que os recursos de auditoria sejam sempre abrangentes. Uma vez que as nuvens, principalmente as públicas são, por definição uma incógnita para o usuário, podendo em muitas das vezes não ser capaz de

mostrar se está compliance ou não com os requisitos de segurança. As nuvens privadas ou híbridas, por outro lado, podem ser configuradas para atender aos requisitos de segurança. Além do mais que, os fornecedores do serviço de *Cloud Computing*, algumas vezes, precisam adquirir auditorias de terceiros e seus clientes podem ser direcionados a investigações forenses quando alguma nuvem está sendo suspeita de violações.

Isso adiciona ainda mais importância para a manutenção de visibilidade adequada de uma nuvem. Em geral, as organizações muitas vezes citam a necessidade de Acordos de Nível de Serviço (SLAs) que são adaptados à cada situação específica, com base em suas experiências com estratégica de terceirização ou serviços gerenciados (SILVA NETO; BONACELLI; PACHECO, 2021).

4.2 Pessoas e identidade

Quando se fala em *Cloud Computing*, as organizações também precisam se certificar de que os usuários autorizados em toda a empresa tenham acesso aos dados e ferramentas que eles precisam, quando precisam, antes do bloqueio de acesso não autorizado ser feito. Ambientes de nuvem normalmente suportam uma comunidade grande e diversificada de usuários, assim estes controles são ainda mais críticos. Além disso, as nuvens introduzem um novo nível de usuários privilegiados: os administradores que trabalham para o provedor de nuvem. A monitoração deve incluir monitoramento físico e checagem de antecedentes (SILVA NETO; BONACELLI; PACHECO, 2021).

4.3 Proteção de dados e informações

A maioria das organizações citam a proteção de dados como o seu problema de segurança mais importantes. Típicas preocupações incluem a maneira pela qual os dados são armazenados e acessados, compliance e requisitos de auditoria e questões de negócios envolvendo o custo das violações de dados, requisitos de notificação aos danos e valor da marca. Todos os dados sensíveis ou regulados precisam ser devidamente segregados na infraestrutura de armazenamento em nuvem, incluindo os dados arquivados. Criptografia e gerenciamento de chaves de criptografia de dados em trânsito na nuvem ou dados parados no provedor de dados é fundamental para proteger a privacidade dos dados e cumprimento de exigências de conformidade (PEREIRA, 2019).

Ou seja, somente o provedor da nuvem ou o consumidor de uma nuvem privada (por exemplo), deve ter acesso as chaves de criptografia, pois a implantação da nuvem pode levantar questões relativas as leis jurídicas, caso haja violação da informação criptografada. Sendo assim, a implementação da nuvem jamais pode expor e ameaçar os dados do usuário.

Em outras palavras, se os dados envolvidos são críticos, a assessoria jurídica da organização deve realizar uma revisão completa de todos os requisitos de segurança antes da implantação nuvem, certificando-se que o provedor pode manter o controle sobre a localização geográfica de dados na infraestrutura. Em áreas que envolvem usuários e dados com diferentes classes de risco (tais como serviços públicos e financeiros), o provedor precisa manter a nuvem de dados de acordo com a escala de classificação do usuário. A classificação dos dados irá reger quem tem acesso, como esses dados são criptografados e arquivados, e como as tecnologias são usadas para evitar perda de dados (SILVA NETO; BONACELLI; PACHECO, 2021).

4.4 Rede e servidor

Dentre os vários tipos de nuvem, no ambiente de nuvem compartilhada, existe a necessidade de garantia por parte do usuário e da empresa fornecedora da nuvem, de que todos os domínios estejam adequadamente isolados, de modo que nenhuma possibilidade de tráfego de dados entre os compartilhadores da nuvem exista (OLIVEIRA, 2020).

Para alcançar este objetivo, os usuários precisam ter a capacidade de configurar domínios virtuais de confiança ou baseado em políticas de zonas de segurança. Como nas nuvens os dados do usuário se movem longe do controle do mesmo, é necessário um sistema de Detecção de Instrusão para prevenir ataques maliciosos ao ambiente. A preocupação não é apenas intrusões, mas também o potencial de vazamentos de dados, ou seja, extrusões. Em outras palavras, é fazer uma utilização abusiva do domínio de um cliente para montar ataques a terceiros. Em um ambiente de nuvem compartilhada por exemplo, todas as partes devem concordar com as suas responsabilidades e revisar a política de segurança da nuvem, além do provedor da nuvem assumir a liderança de gestão de contratos para garantir que haja avaliações de risco (TAMANAHA, 2020).

4.5 Infraestrutura física

A infraestrutura da nuvem, incluindo servidores, roteadores, dispositivos de armazenamento, fontes de alimentação e outros componentes que suportam as operações, devem ser fisicamente seguros. Isso inclui um controle adequado que engloba monitoramento de acesso físico utilizando o controle de acesso biométrico, circuito fechado de televisão de monitoramento, entre outros. Os provedores da nuvem precisam explicar claramente ao usuário como o acesso físico dos servidores que hospedam dados e cargas de trabalho é gerenciado (OLIVEIRA, 2020).

4.6 Preservação da privacidade em computação em nuvem

Existem muitos provedores de serviços na nuvem, possibilitando aos usuários acessar serviços diversos, mas quando as informações são trocadas entre os serviços, surge o problema da divulgação das informações e da consequente violação da privacidade. A partir dessa afirmação, os autores propõem um novo algoritmo de anonimato a ser aplicados nos micro-dados (partes da informação) antes que estes sejam publicados na nuvem. Segundo os autores, o uso da criptografia não seria suficiente para garantir a privacidade das informações, já que o provedor do serviço precisa decifrar as informações antes do processamento (TAMANAHA, 2020).

Avinte, Nascimento e Nascimento (2019) indicam a utilização de uma base de conhecimento externa, não necessariamente armazenada na nuvem, como registros públicos ou outros canais na Internet. A junção dos dados anonimizados com a base externa possibilitaria ao provedor do serviço realizar pesquisas e obter os dados necessários para resolver alguns problemas.

A circulação e manutenção de dados pessoais na nuvem acaba por exigir o uso da criptografia. Todavia, esta impõe limites estritos para a utilização dos dados ao provedor de serviços, por exemplo, se os dados são armazenados em texto não-cifrado, pode-se procurar um documento especificando uma palavra-chave, o que deixa de ser possível com textos cifrados usando algoritmos tradicionais. Contudo, pesquisas recentes em criptografia possibilitaram realizar algumas operações em dados cifrados, como indexação ou

pesquisas (MARTINS, 2019).

Os serviços fornecidos pela nuvem computacional podem ser disponibilizados em qualquer local físico de abrangência da mesma, ou utilizando componentes de infraestrutura incompatíveis com o ambiente do consumidor. A gerência de muitos serviços (SaaS, PaaS, IaaS) e recursos físicos pode gerar um volume considerável de dados a ser administrada de maneira centralizada, pois será necessário coletar, armazenar, analisar e processar estes dados. Assim, a administração centralizada pode ser considerada impraticável, e, portanto, faz-se necessário instanciar serviços de gerenciamento distribuídos e fracamente acoplados (com baixa dependência funcional) (SOUZA; OLIVEIRA, 2019).

Para que as organizações consumidoras utilizem os serviços oferecidos pela nuvem é necessário a implantação de um modelo de gerenciamento seguro e confiável. O esquema a ser utilizado deve facilitar a inserção e remoção de usuários dos serviços oferecidos pela nuvem. A implantação de mecanismos de autenticação robustos e esquemas de delegação de direitos funcionando de maneira confiável são fundamentais para o correto gerenciamento de identidades e para a prestação de serviços em nuvens computacionais (MARTINS, 2019).

Serviços de identidade utilizados pela nuvem devem suportar a delegação de direitos administrativos, com isso o gerenciamento pode ser repassado aos administradores individuais de cada ambiente – SaaS, PaaS, IaaS – então cada administrador pode gerenciar contas dentro de seu próprio domínio. Para fornecer acesso aos diferentes níveis de serviço, a organização consumidora pode utilizar um serviço de SSO (*Single Sign-On*) que faça parte de uma federação para autenticar os usuários das aplicações disponíveis na nuvem (CARVALHO; ARAÚJO, 2021).

O provedor de SSO pode ser terceirizado, instanciado externamente a organização consumidora (Domínio B). O OpenID é uma opção quando a organização consumidora deseja ter o processo de identificação terceirizado. No ambiente de computação em nuvem, a federação de identidades tem um papel fundamental para permitir que organizações consumidoras associadas se autentiquem a partir de um único ou simples *sign-on* (evento ac). Então, poderá acontecer a troca de atributos de identidades entre o provedor de serviço e o de identidade (evento atr). Padrões como a WS-Federation podem auxiliar na federação de identidades para diferentes domínios administrativos (FRANCO et al., 2021).

5. CONCLUSÃO

A presente pesquisa buscou identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem. Verificou-se que a Computação em Nuvem, também conhecida como *Cloud Computing*, diz respeito ao armazenamento e compartilhamento de arquivos e recursos computacionais na internet. Ela diz respeito a um espaço virtual, no qual é completamente possível o acesso às informações armazenadas. Esses dados podem ser compartilhados com outros usuários, tanto por meio do acesso direto à ferramenta de computação escolhida, como através do envio de links que permitirão o acesso aos arquivos desejados.

Diversas empresas estão voltando o seu olhar para a *Cloud Computing*, principalmente em virtude dos benefícios que ela proporciona, podendo-se citar: agilidade, segurança, flexibilidade de acesso às informações, escalabilidade, otimização, controle de acesso e disponibilidade. No entanto, também existem as desvantagens, como o tempo de inatividade por queda de energia ou rede, o custo, visto que para cada ação adicional a uma mudança

no orçamento e o fato de que dados criptografados na nuvem podem sofrer ataques cibernéticos.

Dentre as estratégias de segurança para a proteção de informações e dados armazenados na nuvem, esta pesquisa concluiu que são diversos, merecendo destaque: a segurança, gestão de riscos e conformidade, incluindo a transparência no processo de mudança, falhas ocorridas e gerenciamento de incidentes. Diante disso, pode-se afirmar que, com essa pesquisa, foram identificadas as questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem e o objetivo deste trabalho foi alcançado.

Referências

ARNOLD, Felipe Matheus Wust; ZANELLA, Renata. COMPUTAÇÃO EM NUVEM: um estudo sobre o Google Drive como ferramenta colaborativa aplicada a educação. **Trajetória Multicursos**, v. 12, n. 2, p. 110-136, 2022.

AVINTE, Eduardo Frias; NASCIMENTO, Manoel Henrique Reis; NASCIMENTO, Aline Santos. COMPUTAÇÃO EM NUVEM: REDUZINDO GASTOS EM PEQUENAS E MÉDIAS EMPRESAS. **ITEGAM-JETIA**, v. 5, n. 19, p. 41-47, 2019.

CAMBOIM, Kádna; ALENCAR, Fernanda MR. Requisitos não Funcionais e Sustentabilidade para Computação em Nuvem: uma Revisão Sistemática da Literatura. **WER**, 2018.

CARVALHO, Leonardo Rebouças; ARAUJO, Aleteia Patricia Favacho. Function-as-a-Service: Desenvolvendo Aplicações na Próxima Geração da Computação em Nuvem. **Sociedade Brasileira de Computação**, 2021.

DE PAULA, Laís; OLIVEIRA, Mauricio. COMPUTAÇÃO EM NUVEM: os desafios das empresas ao migrar para a nuvem. **Revista Interface Tecnológica**, v. 18, n. 2, p. 304-315, 2021

FRANCO, Carlos Leonardo Freitas Viveiros et al. VANTAGENS DA COMPUTAÇÃO EM NUVEM PARA EMPRESAS DE MENOR PORTE. **South American Development Society Journal**, v. 7, n. 20, p. 255, 2021.

MARTINS, Ana Paula. CLOUD GAMING: computação em nuvem nos jogos digitais. **Revista Interface Tecnológica**, v. 16, n. 1, p. 158-170, 2019.

NETO, Francisco et al. Computação em nuvem e aprendizado de máquina para análise de grandes volumes de dados educacionais. In: **Anais do XVII Encontro Nacional de Inteligência Artificial e Computacional**. SBC, 2020. p. 58-69.

PEREIRA, Thiago Martins. COMPUTAÇÃO EM NUVEM: PLATAFORMA COMO SERVIÇO. **MARTINS, Ernane Rosa. Fundamentos da Ciência da Computação**, v. 2, p. 116-125, 2019.

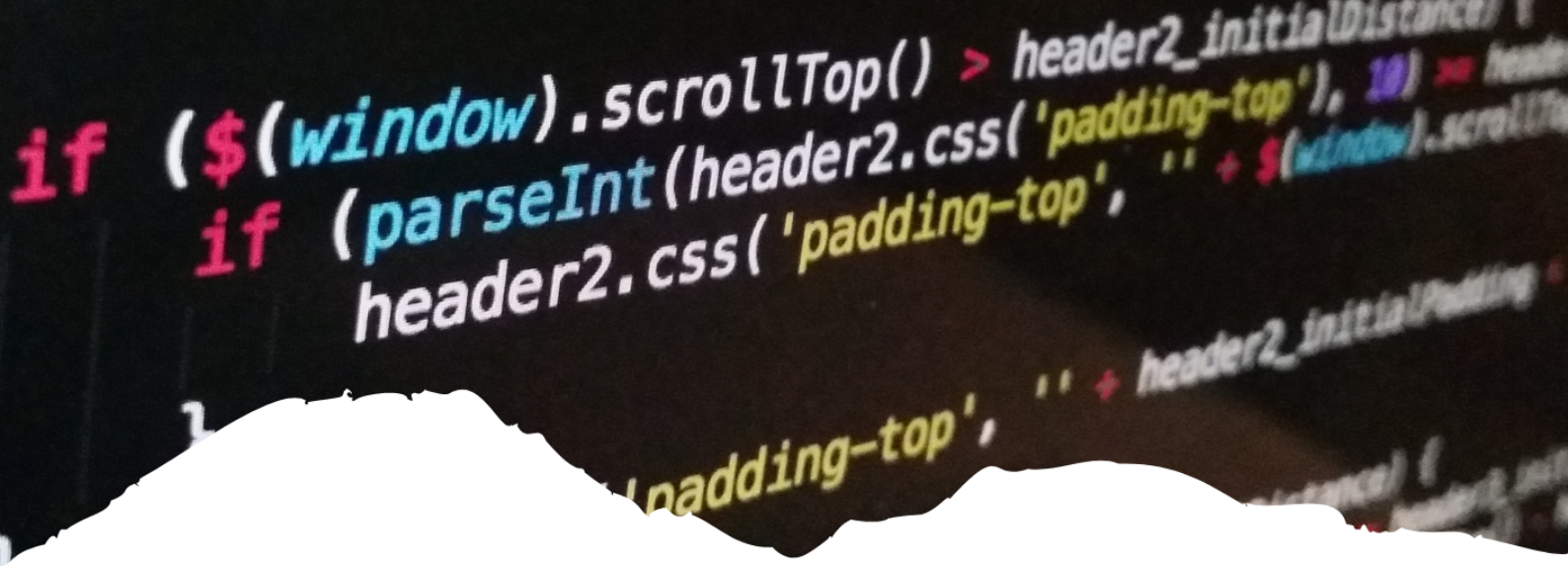
PICOTO, Winnie Ng; CRESPO, Nuno Fernandes; CARVALHO, Filipa Kahn. A influência da estrutura tecnologia-organização-ambiente e da orientação estratégica no uso da computação em nuvem, mobilidade empresarial e desempenho. **Revista Brasileira de Gestão de Negócios**, v. 23, p. 278-300, 2021.

SILVA NETO, Victo José da; BONACELLI, Maria Beatriz Machado; PACHECO, Carlos Américo. O sistema tecnológico digital: inteligência artificial, computação em nuvem e Big Data. **Revista Brasileira de Inovação**, v. 19, 2021.

SILVEIRA, Tiago; CARVALHO, Leonardo Filipe Batista Silva. Benefícios de Redução de custo na Infraestrutura da Migração de Serviços de computação em Nuvem. **PROJETOS E RELATÓRIOS DE ESTÁGIOS**, v. 2, n. 1, 2020.

SOUZA, Mathias Rodrigues; OLIVEIRA, Taciano Balardin. ESTUDO DE CASO SOBRE SISTEMAS DE COMPUTAÇÃO EM NUVEM. **Revista da Mostra de Iniciação Científica e Extensão**, v. 5, n. 1, 2019.

TAMANAHA, Rodolfo Tsunetaka. **Tributação e economia digital: análise do tratamento tributário dos rendimentos da computação em nuvem**. 2020. Tese de Doutorado. Universidade de São Paulo.



2

BANCOS DE DADOS: SEGURANÇA DE BANCOS DE DADOS

DATABASES: DATABASE SECURITY

Rafael Costa Santana
Evinerison Silva Avelar
Iago Emanuel Fernandes Moreira
Roberto Max Louzeiro Pimentel
Robson Mateus Santana do Lago
Thamyres Mikaelly dos Santos Conceição

Resumo

A presente pesquisa apresenta uma revisão de literatura sobre a segurança de banco de dados. Os avanços tecnológicos apresentaram a importância de dados para qualquer empresa, pois o mundo nunca lidou com esse grande volume de dados, sendo assim a necessidade de proteger esse bem valioso. Para elaboração desta pesquisa, foi utilizada a Pesquisa Bibliográfica como metodologia, viabilizando discussão sobre: Conceitos de dados e informação; Apresentação da Lei Geral de Proteção de Dados Pessoais; Conceitos básicos de um Banco de Dados. Assim o resultado dessa pesquisa evidencia que as informações e os dados são um grande ativo para qualquer organização, apresentado um grande interesse nesse mercado tecnológico. A segurança de um banco de dados é importante e tem como foco proteger a informação e os dados contidos nos bancos, diminuindo os danos de um eventual ataque, ataque esse que pode ser usado em forma de ataque pessoal ou alguma organização, e ao divulgado sem qualquer autorização pode trazer prejuízos tanto para a organização ou pessoal, além de apresentar as leis nacionais e internacionais que visam juridicamente proteger toda essa gama de informação.

Palavras-chave: SGBD, Banco de dados, Sistema da Informação, Segurança banco de dados, LGPD.

Abstract

This research presents a literature review on database security. Technological advances have shown the importance of data for any company, as the world has never dealt with this large volume of data, thus the need to protect this valuable asset. To prepare this research, Bibliographic Research was used as a methodology, enabling discussion on: Concepts of data and information; Presentation of the General Law for the Protection of Personal Data; Basic concepts of a Database. Thus, the result of this research shows that information and data are a great asset for any organization, showing a great interest in this technological market. The security of a database is important and is focused on protecting the information and data contained in the banks, reducing the damage of a possible attack, an attack that can be used in the form of a personal attack or some organization, and to be disclosed without any authorization can bring harm to both the organization and personnel, in addition to presenting national and international laws that legally protect this entire range of information.

Keywords: DBMS, Database, Information System, Database Security, LGPD.

1. INTRODUÇÃO

O armazenamento e a utilização de dados está cada vez mais presente no dia-a-dia, dados esses que podem ser produzidos das mais diversas fontes, como rede socias, sendo assim se tornando essenciais para qualquer organização. Diante disso, é essencial que bancos de dados devem priorizar a segurança das informações contidas neles. O aumento crescente dos dados sendo armazenados e utilizados devido aos grandes avanços tecnológicos apresentou uma grande importância para a valorização da segurança das informações contidas nos Banco de Dados, com a crescente de casos de invasões e ataques de hackers, vazamentos e a procura desses dados.

O uso de Bando de Dados tornou-se recorrente para os mais diversos tipos de aplicações, principalmente com o avanço da Internet e das tecnologias. Com tantas informações importantes sendo geradas, é despertado o interesse de pessoas para utilização desse grande fluxo de informações, dados esses como nome de um cliente, endereço, telefone, idade, documentos pessoais, enfim, tudo que é fato é dado.

A segurança em banco de dados, já que as informações são grandes ativos em que podem apresentar grau de sensibilidade, ativos esses que são um dos importantes para qualquer organização, existindo assim uma segurança contra acesso não aprovado e para preservar a integridade e confidencialidade, disponibilidade dos dados.

A busca de dados acaba se tornado de importância não apenas paras as grandes corporações, mas também de maneira maléfica. Dada à grande importância e valor agregado dos dados para qualquer instituição, é necessário garantir a segurança destes ativos. Sem a segurança os dados sensíveis das empresas que sejam vazados, alterados ou até danificados podem gerar problemas em diversas esferas, criando uma quebra na confiança na instituição. Assim a presente pesquisa visa responder a seguinte questão: Qual a importância da proteção e utilização das informações contidas nos Bancos de Dados?

O objetivo geral desta pesquisa é: Identificar as questões das seguranças e a utilização das informações e dados armazenados nos Bancos de Dados. Para chegar nesse objetivo geral, se tem objetivos específicos: Conceituar Segurança da Informação e Dados; analisar os conceitos de um Banco de Dados; apresentar as características principais da Lei Geral de Proteção de Dados Pessoais (LGPD).

O tipo de pesquisa que será realizado nesse trabalho é a revisão de literatura, no qual será realizada uma consulta bibliográfica com a finalidade de coletar informações sobre o assunto que será abordado, serão utilizados trabalhos publicados nos últimos 15 anos encontrados em livros, dissertações e artigos científicos selecionados através de busca nos seguintes palavras-chaves: SGBD, Banco de dados, Sistema da Informação, segurança banco de dados e LGPD.

2. CONCEITOS DE SEGURANÇA E DA INFORMAÇÃO DE DADOS

A internet com a evolução dos anos acabou realizando na produção de grande volume de dados que são gerados a cada minuto, se tornado como citado por Oliveira (2012, p. 07):

> A internet se tornou um mecanismo que dissemina a informação em poucos segundos, tornando-a acessível em nível mundial, o que pode ser positivo ou

> negativo. Por isso existe a segurança da informação e suas medidas de controle e políticas de segurança, tendo como principal objetivo a proteção de informações de clientes e empresas. Essa evolução no meio tecnológico incentivou a fazer alterações de paradigmas, influenciando consideravelmente a forma como as empresas gerenciam seus negócios.

A informação sempre fez parte da nossa vida, a evolução da escrita ajudou na formalização da informação, permitindo sua reprodução e circulação de muitos desses ativos. Mas a sua proteção era básica, como apresentado por Fernandes (2013, p. 18):

> Se voltarmos na história, na época da Revolução Industrial, pouco se pensava em segurança da informação e, se pensavam, o problema era facilmente solucionado, porque as informações que circulavam em uma empresa eram feitas em formulários, apresentadas em papel, e eram arquivadas em armários com chaves.

Com essa evolução da tecnologia e da internet fez com que a internet gerasse ainda mais informações formando dados, como apontado por Paula e Cordeiro (2015, p.58): "A evolução tecnológica, somada aos avanços das áreas relacionadas à gestão, impele grande importância à informação, que passa a se configurar como um dos mais importantes ativos dentro de um ambiente organizacional". Desde então, a confidencialidade e a segurança desses ativos é uma preocupação eminente e a mais lembrada, relacionada ao tema.

Informação é um conjunto de dados que, por sua vez, gera informações, tornando em um ativo valioso para a organização. Segundo Fontes (2006, p.2) citado por Fernandes (2013, p. 17) "Informação é um recurso que move o mundo, além de nos dar conhecimento de como o universo está caminhando [...] É um recurso crítico para realização do negócio e execução da missão organizacional". Onde a proteção da informação passa por todo um processo apresentam elementos que fazem parte de todo processo sendo eles os ativo, vulnerabilidade, ataque e risco assim citado por Neto e Araujo (2019):

> As vulnerabilidades são erros que ainda não geraram incidentes, dependem de um agente causador tornando-as ameaças para a segurança da organização. As organizações devem proteger e verificar suas vulnerabilidades para não causar algo maior (NETO; ARAUJO, 2019).

Uma ameaça é são exploradas as vulnerabilidades causando um incidente indesejado causando um dano para organização (NETO; ARAUJO, 2019).

Os ataques é quando uma ameaça se torna bem-sucedida, causando um dano ainda maior para organização (NETO; ARAUJO, 2019).

Portanto, esses elementos são importantes em todo o processo da segurança, apresentando cada etapa em todo o processo significa. Sendo assim, apresenta que cada vez mais é necessário proteger esses ativos, com segurança.

Segurança, palavra essa que o seu significado é empregado na língua portuguesa, em que possui vários sentidos o que a torna, ficando difícil conceituar. Ela é mais facilmente encontrada quando se refere a capacidade de resistência à intrusão de um determinado edifício, por algum assaltante. Melhor falando, uma agência bancária pode-se dizer que tal prédio será mais ou menos seguro, depende dedo do grau de resistência apresentado. (ALEXANDRIA, 2009).

Um dos maiores atentados a segurança de dados, muito por conta da falta de backup

foi o atentado ao World Trade Center dos Estados Unidos (EUA), como citado por Castilho e Fontes (2012, p. 55):

> O maior exemplo e um dos maiores erros cometidos em questão de ambientes seguros para backups foi o atentado de 11 de setembro, onde foram derrubas as Torres Gêmeas nos EUA. Empresas localizadas na torre A tinham seus backups na torre B. Depois da queda das duas torres, algumas empresas simplesmente sumiram, deixaram de existir. Um erro que poderia ser contornado caso o backup estivesse localizado em outro lado da cidade, ou até distribuídos em outras cidades.

Atentado esses que não são comuns, mas o que normalmente acontecem nas organizações, são criminosos atrás de dados, principalmente bancários para conseguir usufruir de alguma forma deles, como apontado por Neves et al. (2021, p.8).

"O objetivo dos fraudadores é a busca de dados que as corporações detêm em seus bancos de dados, para conseguirem dados básicos de pessoas físicas ou jurídicas. Em poder das informações, criminosos conseguem se passar pelos verdadeiros proprietários dos documentos e assim efetuar quaisquer tipos de ilícitos, como compras, abrir empresas, conseguir empréstimos, trazendo para os verdadeiros donos dos dados, enormes prejuízos". A Figura 1 ilustra um exemplo de uma pirâmide de segurança.

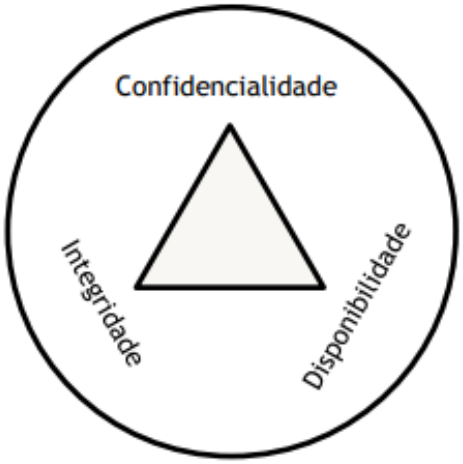


Figura 1- Exemplo de uma pirâmide de segurança

Fonte: RIGON (2010)

A Figura 1 apresenta um modelo de exemplo de uma pirâmide de segurança, apresentando confidencialidade, integridade e disponibilidade, seu conceito é apresentado por Raineri (2006):

Confidencialidade: visa manter informações sigilosas longe de pessoas não autorizadas para terem acesso a elas. Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo; Integridade: visa proteger a informação de modificações não autorizadas, imprevistas ou não intencionais. Assim, toda informação deve ser mantida na condição em que foi disponibilizada pelo seu proprietário; Disponibilidade: toda informação gerada ou adquirida deve estar disponível aos seus usuários no momento em que eles necessitem dela.

A proteção da informação tem deixado de ser tratada meramente como um assunto

técnico da área de informática sem importância, e vem sendo tratado com uma real necessidade nas grandes corporações, visto que a informação é o bem ativo mais valioso de grande importância de uma empresa como apontado por Gross e Gross (2013, p.42):

> A proteção de ativos torna-se cada vez mais necessária em função da concentração de informações em computadores; ela implica a proteção dos recursos de informações contra ameaças resultantes de danos ou deturpação de recursos do domínio.

A segurança da informação pode ser classificada em três camadas, podendo ser físicas, tecnológicas e humanas. Tendo como foco de muitas empresas apenas a camada tecnológica. A classificação desses aspectos, foi apontado por Netto e Silveira (2007):

1. A camada física é o ambiente onde está instalado fisicamente o hardware - computadores, servidores, meio de comunicação - podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis.
2. A camada tecnológica é caracterizada pelo uso de softwares - programas de computador - responsáveis pela funcionalidade do hardware, pela realização de transações em base de dados organizacionais, criptografia de senhas e mensagens.
3. A camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de TI, seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social.

A participação humana é uma das principais pois ela que manipula os elos, correta ou incorretamente, elos esses que são: senhas, logins, firewalls, criptografia, equipamentos, pendrives, antivírus entre outros procedimentos que possuem o foco de promover a segurança dos ativos das organizações, tendo acesso a Tecnologia da informação (TI).

3. CONCEITOS DE BANCO DE DADOS

Antigamente, as empresas guardavam as informações em arquivos físicos em armários, o que acabava causando grande acúmulo de papel e dificultava a organização, com a evolução das tecnologias as empresas passaram a investir na aquisição de computadores e as informações de dados passaram a ser armazenadas em bancos de dados. Como apresentado por Oliveira (2017, p.17):

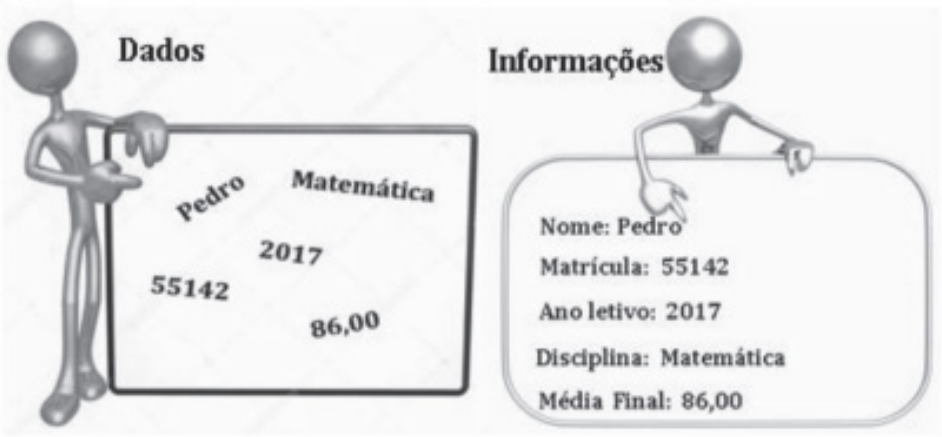
> Coleção de dados que guardam alguma relação entre si. São exemplos: uma agenda de telefones, um caderno de receitas, uma lista de presença de um curso qualquer, o conjunto de pacientes de um médico, um dicionário, um catálogo de tintas de um fabricante.

Esses tipos de bancos de dados acabaram se tornado importante para a sociedade, onde poderia fazer a pesquisa de forma alfabética ou por data para que pudesse ser encontrada a pessoa. Com o avanço da tecnologia e informática surgiu o banco de dados tecnológico, com o objetivo na velocidade para obter essa informação. O banco de dados é uma forma de gerenciar e manter um conjunto de informações, de forma organizada

(BAZZI, 2013).

Antes deve-se lembrar que Dados e Informação possuem diferença onde Dados assim como citado por Silva e Santana (2018, p.13) é “Um dado pode ser definido como um fato bruto, em sua forma primária, que em muitas vezes não faz sentido sozinho” e a informação é explicada também por Silva e Santana (2018, p.13) “Já a informação consistem em um agrupamento de dados de forma organizada, apresentando o significado dos dados de maneira que possa ser interpretado pelas pessoas e gerar conhecimento”.

A Figura 2 ilustra um exemplo dos dados e informação.



Fonte: Silva e Santana (2018)

Figura 2 - Exemplo dos dados e informação.

A figura 2 apresenta de forma para facilitar o entendimento, de que forma os dados e as informações se apresentam, onde a informação pega os dados e organiza para melhor entender. Como citado por Matsumoto (2006, p.46):

> Os dados, os quais tomam o maior volume da memória do computador, oferecem pouca utilidade estratégica na hora de se tomar decisões. A partir dos dados organizados é possível obter muita informação armazenada em computadores centrais proporcionando fácil acesso aos usuários através da rede de comunicações, desenvolvidos para fins específicos como a criação de um banco de dados empresarial realizado pelas ferramentas dos Sistemas Gerenciadores de Banco de Dados (SGBD).

Os principais elementos de um banco de dados (BD) são os campos, os registros, as tabelas e os relacionamentos, assim citador por Silva e Santana (2018, p.13):

> Um campo pode ser definido como a unidade mínima de armazenamento para os valores de uma tabela.
>
> Um registro é uma coleção de campos inter-relacionados e identifica a entrada de um item exclusivo de informação em uma tabela.
>
> Uma tabela representa um objeto e contém todos os dados de um BD. Os dados são organizados de maneira lógica em um formato de linhas e colunas, análogo a uma planilha. Cada linha representa um registro exclusivo e cada coluna representa um campo.

A Figura 3 principais elementos de um Banco de Dados.

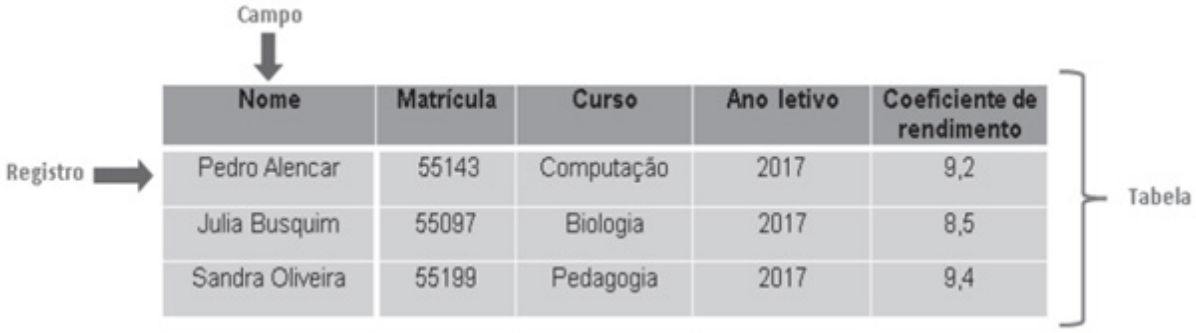


Figura 3 - Exemplo principais elementos de um Banco de Dados.

Fonte: Silva e Santana (2018)

A figura 3 apresenta de forma para facilitar o entendimento, ilustrar os principais elementos de um banco de dados, como eles se localizam em uma tabela.

Em um banco de dados, pode-se dividir em três diferentes usuários, assim citado por Ferrareto e Nishimura (2018, p.20):

> Administradores de Banco de Dados (DBA) é o responsável por manter e zelar por todas as bases de dados. Também controla toda a parte de segurança e controle de acesso, concedendo aos usuários as permissões que cada um pode ter na manipulação e no acesso aos dados. Tem um papel essencial para que o banco de dados possa garantir acesso rápido e eficaz, analisando todos os objetos e programas dentro dele, e também realizando rotinas de backup e restauração para evitar perdas em caso de falha.

Desenvolvedores são responsáveis por implementar e modelar a base de dados. Seu principal papel é desenvolver aplicações (programas escritos em outras linguagens, como C#, PHP, Java, entre outras), conectando ao banco de dados do sistema, podemos, assim, tornar o acesso e a manipulação de dados mais simples ao usuário final (FERRARETO; NISHIMURA, 2018).

Usuários esse grupo trabalha diariamente com a aplicação desenvolvida pelos desenvolvedores, sendo responsável por dar entrada de dados e alterar os já existentes, produzindo novas informações. Esses usuários não precisam ter nenhum conhecimento sobre o banco de dados, pois, para eles, ele já é transparente, só interessa a informação que está salva nele e que possam recuperá-la (FERRARETO; NISHIMURA, 2018).

Dos grupos apresentados o mais importante é o usuário, pois possivelmente ele que dá vida ao banco de dados. Onde ele utiliza e explora o banco de dados para buscar e armazenar novas informações no banco de dados.

Com avanço da tecnologia e com números de dados sendo gerados surge a necessidade de criar um sistema de gerenciamento de banco de dados e o para administrador do Banco de Dados. Assim apresentado por Massino e Roland (2015, p.02) “para que os dados possam ser mantidos são utilizados os SGBD nos quais os dados são armazenados de forma organizada, ficando disponíveis para serem consultados”. Facilitando a realização de algumas ações do processamento, manipulação e compartilhamento do banco de dados.

O SGDB, ou Sistema de Gerenciamento de Banco de Dados é o conjunto de programas de softwares responsáveis pelo gerenciamento de uma base de dados, como citado por Silva (2011, p.19) “é um software de caráter geral para a manipulação eficiente de gran-

des coleções de informações estruturadas e armazenadas de uma forma consistente e integrada".

Sistemas Gerenciadores de Bancos de Dados (SGBD) possuem o objetivo de fornecer, assegurar, administrar e prover mecanismos adequados ao armazenamento de dados. Assim citado por Silva (2011, p.21):

> Fornece interfaces amigáveis e padronizadas para o armazenamento e acesso aos dados, poupando os usuários dos detalhes da implementação interna. Assegurar a privacidade dos dados através de medidas de segurança como: atribuição de permissões de acesso; criação de visões; e fornecimento de senhas de acesso, evitando o acesso a dados por pessoas não autorizadas. Administrar acessos concorrentes aos dados, permitindo que diferentes usuários compartilhem simultaneamente a mesma coleção de dados. Prover mecanismos para a recuperação de dados em caso de eventuais paradas e falhas do sistema, as quais podem ocorrer por causa de erros de software, interrupção no suprimento de energia, defeito de hardware, queda na comunicação com o servidor etc. Qualquer falha pode resultar na perda de dados processados pelo SGBD no momento da parada. A perda desses dados pode levar o BD a uma condição de inconsistência que, se não evitada, torna a tecnologia pouco confiável. Portanto, durante uma venda, o estoque deve ser atualizado e, se uma falha ocorre após a venda, mas antes da atualização do estoque, o BD ficará inconsistente.

4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A evolução da escrita se apresenta como a primeira estruturação da informação, permitindo sua reprodução de geração em geração

Assim com o avanço da tecnologia e a imensa produção de dados como já citado trouxe uma grande importância na necessidade na proteção e limites de bens dos dados armazenados, limites éticos a coleta, utilização e distribuição de informações pessoais, acaba surgindo leis de proteção para esses dados. Como citado por Doneda (2011, p.92): "por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental."

Dados esses que em alguns momentos parecem ser sem relevância, mas quando passam a ser organizados, acabam evoluindo para dados bastante relevantes podendo ser sobre determinada pessoa, trazendo informações pessoais sobre ela (TEFFÉ; VIOLA, 2020).

O problema desses dados quando passam a ter relevância, que podem passar a ter um tipo de manipulação, podendo até discriminar certos usuários. Como citado por Rank e Berberi (2022, p.26):

> Paulatinamente, os dados dos indivíduos, dispersos na rede, dizem mais sobre eles e quem os manipula sabe, inclusive, mais sobre eles próprios. Tal capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência futuramente é uma verdadeira "mina de ouro" para a abordagem publicitária.

Em 2018, houve o da empresa da Cambridge Analytica, que usou sem autorização dados pessoais de milhões de pessoas do Facebook com objetivo de propaganda política, manchou a reputação da rede social em questão de privacidade de dados. Como citado por Barcelos (2021, p. 91):

> Um exemplo foi o escândalo envolvendo o Facebook e a empresa de análise de dados Cambridge Analytica, em 2008. Nessa ocasião houve revelação de que as práticas pouco ortodoxas da empresa poderiam ter influenciado campanhas eleitorais, como a que elegeu Donald Trump, o que sacudiu as manchetes de jornais pelo mundo todo – virando até tema para um documentário produzido pela Netflix. Mais tarde, o próprio Facebook admitiu o vazamento de dados de 87 milhões de usuários de 10 países – incluindo quase 445 mil brasileiros.

Os dados podem ser pessoais e sensíveis, como explicado por Lima, Barros, Ribeiro e Guterres (2021, p. 06):

> Dados pessoais conceitua-se como sendo dado pessoal, toda e qualquer informação relacionada a uma pessoa física, que seja identificada ou identificável. Portanto, qualquer informação que permita a identificação de determinado indivíduo, vem a ser considerada dado pessoal. Os dados pessoais mais comuns são aqueles inerentes a qualquer pessoa natural, como o nome, sobrenome, documentos de identificação, endereço residencial, entre outros. No decorrer do artigo 5º a Lei também dispõe acerca dos dados pessoais sensíveis, no qual conceitua-se como sendo dados referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Neste contexto os dados pessoais sensíveis necessitam de condições especiais para o seu tratamento, visto que devido à sua sensibilidade podem levar a realização de atitudes discriminatórias contra seus titulares e, por esse motivo, precisam de proteção especial quando vinculados a uma pessoa natural.

Esse assunto de proteção de dados já existia no Brasil, mas não especificamente a proteção de dados. Como apresentado por Lugati e Almeida (2022, p.02):

> O assunto de proteção de dados já era indiretamente tratado em legislações esparsas como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Contudo, não existia regulamentação que abordasse especificamente a problemática da proteção de dados, o que colocou em destaque a importância de se ter uma legislação específica sobre isso.

A LGPD tem o objetivo principal de proteção aos dados pessoais das pessoas naturais, pela transparência prevista de forma constitucional, em que se aproxima das normas já vigentes no Brasil que tratam sobre o assunto mesmo que de forma indireta (SANTOS, 2020)

O surgimento da Lei Geral de Proteção de Dados do Brasil (LGPD), Lei 13.709/2018, surgiu como um desafio para as empresas que lidam com dados pessoais. Como citado por Ramos (2019, p.14):

> O legítimo interesse somente poderá fundamentar o tratamento de dados para finalidades legítimas, consideradas a partir de situações concretas, respeitadas as legítimas expectativas do usuário e os direitos previstos na LGPD.

Surgimento esse que teve influência europeia, do GDPR (*General Data Protection Regulation*), brasileira passaram a ter o dever de adequação aos termos da referida Lei, o que passou inclusive pelas variadas áreas do Direito trazendo consigo a colocação do Brasil no circuito internacional dentre os países que dispõem de legislação protetiva dos dados pessoais (LIMA et al., 2022).

Assim, explicado por Freire e Dissenha (2021):

> Ademais, no contexto da Lei Geral de Proteção de Dados, estão expostas diferentes formas de preocupação de uso abusivo de dados pessoais: mineração para fins mercadológicos e publicitários, discriminação de qualquer espécie; divulgação dos dados do usuário sem o seu consentimento; troca prevenção a mecanismos diversos de fraude, por exemplo. A lei exige que medidas de segurança sejam tomadas para garantir a segurança e o sigilo de dados, além de sugerir a necessidade de formulação de programas de governança e manuais de boas práticas a fim de evitar e conter incidentes no tratamento destes dados.

A Lei Geral de Proteção de Dados trata da proteção de dados como regra, sendo um dos objetivos principais da legislação, as primeiras palavras do artigo apresentado por Brasil (2018):

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD estabelece diretrizes importantes e obrigatórias para o processamento e armazenamento de dados pessoais. Ela teve como base a GDPR (*General Data Protection Regulation*), que em 2018 na entrou em vigência na União Europeia. De acordo com o Art. 2 da Lei nº 13.709, de 14 de agosto de 2018, "a disciplina da proteção de dados pessoais tem como fundamentos" (BRASIL, 2018):

> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

A Lei Geral de Proteção de Dados em seu artigo 6° traz importantes atividades em que se refere ao tratamento de dados pessoais (Brasil, 2018):

"I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Além que a empresa poderá ser penalizada, conforme as sanções previstas no artigo 52, mas possuem caráter apenas administrativo e financeiro para as empresas, mas não envolve reflexos penais (BRASIL, 2018):

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a

> infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019).

5. CONSIDERAÇÕES FINAIS

O presente estudo trouxe à tona a importância da segurança de banco de dados. Se justifica o tema escolhido por se tratar de ativos muito valiosos contidos nos banca de dados, visto que armazenam dados e informações muito importantes para qualquer empresa.

Nessa perspectiva a presente pesquisa buscou respostas para o seguinte problema: Qual a importância da proteção e utilização das informações contidas nos Bancos de Dados? teve como objetivo identificar as questões das seguranças e a utilização das informações e dados armazenados nos Bancos de Dados. Para tanto, três capítulos descreveram um pouco sobre conceitos de segurança da informação e dos dados, conceitos de banco de dados e a Lei Geral de Proteção de Dados Pessoais (LGPD).

Em relação aos conceitos de segurança da informação e dos dados, observa-se que existe uma diferença entre eles em que dados é um registro ainda não processado, e a informação é os dados após o tratamento. Sendo assim, apresentando a importância desses ativos a serem protegidos.

A respeito dos conceitos de banco de dados, torna-se importante salientar que com a evolução da tecnologia e dos meios de comunicação os Bancos de dados se tornaram importantes para as empresas, onde o banco de dados é um meio de organização e armazenamento de informação adquiridas pela empresa, em que normalmente guardadas em um sistema de computador.

Sobre a Lei Geral de Proteção de Dados Pessoais, entende-se que seu principal objetivo é estabelecer normas para a coleta e o tratamento de dados pessoais. Leia essa destinada a população brasileira, que foi inspirada pelo Regulamento Geral de Proteção de Dados da União Europeia, que trata sobre os cidadãos europeus.

Diante do estudo realizado, é importante manter seguro os bancos de dados das organizações, por conter inúmeras informações pessoais, pois passa a ser visado para ataques cibernéticos, informações que podem ir desde nome às contas bancárias. Assim é possível afirmar que os objetivos específicos foram alcançados neste estudo científico, por meio da fundamentação teórica na pesquisa bibliográfica.

Referências

ALEXANDRIA, João Carlos Soares de. **Gestão de segurança da informação - uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica**. 2009. Tese (Doutorado em Tecnologia Nuclear - Aplicações) - Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009. doi:10.11606/T.85.2009.tde-22092011-095831. Disponível: http://pelicano.ipen.br/

PosG30/TextoCompleto/Joao%20Carlos%20Soares%20de%20Alexandria_D.pdf Acesso em: 09 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF. Presidência da República. [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 09 out. 2022.

BARCELOS, Ana Karollina; SOUZA, Celestyane Lívia Severino de; CARMO, João Pedro Mendes do; FARIA, Marcela Campos; ALCÂNTARA, Melyssa; CAMARGOS, Pedro Augusto Diniz. A LEI GERAL DE PROTEÇÃO DE DADOS E O PAPEL DO DPO. Revista Projetos Extensionistas, Pará de Minas, v. 1, n. 2, p. 87-92, 2021. Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/455. Acesso em: 08 out. 2022.

BAZZI, Cláudio Leones. Introdução a banco de dados. Curitiba: Editora Utfpr, 2013. 91 p. Disponível em: http://proedu.rnp.br/bitstream/handle/123456789/1550/Introducao_banco_dados_ISBN.pdf. Acesso em: 07 out. 2022.

CASTILHO, Sérgio Duque; FONTE, Miguel Feitoza da. Política de segurança da informação aplicada em uma instituição de ensino mediante análise de Risco. Retec - Revista de Tecnologias, Ourinhos, v. 5, n. 2, p. 51-66, dez. 2012. Disponível em: https://www.fatecourinhos.edu.br/retec/index.php/retec/article/view/99. Acesso em: 09 out. 2022.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, *[S. l.]*, v. 12, n. 2, p. 91–108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 09 out. 2022.

FERNANDES, Nélia O. Campo**. Segurança da Informação**: Cuiabá: IFRO, 2013. Disponível em: http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y#:~:text=Fontes%20(2006%2C%20p.,e%20execu%C3%A7%C3%A3o%20da%20miss%C3%A3o%20organizacional%E2%80%9D. Acesso em 09 out. 2022.

FERRARETO, Leonardo De Marchi; NISHIMURA, Roberto Yukio. **Banco de dados I**. Londrina: Editora e Distribuidora Educacional S.A., 2018. Disponível em: https://biblioteca-virtual.com/detalhes/ebook/6087051254aa8872fb666994. Acesso em: 07 out. 2022.

FREIRE, J. R. B.; DISSENHA, L. A. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E AS COOPERATIVAS: IMPRESSÕES INICIAIS. **Revista Eletrônica do Curso de Direito da UFSM**, *[S. l.]*, v. 16, n. 1, 2021. DOI: 10.5902/1981369441636. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/e41636. Acesso em: 8 out. 2022.

GROSS, Christian Meinecke; GROSS, Jan Charles. **Segurança em Tecnologia da Informação**. Indaial: Uniasselvi, 2013. Disponível em: https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=15312. Acesso em: 09 out. 2022.

LIMA, Marilia Gabriela Silva; BARROS, Thiago Medeiros de; RIBEIRO, Luis Otoni; GUTERRES, Lisandra Xavier. Manual LGPD: Lei Geral de Proteção de Dados. Pelotas: Ifsul, 2021. 14 p. Disponível em: http://proedu.rnp.br/handle/123456789/1704. Acesso em: 07 out. 2022.

LIMA, A. D.; NETO, E. M. M. . A EFICIÊNCIA DO CONSENTIMENTO FRENTE A (HIPER)VULNERABILIDADE INFORMACIONAL DO TITULAR DE DADOS NO CONTEXTO PROTETIVO DA LGPD. **REVISTA JURÍDICA DIREITO, SOCIEDADE E JUSTIÇA**, *[S. l.]*, v. 9, n. 13, p. 226–247, 2022. Disponível em: https://periodicosonline.uems.br/index.php/RJDSJ/article/view/7005. Acesso em: 8 out. 2022.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito, [S.L.], v. 14, n. 01, p. 01-20, 29 jun. 2022. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764/7380. Acesso em: 07 out. 2022.

MASSINO, Eduardo Galvani; ROLAND, Carlos Eduardo de França. **Banco de dados objeto-relacional para aplicações web**. Resiget, São Paulo, v. 5, n. 1, p. 01-11, 2015. Disponível em: https://periodicos.unifacef.com.br/index.php/resiget/article/view/894/767. Acesso em: 09 out. 2022.

MATSUMOTO, Cristina Yoshie. A IMPORTÂNCIA DO BANCO DE DADOS EM UMA ORGANIZAÇÃO. Maringá Management: Revista de Ciências Empresariais, Maringá, v. 3, n. 1, p. 45-55, jun. 2006. Disponível em https://core.ac.uk/download/pdf/199473173.pdf. Acesso em: 07 out. 2022

NETO, Pedro Tenório MASCARENHAS; ARAUJO, Wagner Junqueira de. SEGURANÇA DA INFORMAÇÃO: uma visão sistêmica para implantação em organizações. João Pessoa: Editora Ufpb, 2019. 160 p. Disponível em: https://www.researchgate.net/publication/339107559_SEGURANCA_DA_INFORMACAO_Uma_visao_sistemica_para_implantacao_em_organizacoes. Acesso em: 09 out. 2022.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems**

and Technology Management, v. 4, p. 375-397, 2007. Disponível em: https://www.scielo.br/j/jistm/a/Vx8Yp-v6mDjxdYkKKrfYVgqz/?lang=pt&stop=next&format=html. Acesso em: 09 out. 2022

NEVES, D. L. F.; LOPES , T. S. DE A.; PAVANI, G. C.; SALES, R. M. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, v. 13, p. 186-198, 9 jun. 2021. Disponível em: https://fatecpg.edu.br/revista/index.php/ps/article/view/171. Acesso em: 8 out. 2022.

OLIVEIRA, p. L. De. **Segurança da informação nas pequenas empresas**. Revista tecnologia, [s. L.], v. 33, n. 1, p. 7–11, 2012. Disponível em: https://ojs.unifor.br/tec/article/view/4571. Acesso em: 09 out. 2022

OLIVEIRA, Ruy Flavio de. Segurança de sistemas de banco de dados. Londrina: Editora e Distribuidora Educacional, 2017. 196 p. Disponível em: https://biblioteca-virtual-cms-serverless-prd.s3.us-east-1.amazonaws.com/ebook/1407-seguranca-de-sistemas-de-bancos-de-dados.pdf. Acesso em: 05 out. 2022.

PAULA, Lorena Pires de; CORDEIRO, Douglas Farias. **Políticas de segurança da informação em instituições públicas**. Resiget, São Paulo, v. 6, n. 2, p. 58-68 [set.], 2015. Disponível em: https://periodicos.unifacef.com.br/index.php/resiget/article/view/1046/843. Acesso em 09 out. 2022

RAINERI, Leandro Lima. Análise de adequação da política de segurança da informação dos Ministérios Federais frente as normas do departamento de Segurança da Informação e Comunicações. 2016. 71 f. Monografia (Especialização governança em tecnologia da informação) - Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília, Brasília, 2016. Disponível em: https://repositorio.uniceub.br/jspui/handle/235/12207. Acesso em: 09 out. 2022.

RANK, Angela Teresinha; BERBERI, Marco Antonio Lima. Big data e direitos fundamentais sob o enfoque da Lei Geral de Proteção de Dados (LGPD). International Journal Of Digital Law, Belo Horizonte, v. 3, n. 2, p. 09-28, 18 jul. 2022. International Journal of Digital Law. http://dx.doi.org/10.47975/digital.law.vol.3.n.2. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/rank2022. Acesso em: 09 out. 2022.

RAMOS, Pedro. **A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD**. Publicado em, v. 16, n. 07, 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/07/MP_guia_LGPD.pdf. Acesso em: 8 out. 2022.

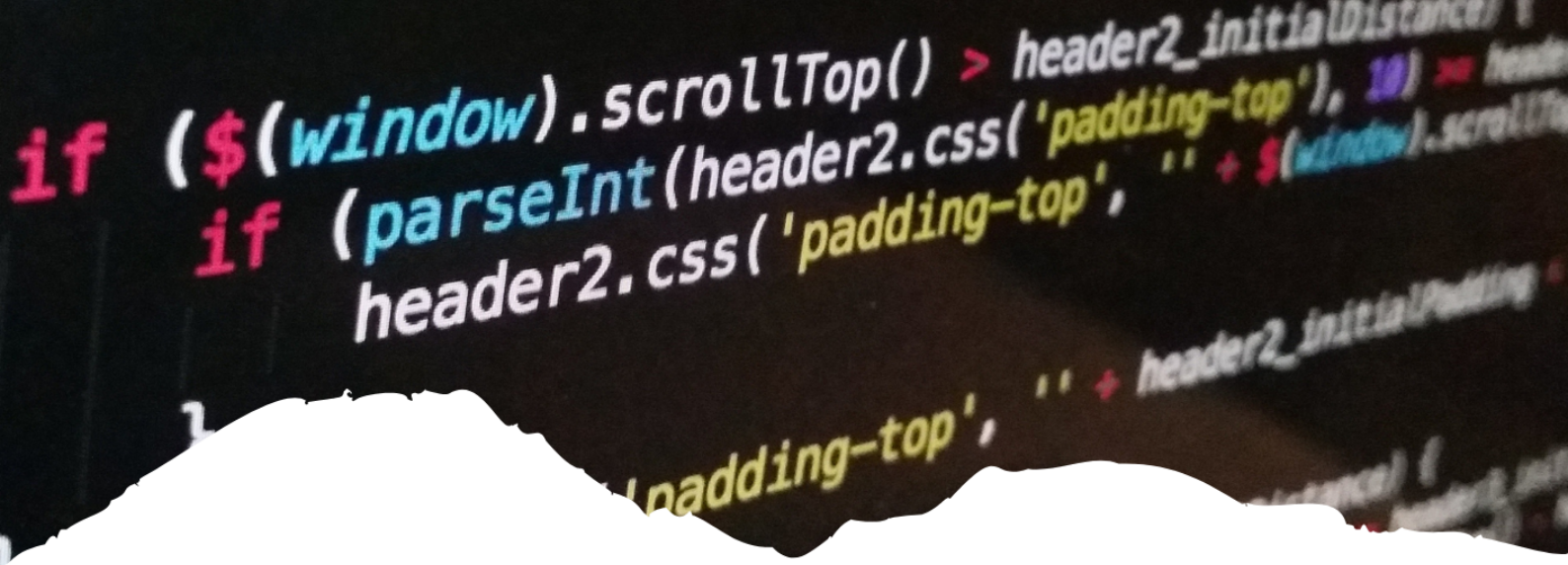
RIGON, Evandro Alencar. Modelo para Avaliação da Maturidade da Segurança da Informação. 2010. 96 f. Tese (Doutorado) - Curso de Sistemas de Informação, Universidade Federal de Santa Catarina, Florianópolis, 2010. Disponível em: https://repositorio.ufsc.br/handle/123456789/184549. Acesso em:14 set. 2022.

SANTOS, Raquel Gitirana Torquato dos. A Lei Geral de Proteção de Dados Brasileira:: uma política pública regulatória. 2020. 68 f. Monografia (Especialização) - Curso de Avaliação de Políticas Públicas, Instituto Serzedello Corrêa, Brasília, 2020. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/a-lei-geral-de-protecao-de-dados-brasileira-uma-politica-publica-regulatoria.htm. Acesso em: 08 out. 2022.

SILVA, Nathalia dos Santos; SANTANA, Gisele Alves. **Fundamentos de banco de dados**. Londrina: Editora e Distribuidora Educacional S.A., 2018. Disponível em: https://biblioteca-virtual.com/detalhes/ebook/6087051554aa8872fb6669ad. Acesso em: 07 out. 2022.

SILVA, Vanderson José Ildefonso. Banco de dados : Curso Técnico de Informática. Colatina: Ifes/Cead, 2011. 176 p. Disponível em: http://proedu.rnp.br/handle/123456789/698. Acesso em: 07 out. 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, 9 maio 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 07 out. 2022



3

APLICAÇÕES DE TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL NA SAÚDE

APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN HEALTH

Carla Thamires Bezerra Soares

Resumo

A informática médica tem progredido rapidamente e já não se pode negar a relevância de sua contribuição para melhorias na prática clínica. Esta evolução vem acontecendo de forma paralela e dinâmica à do conhecimento científico em saúde e nesta trajetória, as boas oportunidades devem ser reconhecidas, analisadas e utilizadas. Neste cenário destacam-se a importância do desenvolvimento e implementação de sistemas de informação adequados na prestação de serviços voltados para a área da saúde. A IA promete mudar a prática da medicina de formas até então desconhecidas, mas muitas de suas aplicações práticas ainda são incipientes e precisam ser mais bem exploradas e desenvolvidas. Os profissionais médicos também precisam entender e se acostumar com esses avanços para uma melhor prestação de cuidados de saúde às massas. Neste sentido, o objetivo geral deste trabalho é discutir a importância e contribuição da aplicação de tecnologias de inteligência artificial na área da saúde. O tipo de pesquisa a ser realizado neste trabalho, será uma Revisão de Literatura, no qual será realizada uma consulta a livros, dissertações e artigos científicos selecionados através de busca nas seguintes bases de dados Scielo, Lilacs, PubMed Central, Medscape Neurology. O período dos artigos pesquisados serão os trabalhos publicados nos últimos 5 anos. Conclui-se que as tecnologias de inteligência artificial (IA) que estão cada vez mais presentes nos negócios modernos e na vida cotidiana também estão sendo aplicadas constantemente à saúde. O uso de inteligência artificial na área da saúde tem o potencial de auxiliar os profissionais de saúde em muitos aspectos do atendimento ao paciente e dos processos administrativos, ajudando-os a melhorar as soluções existentes e superar os desafios mais rapidamente.

Palavras-chave: Inteligência artificial, Saúde, Tecnologias.

Abstract

Medical informatics has progressed rapidly and the relevance of its contribution to improvements in clinical practice can no longer be denied. This evolution has been happening in a parallel and dynamic way to that of scientific knowledge in health and in this trajectory, the good opportunities must be recognized, analyzed and used. In this scenario, the importance of developing and implementing adequate information systems in the provision of services aimed at the health area stands out. AI promises to change the practice of medicine in hitherto unknown ways, but many of its practical applications are still nascent and need to be further explored and developed. Medical professionals also need to understand and get used to these advances in order to better deliver health care to the masses. In this sense, the general objective of this work is to discuss the importance and contribution of the application of artificial intelligence technologies in the health area. The type of research to be carried out in this work will be a Literature Review, in which books, dissertations and scientific articles will be consulted through a search in the following databases: Scielo, Lilacs, PubMed Central, Medscape Neurology. The period of the researched articles will be the works published in the last 5 years. It is concluded that artificial intelligence (AI) technologies that are increasingly present in modern business and everyday life are also being constantly applied to health. The use of artificial intelligence in healthcare has the potential to assist healthcare professionals in many aspects of patient care and administrative processes, helping them to improve existing solutions and overcome challenges more quickly.

Keywords: Artificial intelligence, Health, Technologies.

1. INTRODUÇÃO

Nos últimos anos, com o avanço da tecnologia e suas novas descobertas, a medicina diagnóstica evoluiu bastante favorecendo pacientes e médicos, uma vez que exames, procedimentos e resultados se tornaram mais simples, rápidos e seguros. A informática médica tem progredido rapidamente e não se pode negar a relevância de sua contribuição em práticas clínicas e medicas. Tal evolução vem acontecendo de forma paralela e dinâmica à do conhecimento científico em saúde. Os diferentes tipos de equipamentos de monitoramento em hospitais são em sua grande maioria baseados em programação. Muitos dos modernos métodos de digitalização e imagem são em grande parte com base na tecnologia do computador. Sendo capaz de implementar técnicas novas, pouco invasivas e com menos riscos aos pacientes graças a evolução da ciência.

A importância do desenvolvimento e implementação de sistemas de informação adequados na prestação do cuidado em substituição aos prontuários de papel; a participação estratégica de profissionais de saúde no processo da informatização; e o investimento na formação de futuros médicos capazes de participar, compreender e usufruir cada vez mais desta área do conhecimento, de forma integrada à medicina são hoje indispensáveis. A tecnologia aplicada na área da saúde permite identificar tumores em fases iniciais o que facilita o tratamento aumentando significativamente as chances de cura. Através de exames específicos e programação, o médico pode utilizar um sistema de processamento de imagem para melhorar a imagem de tomografias permitindo uma melhor visualização da imagem proporcionando um diagnóstico precoce.

Neste sentido, o espantoso progresso experimentado pelo uso dos meios informáticos nos últimos anos é um indicador do nível de integração, utilidade e excepcional papel que os computadores desempenham no mundo contemporâneo e em particular na esfera da saúde. O desenvolvimento de tecnologias associadas a técnicas de inteligência artificial (IA), aplicadas à medicina, representa uma nova perspectiva, que pode reduzir custos, tempo, erros médicos; bem como promover a utilização de recursos humanos em ramos médicos com maiores exigências. Tecnologia e medicina seguem um caminho paralelo nas últimas décadas.

Os avanços tecnológicos estão mudando o conceito de saúde e as necessidades de saúde estão influenciando o desenvolvimento da tecnologia. A inteligência artificial (IA) é composta por uma série de algoritmos lógicos suficientemente treinados a partir dos quais as máquinas são capazes de tomar decisões para casos específicos com base em regras gerais. Esta tecnologia tem aplicações no diagnóstico e acompanhamento de pacientes com avaliação prognóstica individualizada dos mesmos. Além disso, essa tecnologia quando combinada com a robótica, pode criar máquinas inteligentes que fazem propostas de diagnóstico ou que são muito mais eficientes em seu trabalho. Neste contexto, surge a seguinte questão norteadora: qual a importância e contribuição da aplicação de tecnologias de inteligência artificial na área da saúde?

O objetivo geral deste trabalho é discutir a importância e contribuição da aplicação de tecnologias de inteligência artificial na área da saúde. Os objetivos específicos são: conceituar a inteligência artificial; destacar as diferentes tecnologias baseadas em inteligência artificial e suas contribuições; correlacionar e evidenciar as aplicações de tecnologias baseadas em inteligência artificial na área da saúde.

O tipo de pesquisa a ser realizado neste trabalho, será uma Revisão de Literatura, no qual será realizada uma consulta a livros, dissertações e por artigos científicos selecionados

através de busca nos seguintes bases de dados Scielo, Lilacs, PubMed Central, Medscape Neurology. O período dos artigos pesquisados serão os trabalhos publicados nos últimos 5 anos. As palavras-chave utilizadas na busca serão: inteligência artificial, saúde, tecnologias.

Portanto, a IA é uma tecnologia que será cada vez mais presente em diversas áreas da saúde por meio de máquinas ou programas de computador, que de forma mais ou menos transparente para o usuário, se tornará uma realidade cotidiana nos processos de saúde. Os profissionais da área têm de conhecer esta tecnologia, as suas vantagens e desvantagens, porque será parte integrante de seu trabalho. Num cenário de crescimento e envelhecimento populacional, a necessidade de atender a saúde da população o mais rápido possível torna-se uma prioridade que parece ser resolvida, em maior ou menor medida, através do desenho e aplicação de novas tecnologias que permitem automatizar processos que hoje são realizados manualmente e presencialmente. Os desafios, no entanto, são muitos e diversos. Por um lado, a necessidade de reduzir preconceitos para que a implementação dessas técnicas não aprofunde a discriminação e as desigualdades existentes nas sociedades.

2. INTELIGÊNCIA ARTIFICIAL

As tecnologias de inteligência artificial (IA) que estão cada vez mais presentes nos negócios modernos e na vida cotidiana também estão sendo aplicadas constantemente à saúde. O uso de inteligência artificial na área da saúde tem o potencial de auxiliar os profissionais de saúde em muitos aspectos do atendimento ao paciente e dos processos administrativos, ajudando-os a melhorar as soluções existentes e superar os desafios mais rapidamente. A maioria das tecnologias de IA e saúde tem forte relevância para o campo da saúde, mas as táticas que elas suportam podem variar significativamente entre hospitais e outras organizações de saúde. A IA estar sendo aproveitada para implantar invenções eficientes e precisas que ajudarão a cuidar de pacientes que sofrem das mais diversas doenças.

A Inteligência Artificial (IA) refere-se à simulação da inteligência humana em máquinas como computadores ou robôs que são programados para imitar funções cognitivas que os humanos associam a outras mentes humanas, como aprendizado e resolução de problemas. Inteligência artificial, aprendizado de máquina e aprendizado profundo são palavras de ordem populares que todo mundo parece usar hoje em dia (MA et al., 2017).

A inteligência artificial (IA) é um termo mais amplo do que os outros dois. O aprendizado de máquina inclui algoritmos para vários tipos de tarefas, como regressão, agrupamento etc., e os algoritmos devem ser treinados em dados. O aprendizado profundo é um campo muito jovem de inteligência artificial baseado em redes neurais artificiais. Os algoritmos de aprendizado profundo também exigem dados para aprender a resolver tarefas.

Segundo Kaplan e Haenlein (2019) a inteligência artificial é definida como uma habilidade de um sistema para interpretar corretamente dados externos para aprender por tal data e usar aqueles aprendizados para atingir objetivos específicos e tarefas por meio de adaptações flexíveis. Como as tecnologias baseadas em IA estão agora sendo integradas à vida cotidiana, a aplicação de tecnologias baseadas em IA será indispensável para todas as organizações. Mesmo que o aprendizado profundo tenha avançado na resolução de problemas nas áreas de IA por muitos anos, as organizações precisam considerar os custos computacionais a serem ocorridos no treinamento dos algoritmos usando a grande quantidade de dados.

De acordo com a Organização Mundial da Saúde (2016), 60% dos fatores relacionados à saúde individual e qualidade de vida se correlacionam com fatores de estilo de vida, como exercícios, dieta, sono, redução do estresse, abuso de substâncias e medicamentos e/ou recreação. As tecnologias auxiliadas por IA e seus aplicativos agora podem fornecer intervenções e lembretes de estilo de vida durante o dia com base nos sinais vitais de um indivíduo por meio de dispositivos digitais (DIGNUM, 2018).

Nas organizações de saúde, as tecnologias baseadas em IA estão definidas para transformar significativamente a maneira como os sistemas de saúde operam, otimizam e interagem com os pacientes e fornecem serviços de atendimento para aumentar a eficiência geral dos resultados dos pacientes. Espera-se que a IA facilite o diagnóstico de pacientes com doenças específicas (KRAUSOVÁ, 2017).

A Inteligência Artificial prova ser de imensa ajuda quando se trata de diagnosticar doenças relacionadas ao sangue possivelmente fatais em um estágio inicial. Com a ajuda de microscópios aprimorados por IA, os médicos agora podem escanear substâncias nocivas e bactérias em amostras de sangue a uma taxa muito mais rápida em comparação com a velocidade da varredura manual (KAPLAN; HAENLEIN, 2019). A IA permite que as máquinas aprendam a identificar bactérias no sangue e prever sua presença em amostras com uma precisão de 95%, reduzindo a mortalidade por uma grande margem (KRAUSOVÁ, 2017).

Obviamente, é imperativo que os profissionais de saúde levem em consideração todas as informações cruciais ao diagnosticar os pacientes. Como resultado, isso leva a peneirar várias notas não estruturadas complicadas mantidas em registros médicos. Se houver um erro no acompanhamento de um único fato relevante, a vida de um paciente pode ser colocada em risco (DAVENPORT et al., 2019).

A assistência do Processamento de Linguagem Natural (NLP) torna mais conveniente para os médicos restringir todas as informações relevantes dos relatórios dos pacientes. A Inteligência Artificial detém a capacidade de armazenar e processar grandes conjuntos de dados, que podem fornecer bancos de dados de conhecimento e facilitar o exame e a recomendação individualmente para cada paciente, ajudando assim a aprimorar o suporte à decisão clínica (BROOKS; TEGMARK, 2018).

O aprendizado de máquina é uma das formas mais comuns de inteligência artificial na área da saúde. É uma técnica ampla no centro de muitas abordagens de IA e tecnologia de saúde e há muitas versões dela. Usando inteligência artificial na área da saúde, a utilização mais difundida do aprendizado de máquina tradicional é a medicina de precisão (KRAUSOVÁ, 2017). Ser capaz de prever quais procedimentos de tratamento provavelmente serão bem-sucedidos com os pacientes com base em sua composição e na estrutura de tratamento é um grande avanço para muitas organizações de saúde. A maioria da tecnologia de IA na área da saúde que usa aplicativos de aprendizado de máquina e medicina de precisão requer dados para treinamento, para os quais o resultado final é conhecido. Isso é conhecido como aprendizado supervisionado (KRAUSOVÁ, 2017).

A inteligência artificial na área da saúde que usa aprendizado profundo também é usada para reconhecimento de fala na forma de processamento de linguagem natural (NLP) (DAVENPORT et al., 2019). Os recursos em modelos de aprendizado profundo normalmente têm pouco significado para observadores humanos e, portanto, os resultados do modelo podem ser difíceis de delinear sem a interpretação adequada. Outro papel significativo da Inteligência Artificial e suas ferramentas na área da saúde é que ela automatiza tarefas redundantes e demoradas (MA et al., 2017).

Isso faz com que os administradores tenham algum tempo livre e continuem trabalhando com outras tarefas importantes e necessárias. Há uma série de aplicações ad-

ministrativas para inteligência artificial na área da saúde. O uso de inteligência artificial em ambientes hospitalares é um pouco menos revolucionário nesta área em comparação com o atendimento ao paciente (KRAUSOVÁ, 2017). Mas a inteligência artificial nas áreas administrativas do hospital pode fornecer eficiências substanciais. A IA na área da saúde pode ser usada para uma variedade de aplicações, incluindo processamento de sinistros, documentação clínica, gerenciamento do ciclo de receita e gerenciamento de registros médicos.

Portanto, a Inteligência Artificial (IA) beneficiou muito o mundo, uma vez que sua popularidade cresceu nas últimas décadas. Especificamente, afetou a fabricação, educação, transporte, saúde e muitas outras áreas de interesse. Uma das principais áreas beneficiadas, a saúde, teve os avanços mais interessantes na forma de previsões para salvar vidas e prognósticos mais rápidos (DIGNUM, 2018). Isso é feito com o uso de algoritmos complexos para simular a cognição humana na análise de dados com e sem entrada humana. A maior vantagem se origina da capacidade de coletar informações, processá-las e fornecer uma saída bem definida ao usuário (DAVENPORT et al., 2019). As tecnologias assistivas também foram muito beneficiadas pela IA. Pessoas com deficiência e idosos, comumente chamados de pessoas necessitadas, estão sendo ajudados por pesquisadores que encontram maneiras inovadoras de colocar a inteligência artificial para trabalhar com suas condições atuais. Com os avanços na tecnologia e na ciência, as tecnologias assistivas continuarão a produzir plataformas novas e aprimoradas para ajudar a criar um melhor padrão de vida para esses indivíduos.

3. INTELIGÊNCIA ARTIFICIAL E SUAS TECNOLOGIAS

Para entender como a inteligência artificial pode ajudar no diagnóstico médico é necessário primeiro saber qual técnica é utilizada e como ela funciona. Segundo Othman (2001) redes neurais são uma das técnicas de IA mais populares implementadas em aplicações médicas. Ramesh (2004) corrobora quando afirma que a julgar pelo volume de publicação nas duas últimas décadas, rede neural artificial é a técnica de IA mais popular na medicina. Medeiros (2018) afirma que as redes neurais artificiais podem ser consideradas um dos adventos mais significativos da área da inteligência artificial. Haykin (2008) afirma que o trabalho em redes neurais artificiais, usualmente denominadas “redes neurais”, tem sido motivado desde o começo pelo reconhecimento de que o cérebro humano processa informações de forma inteiramente diferente do computador digital convencional. O cérebro é um computador (sistema de processamento de informação) altamente complexo, não linear e paralelo.

Ele tem a capacidade de organizar seus neurônios de forma a realizar certos processamentos muito mais rapidamente que o mais rápido computador digital hoje existente, como reconhecimento de padrões, percepção e controle motor. Conforme Medeiros (2018), o funcionamento das redes neurais possibilita o aprendizado de padrões que emergem com base na complexibilidade da interligação de elementos mais simples que simulam o comportamento de neurônios. Haykin (2008) define redes neurais como sendo um processador maciçamente paralelamente distribuído, construído com milhares de unidades de processamento simples, que tem a propensão natural para armazenar o conhecimento experimental e torná-lo disponível para o uso. Ainda segundo o autor, as redes neurais se assemelham ao cérebro em dois aspectos: O conhecimento é adquirido pela rede a partir de seu ambiente através de um processo de aprendizagem e as forças de conexão entre neurônios, conhecidas como sinápticas, são utilizadas para armazenar o conhecimento adquirido.

Medeiros (2018) afirma que redes neurais podem executar tarefas básicas como associação de padrões (quando determinado conjunto deve ser associado a outro conjunto), reconhecimento de padrões (quando um conjunto de padrões deve ser associado a um determinado identificador), aproximação de funções (quando uma rede neural pode ser utilizada para regressão de dados), controle (quando uma rede neural executa uma função de controle de um sistema de forma automatizada) e filtragem (quando uma rede neural é utilizada para extração de um ruído em determinado sinal). Luger (2013) explica que em redes neurais o processamento é paralelo e distribuído sem manipulação de símbolos. Os padrões de um domínio são codificados como vetores numéricos e as conexões entre componentes são também representadas por valores numéricos.

A transformação de padrões é resultado de operações numéricas como multiplicação de matrizes. As escolhas do projetista para uma arquitetura constituem o viés indutivo do sistema. Os algoritmos e as arquiteturas que implementam essas técnicas são normalmente treinados, ou condicionados em vez de serem explicitamente programados. A respeito da estrutura de uma rede neural Amato et al. (2013) diz que é formada por uma camada de "entrada", uma ou mais camadas "ocultas" e a camada de "saída". O número de neurônios em uma camada e o número de camadas depende fortemente da complexidade do sistema estudado. Portanto, a arquitetura de rede ideal deve ser determinada. Luger (2013) ainda acrescenta que para construir uma rede neural, por exemplo, o projetista deve criar um esquema para codificar padrões do mundo em quantidades numéricas da rede. A escolha de um esquema de codificação desempenha um papel crucial no sucesso ou no fracasso de aprendizado da rede.

A partir da criação dos neurônios artificiais e da criação de uma rede, as redes neurais adquirem a capacidade de aprender. Haykin (2008) explica que a propriedade que é de vital importância para uma rede neural é a habilidade de aprender a partir do seu ambiente e de melhorar o seu desempenho através da aprendizagem. A rede neural aprende sobre seu ambiente pelo processo interativo de ajustes aplicados a seus pesos sinápticos. Idealmente a rede se torna mais instruída sobre o seu ambiente após cada iteração do processo de aprendizagem. Assim Haykin (2008) define aprendizagem no contexto de redes neurais como um processo pelo qual os parâmetros livres de uma rede neural são adaptados através de um processo de estimulação pelo ambiente no qual a rede está inserida. O tipo de aprendizagem é determinado pela maneira pela qual a modificação dos parâmetros ocorre. Desta forma o processo de aprendizagem implica na rede neural ser estimulada por um ambiente, a rede sofrer modificações nos seus parâmetros livres como resultado deste estímulo e está responder de maneira nova ao ambiente, devido as modificações na sua estrutura interna.

Neste mesmo contexto, existem três características que definem a Big Data: seu volume, sua variedade e sua velocidade. Combinadas, essas características definem o que os profissionais se referem como "Big Data". Eles criaram a necessidade de uma nova classe de recursos para aumentar a forma como as coisas são feitas a fim de fornecer uma melhor linha de site e controlar os domínios de conhecimento existentes e a capacidade de agir sobre eles. Big Data oferece a oportunidade única de extrair percepção de um imenso volume, variedade e velocidade de dados, em contexto, além do que era anteriormente possível (ZIKOPOULOS; EATON, 2011).

Estes dados podem ser analisados e se extrair informações as quais não é possível se obter por meios tradicionais; estas informações adicionais podem auxiliar em diversas áreas incluindo a medicina. Zikopoulos e Eaton (2011) explicam que este grande volume traz novos desafios para os data centers administrarem. Com a explosão de sensores e dispositivos inteligentes, bem como tecnologias de colaboração social, os dados tornaram-se

complexos, porque inclui não apenas a relação tradicional de dados, mas também dados brutos, semiestruturados e não estruturados de web páginas, arquivos de registro da web (incluindo dados de fluxo de cliques), índices de pesquisa, mídias sociais, fóruns, e-mails, documentos, dados de sensores de sistemas ativos e passivos, e até wearables.

Bancos de dados tradicionais podem ter problemas para lidar com tais tipos de informações, uma vez que estes conseguem manipular apenas dados estruturados, com pouca variância e segundos os autores, mais de 80% dos dados do mundo são não estruturados ou semi-estruturados na melhor das hipóteses. Além do volume e sua variedade de dados coletados e armazenados terem aumentado, a velocidade na qual estes dados são gerados e manipulados também aumentou. A quantidade de dispositivos gerando dados levou a um fluxo constante de dados em um ritmo que tornou impossível o manuseio dos sistemas tradicionais.

Zikopoulos e Eaton (2011) afirmam que a ideia da velocidade em big data vai além dos conceitos tradicionais. Para acomodar a velocidade, uma nova maneira de pensar sobre um problema deve começar no ponto de início dos dados. Em vez de limitar a ideia de velocidade às taxas de crescimento associadas aos seus repositórios de dados, eles sugerem aplicar essa definição aos dados em movimento: a velocidade na qual os dados fluem e são processados. Toda esta quantidade de dados gera um novo conceito: Data Mining (mineração de dados).

Han, Kamber e Pei (2012) definem Data Mining, como sendo o conhecimento adquirido por meio de dados. Segundos os autores, data mining pode ser vista como a evolução natural da tecnologia da informação. O processo adquire grandes massas de dados, dos quais não se tem muito valor no momento, e o transforma em informação de valor. Este processo de mineração de dados é de suma importância para a análise preditiva e outros tipos de análise existentes em big data. Para realizar a mineração dos dados é preciso passar por um processo: Primeiro é realizado o data cleaning (limpeza dos dados) em que se remove os ruídos e dados inconsistentes. Após esta limpeza, realiza-se o data integration (integração de dados), onde muitas fontes de dados são combinadas.

Depois é realizado o data selection (seleção de dados), em que são selecionados apenas os dados possivelmente relevantes para serem tratados. Já com os dados selecionados, é realizado o data transformation (transformação de dados), onde os dados são transformados e consolidados em um formato apropriado para a mineração, executando uma operação de resumo ou agregação. Finalmente com os dados já tratados, é realizado o data mining, utilizando métodos inteligentes para extrair padrões de dados. Lobo (2017) afirma que big data está sendo gradualmente introduzido no sistema de atenção à saúde. Dados de prevalência, incidência e evolução de enfermidades permitiriam gerar dados estatísticos, antecipar surtos epidemiológicos e prescrever ações preventivas. Dados de pacientes, como idade, sexo, etnia, local de residência, antecedentes pessoais e familiares, sintomas e sinais apresentados, exames realizados ou obtidos por meios eletrônicos (wearable devices), diagnósticos feitos, tratamento e evolução coletados, permitiriam estabelecer uma base de dados e aprimorar condutas estabelecidas.

Taurion (2013) explica que os médicos poderão trabalhar com informações dos hábitos dos pacientes fora dos hospitais, no seu dia a dia. O conceito do uso de informações muda de análise de fatos ocorridos para análise preditiva, permitindo tomar decisões e ações muito mais eficazes. Hekima (2015) define análise preditiva como uma análise das possibilidades futuras. A partir da identificação de padrões passados em sua base dados, esse tipo de análise permite o mapeamento de possíveis futuros em seus campos de atuação. Conhecida por “prever” o futuro, a análise preditiva usa mineração de dados, dados

estatísticos e dados históricos para conhecer as futuras tendências. Hekima (2015) ainda descreve outros três tipos de análise que podem ser úteis. A análise prescritiva, análise descritiva e análise diagnostica. A análise prescritiva trabalha com uma lógica similar á análise preditiva, porém possui outros objetivos. A análise prescritiva tenta traçar as possíveis consequências de cada ação. A partir dela é possível definir qual escolha será mais efetiva para cada tipo de situação. Na área da saúde por exemplo, é possível traçar padrões de determinados pacientes e doenças e analisar possíveis impactos de ações sobre esse grupo, analisando qual a melhor opção de gestão para eles. Já a análise descritiva, busca a compreensão em tempo real de acontecimentos, esta é uma maneira de visualizar os dados, entender como uma database se organiza e o que significa para o presente sem necessariamente relacioná-la com padrões passados ou futuros. Por último tem-se a análise diagnóstica. Este tipo de análise tem como objetivo compreender de maneira causal todas as possibilidades. Como uma espécie de relatório expandido, quando feita em uma base de dados volumosa, esse tipo de análise permite ainda entender a razão de cada um dos desdobramentos das ações adotadas e, a partir disso, mudar estratégias ineficazes ou reforçar as funcionais. Unindo inteligência artificial com big data, é criada uma ferramenta poderosa para o auxílio na medicina e em várias outras áreas.

4. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO DIAGNÓSTICO MÉDICO

A medicina moderna é confrontada com o desafio de adquirir, analisar e aplicar a grande quantidade de conhecimento necessário para resolver problemas clínicos complexos. Tem-se observado na medicina o crescimento acelerado da necessidade de diagnósticos cada vez mais rápidos e mais precisos (NOGUEIRA et al., 2022). Todo ser humano comete erros, porém na medicina erros podem ser fatais e tirar vidas, então é necessário minimizar este cenário. Segundo Lobo (2017), em 2009, verificou-se que 32% dos erros médicos nos EUA resultavam da diminuição do tempo de interação do médico com os pacientes, produzindo diagnósticos equivocados, não conhecimento da urgência ou piora da evolução do paciente que demandariam prescrever ou realizar ações pertinentes.

Mesmo em hospitais que disponham de prontuários médicos eletrônicos, com a possibilidade de melhor coleta de dados, admite-se que 78,9% dos erros médicos estariam relacionados a problemas na relação médico-paciente, exame clínico deficiente, falha de avaliação dos dados do paciente ou falta de exames que comprovassem a hipótese diagnóstica (DAVENPORT, 2019). Também é caracterizado outro problema: apesar da grande capacitação do especialista, é extremamente difícil assimilar todas as informações dos sintomas, causas, histórico do paciente e cenários possíveis. Estes detalhes muitas vezes passados despercebidos, porém, ser cruciais para o diagnóstico do paciente.

Nogueira et al. (2022) visto o poder que a inteligência artificial tem em analisar grandes quantidades de dados, reconhecer padrões, capacidade de responder a novos ambientes e parâmetros, a IA estar sendo usada para tentar prevenir estes casos. Desde os anos 50 a IA foi se desenvolvendo e com esta expansão tornou-se possível desenvolver sistemas baseados no conhecimento de áreas específicas, denominados Sistemas Especialistas (SE), cujo objetivo é fornecer auxílio à tomada de decisão médica, diminuindo os riscos na realização dos diagnósticos. Grande parte dos sistemas especialistas tem estrutura fundamentada na tecnologia de Redes Neurais Artificiais (RNA), devido à sua característica única de imitar o funcionamento do cérebro humano, reproduzindo artificialmente neurônios que recebem e enviam sinais, agregando aprendizado ao sistema (NOGUEIRA et al., 2022).

Mendes (1997) afirma que a área médica, desde o início das pesquisas, tem sido uma

das áreas mais beneficiadas pelos sistemas especialistas, por ser considerada detentora de problemas clássicos possuidores de todas as peculiaridades necessárias, para serem instrumentalizados por tais sistemas. Segundo ele, Sistemas Especialistas (SE) são sistemas baseados em conhecimento, construídos, principalmente, com regras que reproduzem o conhecimento do perito, são utilizados para solucionar determinados problemas em domínios específicos. Nogueira et al. (2022) acrescenta que os SE utilizam informações não numéricas com o objetivo de auxiliar na resolução de problemas que não possuem regras ou processos claramente definidos, ou cuja solução exige excessivo tempo de processamento.

A saúde digitalizada apresenta inúmeras oportunidades para reduzir erros humanos, melhorar os resultados clínicos, rastrear dados ao longo do tempo etc. Os métodos de IA, do aprendizado de máquina ao aprendizado profundo, assumem uma função crucial em vários domínios relacionados ao bem-estar, incluindo a melhoria de novos sistemas clínicos, informações e registros de pacientes e tratamento de várias doenças (DIGNUM, 2018). As técnicas de IA também são mais eficientes na identificação do diagnóstico de diferentes tipos de doenças. A presença do raciocínio computadorizado (IA) como método para melhorar os serviços médicos oferece oportunidades inéditas para recuperar resultados de pacientes e grupos clínicos, diminuir custos. A IA também pode ajudar a reconhecer as áreas demográficas ou ambientais precisas onde existe a frequência de doenças ou comportamentos de alto risco. Os pesquisadores usaram efetivamente as classificações de aprendizado profundo em abordagens diagnósticas (KAPLAN; HAENLEIN, 2019).

Os algoritmos de IA devem ser treinados em informações representativas da população para atingir níveis de apresentação essenciais para “realização” adaptável. Tendências, como a cobrança de guardar e direcionar realidades, coleta de informações por meio de registros eletrônicos de bem-estar e estado exponencial das informações do cliente, tornaram um sistema biológico de assistência médica rico em dados. Essa ampliação dos dados de saúde luta com a falta de mecanismos bem-organizados para integrar e reconciliar esses dados. Várias técnicas baseadas em IA, como modelos de máquina e aprendizado profundo, podem ser usadas para detectar doenças na pele, fígado, coração, Alzheimer etc. que precisam ser diagnosticadas precocemente (KAPLAN; HAENLEIN, 2019).

A inteligência artificial (IA) tornou-se sinônimo de suporte e eficiência na comunidade médica. A partir de uma tecnologia vista com suspeita, pois as alegações apontavam como a substituta do profissional médico, a IA evoluiu para se tornar o segundo par de olhos que nunca precisa dormir. A inteligência artificial em diagnóstico médico e assistência médica fornece suporte confiável aos médicos e instalações sobrecarregados, ajudando a minimizar a pressão da carga de trabalho e maximizando a eficiência do profissional (KRAUSOVÁ, 2017).

A inteligência artificial no diagnóstico médico ajuda na tomada de decisões médicas, gerenciamento, automação, administração e fluxos de trabalho. Ela pode ser usada para diagnosticar câncer, fazer a triagem de achados críticos em imagens médicas, sinalizar anormalidades agudas, fornecer ajuda aos radiologistas na priorização de casos de risco de vida, diagnosticar arritmias cardíacas, prever resultados de AVC e ajudar no manejo de doenças crônicas (MA et al., 2017). A IA é um domínio rico de dados, algoritmos, análises, aprendizado profundo, redes neurais e insights que estão em constante crescimento e se adaptando às necessidades do setor de saúde e de seus pacientes. Nos últimos anos, a inteligência artificial no diagnóstico médico mostrou-se imensamente promissora em mudar os padrões de atendimento médico, reduzindo as pressões extremas sentidas pela indústria médica.

O esgotamento médico é um problema muito real. A exaustão e o excesso de traba-

lho sentido por muitos profissionais médicos estão impactando em seu desempenho. Os médicos estão deixando seus empregos, lutando para oferecer atendimento de qualidade ao paciente e fazendo malabarismos com desafios emocionais complexos. Isso é em grande parte causado por longas horas, cargas de trabalho esmagadoras e falta de suporte. Os médicos tomam decisões complexas e que mudam a vida, diariamente, e muitas vezes não têm espaço nem tempo para gerenciar suas cargas de trabalho de forma eficaz. No recente relatório Medscape National Physician Burnout and Suicide Report (2020), as estatísticas apontaram para os riscos inerentes à pressão excessiva sobre os profissionais, especialmente aqueles que tentam conciliar famílias, planejamento de aposentadoria e as complexidades de seus trabalhos (NOGUEIRA et al., 2022).

No relatório, 42% dos médicos revelaram que estão esgotados. As especialidades mais afetadas são medicina de emergência, cuidados intensivos, medicina de família, neurologia, urologia e medicina interna. A causa principal? A carga administrativa. É aqui que a IA pode desempenhar um papel fundamental. Projetada com intenção, a inteligência artificial no diagnóstico médico pode não apenas reduzir a pressão sobre os médicos ao trabalhar com grandes quantidades de informações e imagens, mas também pode ser usada para realizar uma grande porcentagem da carga administrativa. As soluções certas, desenvolvidas especificamente para o setor de saúde, podem ser usadas para fornecer aos médicos um suporte essencial à medida que gerenciam volumes crescentes de dados, informações e volumes de imagens. A IA pode fornecer suporte tangível a médicos sobrecarregados com sistemas projetados para minimizar o estresse e aumentar o tempo gasto com os pacientes (NOGUEIRA et al., 2022).

Portanto, a inteligência artificial no diagnóstico médico é uma ferramenta poderosa para reduzir o desgaste do médico, mas também para fornecer ao profissional um suporte excepcional no gerenciamento de cargas de trabalho que estão aumentando. Os profissionais precisam lidar com volumes de imagens múltiplos e crescentes, e espera-se que o façam em velocidades nunca antes vistas. Hoje, eles precisam filtrar volumes de imagens enquanto ainda priorizam aquelas que são urgentes e gerenciam o atendimento ao paciente. É aqui que a inteligência artificial no diagnóstico médico realmente brilha (KAPLAN; HAENLEIN, 2019). As soluções de IA e aprendizado profundo têm fornecido suporte essencial à medida que gerenciam esses grandes volumes de imagens, oferecendo a capacidade de otimizar fluxos de trabalho, economizar tempo, aumentar a capacidade e aumentar a confiabilidade do diagnóstico. Isso reduz significativamente a pressão profissional. A inteligência artificial no diagnóstico médico ainda está no limite de seu potencial. Há muito espaço para crescimento e para a tecnologia melhorar o que pode fazer para apoiar a profissão médica. A IA, como está hoje, já está sendo integrada à prática e aos fluxos de trabalho e, à medida que continua a evoluir, mudar e se adaptar, provavelmente aumentará para fornecer à profissão médica um conjunto confiável de ferramentas que podem ajudar no diagnóstico, fluxo de trabalho, administração e carga de trabalho.

5. CONCLUSÃO

A inteligência artificial (IA) em várias formas e graus tem sido usada para desenvolver e avançar em um amplo espectro de campos, como bancos e mercados financeiros, educação, cadeias de suprimentos, manufatura, varejo e comércio eletrônico e saúde. Dentro da indústria de tecnologia, a IA tem sido um facilitador importante para muitas inovações de negócios. Isso inclui pesquisa na web (por exemplo, Google), recomendações de conteúdo (por exemplo, Netflix), recomendações de produtos (por exemplo, Amazon), publicidade direcionada (por exemplo, Facebook) e veículos autônomos (por exemplo, Tesla).

Os seres humanos colhem os benefícios de sistemas artificialmente inteligentes todos os dias. Desde os e-mails até relógios inteligentes que usam entradas de sensores de acelerômetro para distinguir entre atividades mundanas e atividades aeróbicas. Esses exemplos representam o uso da IA em diversos campos, como tecnologia e varejo. A IA transformou a vida cotidiana, afetando a maneira como percebemos e processamos informações. Neste contexto, grandes avanços foram feitos no uso de sistemas artificialmente inteligentes em caso de diagnóstico do paciente. Por exemplo, no campo das especialidades visualmente orientadas, como a dermatologia, dados de imagens clínicas podem ser usados para desenvolver modelos de classificação para auxiliar os médicos no diagnóstico de câncer de pele.

Grandes avanços foram feitos na aplicação de sistemas de IA para a descoberta de medicamentos e no fornecimento de opções de tratamento personalizadas. Sistemas artificialmente inteligentes também estão sendo aplicados no setor de saúde para aprimorar a experiência do paciente. A aplicação mais recente da IA na área da saúde global é a previsão de pontos de acesso emergentes usando rastreamento de contato e dados de viajantes de voos para combater a nova pandemia de coronavírus (COVID-19).

O uso da IA em qualquer campo de estudo consiste em muitos componentes e a programação é apenas um deles. Para o crescimento, desenvolvimento e sucesso contínuos de aplicativos de IA na área da saúde, médicos e cientistas de dados precisam continuar colaborando para criar sistemas de IA significativos. Os médicos precisam entender o que a IA é capaz de alcançar e precisam avaliar como seu papel pode ser melhorado com a IA. Os médicos precisam comunicar essas informações aos cientistas de dados que podem construir um sistema de IA. A colaboração não termina aqui. Juntos, médicos e cientistas de dados devem descobrir que tipo de dados eles têm disponível para usar no treinamento do modelo e, além disso, uma vez que o modelo é construído, seu desempenho deve ser analisado e interpretado, o que requer colaboração entre médicos e cientistas de dados.

A IA parece bem-posicionada para revolucionar o setor de saúde. Os sistemas de IA podem ajudar a liberar o tempo de médicos ocupados, transcrevendo anotações, inserindo e organizando dados de pacientes em portais e diagnosticando pacientes, servindo potencialmente como um meio de fornecer uma segunda opinião aos médicos. Sistemas artificialmente inteligentes também podem ajudar os pacientes com cuidados de acompanhamento e disponibilidade de alternativas de medicamentos prescritos. A IA também tem a capacidade de diagnosticar pacientes remotamente, estendendo assim os serviços médicos para áreas remotas, além dos grandes centros urbanos do mundo. O futuro da IA na área da saúde é brilhante e promissor, mas ainda há muito a ser feito. Como sugestão de trabalhos futuros, pretende-se fazer um aprofundamento das técnicas de IA abordadas e a investigação de outras técnicas abrangendo todas as áreas da inteligência artificial, para que com o conhecimento adquirido com a pesquisa possa ser feita a implementação das técnicas em uma possível aplicação desenvolvida posteriormente.

Referências

AMATO, Filippo et al. Artificial neural networks in medical diagnosis. **Journal of Applied Biomedicine**, [S.l.], p. 47-57, jan. 2013.

ANDRADE, P.J.N. Sistemas Especialistas de Apoio ao Diagnóstico em Medicina: relações com o teorema de Bayes e com a lógica do raciocínio diagnóstico, **Arq Bras Cardiol**.v. 73, n. 6, p. 537-544, 1999.

BROOKS, Rodney; TEGMARK, Max.**Discovery Brasil | Inteligência Artificial**. IBM.2018.

CHEN, Ying; ARGENTINIS, Elenee; WEBER, Griff. IBM Watson: How Cognitive Computing Can Be Applied to

Big Data Challenges in Life Sciences Research. **Clinical Therapeutics**, New York, p. 688-701, mar. 2016.

DAVENPORT, Thomas et al. How artificial intelligence will change the future of marketing. **Journal of the Academy of Marketing Science**, p. 1-19, 2019.

DIGNUM, Virginia. **Ethics in artificial intelligence: introduction to the special issue**, 2018.

HAN, Jiaway; KAMBER, Micheline; PEI, Jian. Data Mining: Concepts and techniques: **Elsevier**, 2012. 673 p. v. 3.

HAYKIN, Simon. **Redes Neurais**: Princípios e prática. 2. ed. Ontário: Bookman, 2008. 908 p.

KAPLAN, Andreas; HAENLEIN, Michael. **Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence**. Business Horizons, v. 62, n. 1, p. 15-25, 2019.

KRAUSOVÁ, Alžběta. Intersections between law and artificial intelligence. **InternationalJournalof Computer**, v. 27, n. 1, p. 55-68, 2017.

LOBO, Luiz Carlos. Inteligência Artificial e Medicina. **Rev. bras. educ. med**., Rio de Janeiro, v. 41, n. 2, p. 185-193, jun. 2017.

LUGER, George F. **Inteligência Artificial**. 6. ed: Pearson, 2013. 614 p.

MEDEIROS, Luciano Frontino. **Inteligência Artificial Aplicada**: Uma abordagem introdutória: Intersaberes, 2018. 263 p.

MENDES, Raquel Dias. **Inteligência Artificial**: Sistemas Especialistas no Gerenciamento da Informação. Ci. Inf., Brasília, v. 26, n. 1, p., Jan. 1997.

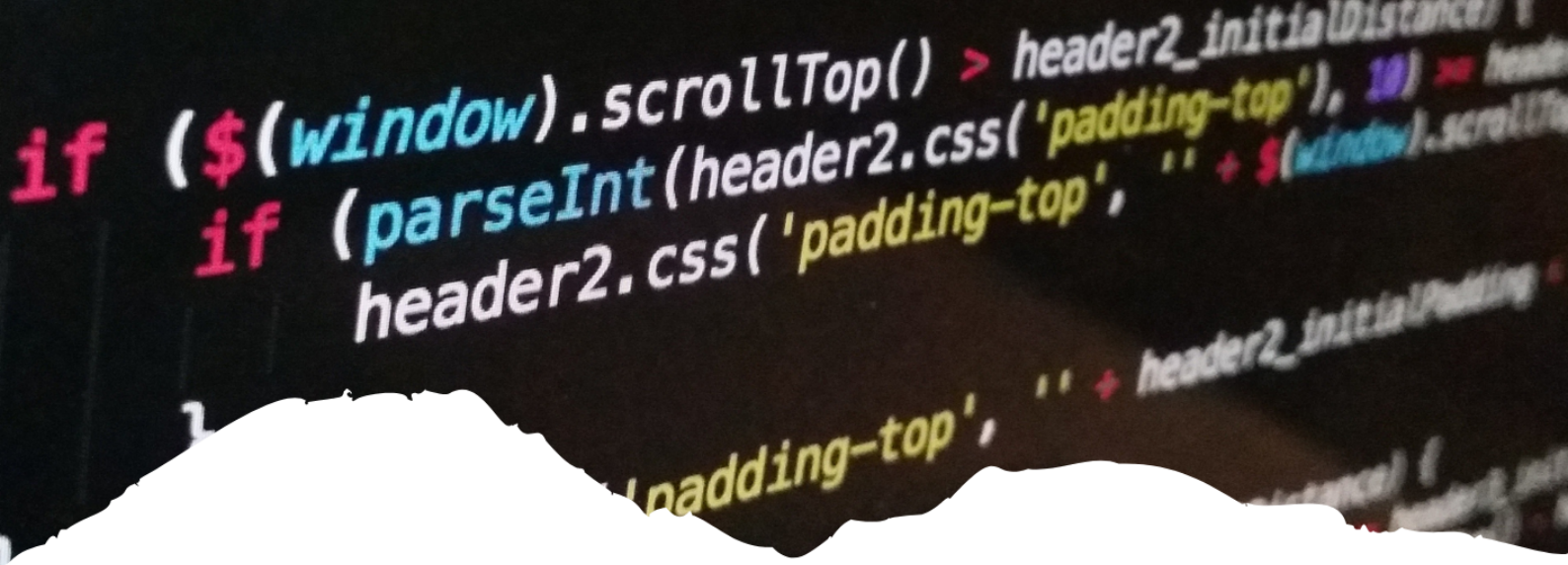
MOEIN, Sara. **Medical Diagnosis Using Artificial Neural Networks**. TEXAS: KOBO EDITIONS, 2014. 309 p.

NOGUEIRA, Israel et al. Impactos da implementação da Inteligência Artificial na tomada de decisão médica. **Revista Gestão & Saúde**. p. 146- 158, jan. 2022.

OTHMAN, Abu Talib. **Neural Network In Medical Application**: A Review. 2001. 8 f. Artigo (Mestrado)- Universiti Utara, 2001.

TAURION, Cezar. BIG DATA. **Rio de Janeiro**: Brasport, 2013. 110 p.

ZIKOPOULOS, Paul; EATON, Chris. **Understanding Big Data**: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media, 2011. 166 p.



4

O USO DA INTELIGÊNCIA ARTIFICIAL NO COTIDIANO DAS PESSOAS

THE USE OF ARTIFICIAL INTELLIGENCE IN PEOPLE'S DAILY LIFE

Jhonatan de Jesus Anuncio de Oliveira

Bruno Roberto

Resumo

A evolução tecnológica mudou a vida das pessoas em diversas instâncias, e também provocou grandes transformações nas organizações e no mundo do trabalho. Neste contexto, tarefas consideradas manuais e repetitivas começam a ser executadas por sistemas automatizados. O desemprego era recorrente, mas não definitivo, o que nos leva a acreditar que o mesmo ocorrerá futuramente: um remanejamento de pessoas que eram empregadas em funções que se tornaram desnecessárias a humanos e que agora são melhor executadas por máquinas, abrindo novas oportunidades de atuação no mercado de trabalho. Sendo assim, o objetivo deste trabalho é mostrar a Inteligência artificial no cotidiano das pessoas, em seus trabalhos e também para uso pessoal. A IA é usada atualmente em várias áreas, como reconhecimento facial, na televisão smart, quando acessar sistemas de busca, GPS, em Marketing etc. A inteligência artificial (IA) no cotidiano das pessoas tem se tornado cada vez mais presente, seja em serviços financeiros, atendimento ao cliente, indústria, saúde, educação, mobilidade urbana e entretenimento. A IA traz benefícios como eficiência, produtividade, redução de custos e melhorias na qualidade de vida. Porém, também existem desafios e riscos associados, como questões éticas e de privacidade, preocupações com a segurança e riscos de exclusão social. É necessário regulamentar a IA e desenvolver soluções para minimizar os riscos e maximizar os benefícios dessa tecnologia. Está tecnologia nos permitindo progredir mais rápido e automatizar nossas tarefas.

Palavras-chave: Tecnologia. Automação. Inteligência Artificial. Trabalho, Aprendizado de máquina.

Abstract

Technological evolution has changed people's lives in several instances, and has also caused major transformations in organizations and in the world of work. In this context, tasks considered manual and repetitive begin to be performed by automated systems. Unemployment was recurrent, but not definitive, which leads us to believe that the same will occur in the future: a reallocation of people who were employed in functions that became unnecessary for humans and that are now better performed by machines, opening up new opportunities for action in the business market. Therefore, the objective of this work is to show Artificial Intelligence in people's daily lives, in their work and also for personal use. AI is currently used in many areas such as facial recognition, in smart television, when accessing search engines, GPS, in Marketing, etc. Artificial intelligence (AI) in people's daily lives has become increasingly present, whether in financial services, customer service, industry, health, education, urban mobility and entertainment. AI brings benefits such as efficiency, productivity, cost reduction and improvements in quality of life. However, there are also associated challenges and risks, such as ethical and privacy issues, security concerns and risks of social exclusion. There is a need to regulate AI and develop solutions to minimize the risks and maximize the benefits of this technology. This technology allows us to progress faster and automate our tasks.

Keywords: Technology. Automation. Artificial intelligence. Work, Machine Learning.

1. INTRODUÇÃO

A Inteligência Artificial (IA) tem se tornado cada vez mais presente no cotidiano das pessoas, transformando a maneira como elas trabalham, se divertem e interagem com o mundo ao seu redor. Desde assistentes virtuais até algoritmos de recomendação, a IA estar mudando a forma como consumimos conteúdo, tomamos decisões e resolvemos problemas.

O uso da inteligência artificial, tem como definição um conjunto de tecnologia que permite que as máquinas realizem tarefas ao aprender e raciocinar de modo semelhante a mente humana. Muitas empresas adotam o uso desta tecnologia para otimizar os processos. Um exemplo disso é a automação predial, que garante a eficiência para abrir portões de modo automática, acender e apagar luzes, entre outros fatores que envolvem a otimização e processo sem a necessidade de intervenção humana.

Hoje em dia, a IA estar cada vez mais presente na rotina da população, desde ao uso pessoal, como nos reconhecimentos faciais nos dispositivos móveis e em processos profissionais, como nos serviços de manutenção de elevadores residenciais. A IA pode ocasionar preocupação para muitas pessoas em relação as oportunidades de empregos. Outra questão importante a ser considerada é a forma como a IA pode mudar as interações entre as pessoas e as máquinas. Com a automatização de processos e a criação de sistemas inteligentes, é possível que as pessoas se tornem cada vez mais dependentes da tecnologia e percam a habilidade de realizar tarefas simples sem a ajuda de sistemas automatizados.

Com toda essa tecnologia, trabalhos manuais e rotineiros já estão sendo automatizados por muitas organizações e postos de trabalho ocupados por humanos convertendo-se em máquinas inteligentes. A IA tem se mostrado uma tecnologia cada vez mais versátil, capaz de ser aplicada em diversos setores e atividades cotidianas. Na saúde, por exemplo, a IA é usada para análise de dados médicos e diagnósticos mais precisos. Na educação, ela é utilizada para personalização do ensino, adaptação do conteúdo ao ritmo de aprendizagem do aluno e análise do desempenho. Na mobilidade urbana, a IA é aplicada em sistemas de transporte autônomo, monitoramento do tráfego e planejamento de rotas. Acontece que inovações baseadas em IA já fazem parte das nossas rotinas e, sendo cada vez mais evidentes, as especulações de que seremos substituídos aumentam consideravelmente.

A Inteligência Artificial substituirá o ser humano ou criará áreas de trabalho? Neste contexto, Wolkan (2018) explica que o impacto pode ser grande, pois muitos empregos serão eliminados; mas será preciso preparar as pessoas para que executem atividades que ainda não existem, pois novas ocupações e cargos serão criados através de inovações significativas neste ambiente tecnológico.

2. DESENVOLVIMENTO

2.1 Fundamentação teórica

No contexto atual em que a sociedade se encontra onde para quase tudo se necessita da tecnologia, e as relações humanas estão concentradas cada vez mais no meio virtual do que no presencial, é importante conhecer e entender como se deu o surgimento dessas novas tecnologia, principalmente a inteligência artificial.

Para Silva e Mairink (2019), “a Inteligência artificial é a possibilidade de uma máquina

através de algoritmos programados, possui a capacidade cognitiva semelhante à do ser humano". Desta forma, atividades que eram realizadas apenas por humanos começam a ser executadas por máquinas e computadores. Damaceno e Vasconceles (2018), complementam a definição de inteligência artificial, afirmando que a tecnologia é preparação de máquinas com a capacidade de aprender sendo programadas previamente, proporcionando tomada de decisões, especulações e interações baseadas nos dados fornecidos a elas. E ressaltando que a inteligência artificial não necessariamente precisa simular interações e comportamentos humanos, mas sim executar ações de forma inteligente.

Segundo Quaresma (2018), desde o fim da Segunda Guerra Mundial (1945), existem estudos sobre a inteligência Artificial. Pois desde essa época pesquisadores acreditavam ser possível replicar em máquinas e consciência humana. No entanto, após longos anos de estudos observam-se limitações na aplicação desta prática, como por exemplo, falta de um técnico especialista capaz de transformar conhecimento e comportamento humano em linguagem computacional. E que este computador fosse capaz de "aprender" de forma autônoma e continua sem a intervenção de um humano.

Mesmo assim com essas limitações os estudos continuaram e em 1950, Alan Turing, considerado o pai da computação realizou um teste que consistia em colocar um humano e uma máquina para responder perguntas e uma terceira pessoa teria que identificar sem visualizar e apenas lendo as repostas, quem seria a máquina e quem seria o humano. Tal proposto foi fundamental para o desenvolvimento da ciência cognitiva e para o prosseguimento dos estudos relacionadas à inteligência artificial (ZILIO, 2019).

Hoje, cerca de 70 anos depois, estamos em um cenário de pesquisa mais solido, quando de se trata da inteligência artificial. Embora ainda se tenha muito que explorar, a inteligência artificial é considerada capaz de replica algumas habilidades que apenas um humano era capaz (SILVA; MAIRINK, 2019).

É importante destacar devido à crescente expansão dos estudos relacionados à Inteligência Artificial, aumentou-se também sua utilização em diversas áreas realizando o surgimento de novos negócios e aprimorando os já existentes. Sendo assim, se faz necessário entender as principais utilidades dessas tecnologias.

Segundo Silva e Mairink (2019), o fato de ser possível utilizar a inteligência artificial em diversas áreas, facilita a produção e otimiza o tempo gasto na realização de atividades a ser executadas. Além disso, o uso da inteligência artificial traz solução para um dos maiores problemas da sociedade e é a falta de tempo. Os autores também apresentam desvantagem em relação ao uso dessa tecnologia, pois visto que a mesma ainda é recente e continua sendo estudada, as máquinas que utilizam a inteligência artificial são programadas com conceitos humanos e não evoluem com o tempo, a não ser que uma pessoa programe a mesma máquina novamente e com novas informações. E caso a máquina não seja adaptada para realidade da população pode gerar conflitos na sociedade.

Como relatado por Néri (2005), enquanto ainda existem tarefas que necessitam de automação, de natureza distribuída, que exigem comunicação entre partes e que possui diversas especializações, o uso de agentes inteligentes é uma boa solução para estas atividades. A delegação de tarefas como essas podem ter impactos surpreendentes na sociedade, que até a forma com que as pessoas decidem, negociam e pesquisam é modificada e as empresas podem aproveitar disso para ampliar o seu poder de negociação com os fornecedores.

São vários exemplos de aplicações da inteligência artificial, tais como veículos autônomos, diagnóstico médico, desenvolvimento da arte, teoremas matemáticos, jogos, motores de busca, assistente online, reconhecimento de imagem, filtragem de spam, decisões judiciais e marketing online (NOVAIS; FREITAS,2018).

Para Monard e Baranauskas (2000) a inteligência artificial é um ramo da ciência da computação, mas também aplicada a área como, psicologia, linguística, biologia, logica, matemática, engenharia, filosofia, entre outras áreas.

Conforme Vasconcelos e Damasceno (2018), um exemplo de *Machine Learning* é a identificação de spams, sendo que inicialmente são fornecidos e-mail rotulados como spam e a partir disso o software anti-spam detecta nos próximos e-mails padrões para rotulá-los como spam ou não. Para Gomes (2010), a *Natural Language Processing* pode ser utilizada para recuperar informações sem digitar comandos ou palavras chaves. Por fim, um exemplo de *Deep Learning* é o reconhecimento de imagens do Google Fotos, que possui uma ferramenta que seleciona as melhores fotos, e também consegue reconhecer, pessoas, animais e objetos com características em comum (GRACIOSO et al., 2018).

Schwab (2016) faz um alerta para o risco do desemprego em massa, pois com o crescimento de tarefas sendo executadas por uma Inteligência Artificial, os seres humanos podem demorar para se adaptar em um novo emprego gerando uma escala massiva de desempregos. Para Gil, Rodrigues e Dutra (2018) complementam que o uso desta tecnologia deve ser orientado pela ética organizacional de forma a abrangem diferentes costumes, crenças e valores que compõem a diversidade humana.

É necessário, portanto, entender, as vantagens e desvantagens do uso da inteligência artificial para que diante deste contexto as organizações junto ao governo criem estratégias para capacitação de pessoas e realocação no mercado de trabalho.

A rápida evolução da IA e o aumento da capacidade computacional têm possibilitado avanços significativos em áreas como reconhecimento de fala, processamento de linguagem natural, visão computacional e aprendizado de máquina. Esses avanços têm resultado em uma série de inovações tecnológicas que têm transformado a forma como interagimos com a tecnologia e como vivemos nossas vidas.

Outra área em que a IA tem desempenhado um papel fundamental é na automação de processos, tanto no contexto doméstico quanto no ambiente de trabalho. Robôs e sistemas automatizados, impulsionados pela IA, estão sendo utilizados em tarefas como limpeza doméstica, atendimento ao cliente, diagnóstico médico, manufatura e logística, proporcionando eficiência e produtividade.

Espera-se que esta pesquisa contribua para um maior entendimento do impacto da inteligência artificial no cotidiano das pessoas, fornecendo insights para a sociedade, empresas e governos sobre como lidar com os desafios e aproveitar os benefícios dessa tecnologia de forma responsável.

2.2 Metodologia

Considerando que o objetivo deste trabalho é identificar os estudos disponíveis sobre o uso da Inteligência Artificial no cotidiano das pessoas, por meio de pesquisa em sites.

O presente trabalho foi realizado por meio de uma pesquisa bibliográfica, o qual segundo Prodanov e Freitas (2013), é elaborada a partir de material já publicado, constituído principalmente de livros, revistas, publicações em periódicos, artigos científicos, internet, dissertações, teses etc. Com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa.

Sendo assim, a pesquisa realizada pautou-se na leitura e no fechamento de escritas de diferentes autores afetos à área da história da inteligência artificial, e os benefícios tra-

zidos com a evolução das máquinas, bem como o impacto social causado pela automatização das tarefas.

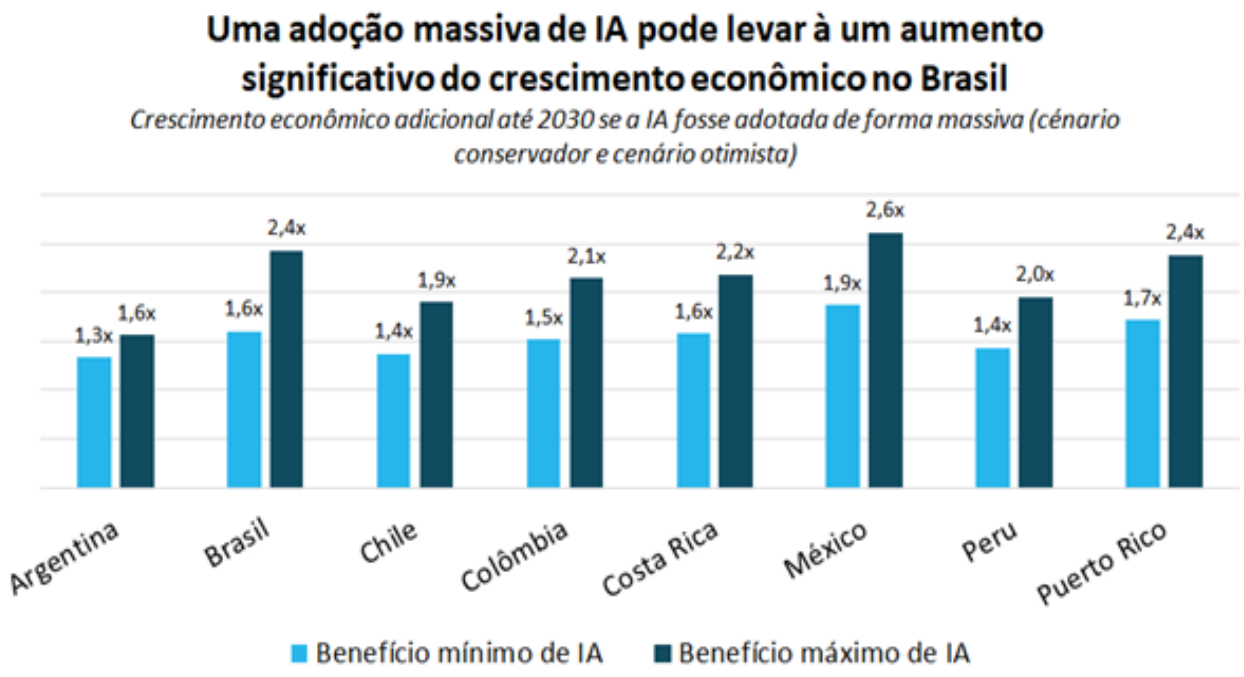
No planejamento da pesquisa ficou definido que ela será realizada no portal de Periódicos CAPES (http://www.periodicos.capes.gov.br/) por possuir trabalhos acadêmicos e científicos que abrangem todas as áreas de conhecimento, e outro portal utilizado foi o Google Scholar ele abrange várias áreas do conhecimento e é uma referência importante para pesquisadores, incluindo artigos revisados por pares, teses, dissertações, livros, resumos e relatórios técnicos. Ele é projetado especificamente para ajudar os usuários a encontrar informações acadêmicas relevantes em várias disciplinas. Foi utilizada as buscas por palavras chaves por título e combinadas: inteligência artificial, IA no trabalho e Inteligência Artificial no cotidiano a fim de obter maior quantidade de artigos relacionados à temática deste trabalho.

Para delimitar o período de análise dos artigos, foram identificados o mais antigo (2013) e o mais recente (2020) sobre o tema. Optando assim, por selecionar artigos publicados entre 2007 e 2021 para análise, abrangendo assim um intervalo adequado de estudos relevantes ao tema. Isso permitiu obter uma compreensão abrangente e atualizada das informações pertinentes ao estudo. As palavras-chaves utilizadas na busca sobre o tema, foram “inteligência artificial”, “ IA no trabalho”, “impacto da IA”, “aplicações da IA”, “ Inteligência Artificial no cotidiano”, entre outras combinações.

2.3 Resultados e Discussão

Vários estudos mostram que o uso da inteligência artificial no cotidiano das pessoas já é uma realidade em muitas áreas, incluindo saúde, finanças, transporte, varejo e entretenimento. De acordo com um relatório da PwC, a inteligência artificial pode impulsionar a economia global em até US $ 15,7 trilhões até 2030 (PwC, 2018).

Gráfico 1 – Crescimento econômico no Brasil



Fonte: Microsoft (2020)

A implementação massiva da inteligência artificial (IA) no setor de tecnologia no Bra-

sil, conforme demonstrado no Gráfico 1, traz resultados concretos. Isso inclui a geração de novas oportunidades de emprego, o aumento dos investimentos em pesquisa e desenvolvimento, e uma maior competitividade no mercado global. A IA possibilita a automação de processos, análise avançada de dados e aprendizado de máquina, resultando em maior eficiência, inovação e qualidade dos produtos e serviços tecnológicos brasileiros. Essa ampla adoção da IA coloca o Brasil como um protagonista no cenário tecnológico, impulsionando o crescimento econômico e fortalecendo o setor no país. O uso de IA também pode ajudar o Brasil a alcançar seus objetivos de desenvolvimento sustentável, melhorando a eficiência e a sustentabilidade em diversos setores da economia.

Além disso, a mesma pesquisa prevê que a adoção da inteligência artificial pode aumentar a eficiência do trabalho em até 40%, reduzir os custos operacionais em até 30% e aumentar a satisfação do cliente em até 50%. Outro estudo conduzido pela Accenture (2019) mostra que a adoção da inteligência artificial pode ajudar a reduzir o tempo de resposta do atendimento ao cliente em até 90% e aumentar a precisão do diagnóstico médico em até 50%.

No entanto, a implementação da inteligência artificial também apresenta riscos e desafios significativos. Um estudo realizado pelo Institute for Public Policy Research destaca a preocupação de que a inteligência artificial possa aumentar a desigualdade social, já que as pessoas de baixa renda e com pouca educação terão menos acesso aos benefícios da tecnologia (IPPR, 2018). Além disso, o mesmo estudo argumenta que a inteligência artificial pode levar à discriminação algorítmica e reforçar estereótipos e preconceitos existentes na sociedade.

Existem muitos artigos que abordam o tema do uso da inteligência artificial no cotidiano das pessoas, e a maioria deles apresenta argumentos tanto a favor quanto contra essa tecnologia.

Por um lado, os defensores da inteligência artificial argumentam que ela tem o potencial de tornar nossas vidas mais eficientes, convenientes e seguras. A tecnologia pode ajudar a automatizar tarefas repetitivas e mundanas, permitindo que os seres humanos se concentrem em tarefas mais criativas e complexas. Além disso, a inteligência artificial pode ajudar a resolver problemas complexos, como a detecção precoce de doenças e a prevenção de acidentes em ambientes perigosos.

No entanto, há também muitos críticos da inteligência artificial que argumentam que ela representa uma ameaça à privacidade, segurança e direitos humanos. A tecnologia pode ser usada para monitorar e controlar as pessoas, e há preocupações de que ela possa ser usada para criar armas autônomas perigosas ou para substituir muitos empregos humanos.

Além disso, a inteligência artificial pode ser tendenciosa e reproduzir preconceitos e desigualdades existentes na sociedade. Por exemplo, algoritmos de recrutamento de emprego podem discriminar candidatos com base em sua raça, gênero ou origem étnica, mesmo sem intenção.

É importante reconhecer que a inteligência artificial não é uma solução mágica para todos os nossos problemas. Embora possa oferecer muitos benefícios, também apresenta riscos e desafios significativos. É importante que as empresas, governos e pesquisadores trabalhem juntos para garantir que a inteligência artificial seja desenvolvida e usada de maneira responsável, ética e equitativa. Isso inclui a criação de políticas regulatórias claras e eficazes, bem como a promoção de pesquisas e discussões públicas sobre o impacto da inteligência artificial em nossa sociedade e nosso futuro.

Com o rápido avanço da tecnologia, a inteligência artificial (IA) vem se tornando cada

vez mais presente em nossas vidas, afetando a forma como vivemos e interagimos com o mundo ao nosso redor.

No cotidiano, a IA pode ser encontrada em diversos campos, desde assistentes pessoais como a Siri e a Alexa, até sistemas de recomendação de produtos em lojas online e análises de dados em empresas. Além disso, a IA também está sendo usada em setores como a saúde, a segurança e o transporte, para melhorar a qualidade de vida das pessoas e aumentar a eficiência das operações.

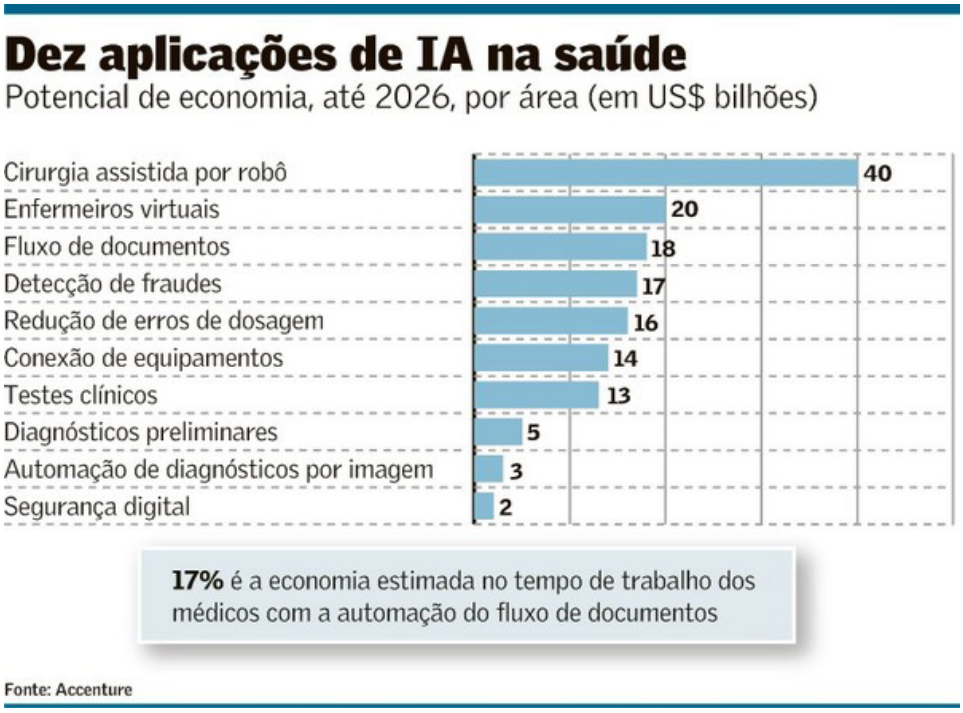
No entanto, o uso da IA no cotidiano também traz preocupações em relação à privacidade e à segurança dos dados pessoais. A coleta e o processamento de informações podem ser usados de forma abusiva e invasiva, levando à violação da privacidade dos indivíduos. Além disso, a IA pode ser programada de maneira tendenciosa ou preconceituosa, reproduzindo e ampliando desigualdades sociais e raciais.

É importante que a implementação da IA no cotidiano das pessoas seja cuidadosamente avaliada, levando em consideração não apenas os benefícios potenciais, mas também os possíveis riscos e desafios éticos e legais. É necessário estabelecer regulamentações claras e mecanismos de controle para garantir que a IA seja usada de forma responsável e equitativa, respeitando os direitos e a privacidade dos indivíduos.

2.3.1 Benefícios da IA em diversas áreas

A inteligência artificial (IA) tem se mostrado cada vez mais benéfica em diversas áreas, desde a saúde até a indústria, passando pela educação e pelo entretenimento. Na área da saúde, um estudo mostrou que a IA pode ajudar a diagnosticar o câncer de mama com mais precisão do que os radiologistas humanos. A IA identificou 94,5% dos casos de câncer, enquanto os radiologistas identificaram 89,9%. A IA também pode ajudar a reduzir custos e melhorar a eficiência da indústria. Um relatório da Accenture estima que a IA pode economizar US$ 1,2 trilhão em custos de trabalho em todo o mundo até 2025.

Gráfico 2 – Economia com IA pode chegar a US$ 150 bilhão



Fonte: Globo.com (2019)

No relatório, apresentado no Gráfico 2, é possível observar um aumento significativo na economia em diversas áreas, previsto até o ano de 2026, destaca a importância da inteligência artificial como um fator impulsionador de crescimento e inovação em diversos setores, oferecendo benefícios tangíveis tanto para as empresas quanto para a sociedade como um todo. Na educação, a IA pode ajudar a personalizar o aprendizado para cada aluno. Uma pesquisa da Pearson descobriu que 60% dos professores acreditam que a IA pode ajudar a tornar o ensino mais eficiente. A IA também tem um grande potencial para melhorar a experiência do usuário no setor de entretenimento. Um estudo da Juniper Research estima que a IA pode economizar US$ 11 bilhões em custos de produção até 2023.

Essas estatísticas demonstram que a IA pode trazer muitos benefícios para diversas áreas e setores, melhorando a precisão, eficiência e qualidade do trabalho humano. No entanto, é importante lembrar que a IA não é uma solução milagrosa para todos os problemas e desafios. É importante usá-la com cuidado, ética e responsabilidade, garantindo que seus benefícios sejam maximizados e seus riscos minimizados.

3. CONCLUSÃO

Concluímos este trabalho enfatizando a importância da Inteligência Artificial na evolução da tecnologia, e a forma pela qual ela está sendo inserida no mundo, mais especificamente na questão trabalhista. Com o avanço desta ciência, atividades que antes eram realizadas apenas pelo homem, passaram a ser também realizadas pela máquina, esta que é desenvolvida e capacitada para atender as necessidades específicas para a qual foi elaborada, com autonomia para decidir sobre o melhor comportamento no momento de agir.

A automação impulsionada pela IA tem se mostrado eficiente em tarefas domésticas e profissionais, proporcionando ganhos de eficiência e produtividade. Robôs e sistemas automatizados são capazes de executar tarefas repetitivas e complexas, como limpeza, atendimento ao cliente e diagnóstico médico, liberando as pessoas para se dedicarem a atividades mais criativas e estratégicas.

Destacamos também, o modo como o trabalho e o emprego são afetados neste contexto, suas implicações no meio social e econômico, pois a IA uma vez inserida no dia a dia das pessoas pode afetar consideravelmente a forma que elas irão lidar com esses desafios. Portanto, é fundamental que o uso da IA seja avaliado cuidadosamente, levando em consideração seus impactos sociais, econômicos e éticos. É necessário garantir que a IA seja utilizada de maneira responsável e transparente, com mecanismos de controle e regulamentação adequados. Além disso, é importante que a sociedade como um todo esteja preparada para as mudanças trazidas pela IA, tanto em termos de capacitação profissional quanto de conscientização sobre seus impactos.

Com o uso responsável e ético da IA, podemos aproveitar ao máximo seus benefícios e minimizar suas desvantagens, tornando-a uma ferramenta poderosa para melhorar a qualidade de vida das pessoas e impulsionar o progresso social e econômico.

Mas, de fato, podemos enfatizar que a combinação da Inteligência Artificial com a humana pode ajudar a superar os nossos limites e elevar nossa racionalidade a outro patamar. Associar estas forças é mais um passo da humanidade em sua evolução, e conhecer os benefícios e os proveitos desta tecnologia nos faz pensar que o avanço da transformação digital não aconteceu para prejudicar os profissionais, nem para tirar seus cargos, mas é uma vantagem, que desocupa as pessoas sob a responsabilidade do trabalho braçal e

repetitivo, e oferece a oportunidade de apresentarem capacidade suficiente em uma função estratégica, para executar tarefas mais importantes no andamento dos negócios.

Em suma, a inteligência artificial está transformando o cotidiano das pessoas, oferecendo benefícios em termos de interação, personalização e automação. No entanto, é fundamental acompanhar de perto os avanços tecnológicos, avaliar seus impactos e buscar soluções responsáveis e inclusivas. A IA tem o potencial de aprimorar a qualidade de vida e impulsionar o progresso, desde que seja utilizada de forma ética, responsável e considerando sempre o bem-estar humano.

Referências

Accenture. (n.d.). **Artificial Intelligence Summary Index**.

Araújo, F. M. (2020). **A inteligência artificial e os seus impactos no mundo do trabalho**.

Autor, D., Mindell, D., & Reynolds, E. (dezembro, 2020). **Inteligência Artificial e Trabalho: O trabalho do futuro: moldando a tecnologia e as instituições** (4ª ed.).

DAMACENO, Siuari Santos; VASCONCELOS, Rafael Oliveira. **INTELIGÊNCIA ARTIFICIAL: UMA BREVE ABORDAGEM SOBRE SEU CONCEITO REAL E O CONHECIMENTO POPULAR**. Caderno de Graduação - Ciências Exatas e Tecnológicas - Unit - Sergipe, Aracaju, v. 5, n. 1, p. 11-16, out. 2018.

DOS SANTOS GOMES, D. (2010, ago./dez.). **Inteligência Artificial: Conceitos e Aplicações [PDF]**.

ERNER, Deivid Augusto. **A quarta revolução industrial e a inteligência artificial: um estudo sobre seus conceitos, reflexos e possível aplicação no direito por meio da análise de texto jurídico como forma de contribuição no processo de categorização preditiva de acórdãos.** 2019. 211 f. Dissertação (Mestrado) - Curso de Direito, Universidade do Vale do Rio dos Sinos, Porto Alegre, 2019.

Globo. (2019, 26 de setembro). **Economia com IA pode chegar a US$ 150 bi. Valor Econômico**. Disponível em https://valor.globo.com/publicacoes/suplementos/noticia/2019/09/26/economia-com-ia-pode-chegar-a--us-150-bi.ghtml. Acesso em: 20 mar. 2023.

GOMES, Dennis dos Santos. Inteligência Artificial: conceitos e aplicações. Revista Olhar Científico, [S. L.], v. 1, n. 2, p. 234-246, dez. 2010.

GRACIOSO, Luciana de Souza, et al. Indexação automática de imagens na web: tendências e desafios no contexto deep learning. Revista Ibero-Americana de Ciência da Informação, [s. l], v. 11, n. 2, p. 541-561, 2018.

Keith, A. B. P. (Novembro - 2021). **Um estudo sobre o uso da inteligência artificial nas empresas**.

MENDONÇA, Claudio Marcio Campos de; ANDRADE, António Manuel Valente de. **Uso da IoT, Big Data e Inteligência Artificial nas capacidades dinâmicas: um estudo comparativo entre cidades do Brasil e de Portugal.** Informação & Sociedade: Estudos, João Pessoa, v. 29, n. 4, p. 37-60, dez. 2019.

Microsoft. (2020). **A adoção de inteligência artificial pode adicionar 42 pontos percentuais de crescimento adicional ao PIB do Brasil até 2030**.

MONARD, Maria Carolina; BARANAUSKAS, José Augusto. **Aplicações de Inteligência Artificial: uma visão geral**. In: CONGRESSO DE LÓGICA APLICADA **À** TECNOLOGIA, 1., 2000, São Paulo. Anais [...]. São Paulo: Faculdade Senac de Ciências Exatas e Tecnologia, 2000. p. 339-348.

NÉRI, Edmilson Lucena. **Agentes de software: delegando decisões a programas**. Rae Eletrônica, [S.L.], v. 4, n. 1, p. 1-11, jun. 2005. FapUNIFESP (SciELO).

NOVAIS, Paulo; FREITAS, Pedro Miguel. **Inteligência Artificial e regulação de algoritmos.** 2018.

QUARESMA, Alexandre Quaresma. Inteligências artificiais e os limites da computação. Paakat: Revista de Tecnologia y Sociedade, [Guadalajara], v. 8, n. 15, p. 69-84, ago. 2018.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda. São Paulo. Edipro. 2016

Sgarbosa, P., & Del Vechio, G. H. (2020). **Inteligência artificial e suas implicações: como os dispositivos inteligentes e assistentes virtuais influenciam o cotidiano das pessoas**. Interface Tecnológica, 12(2), 153-165.

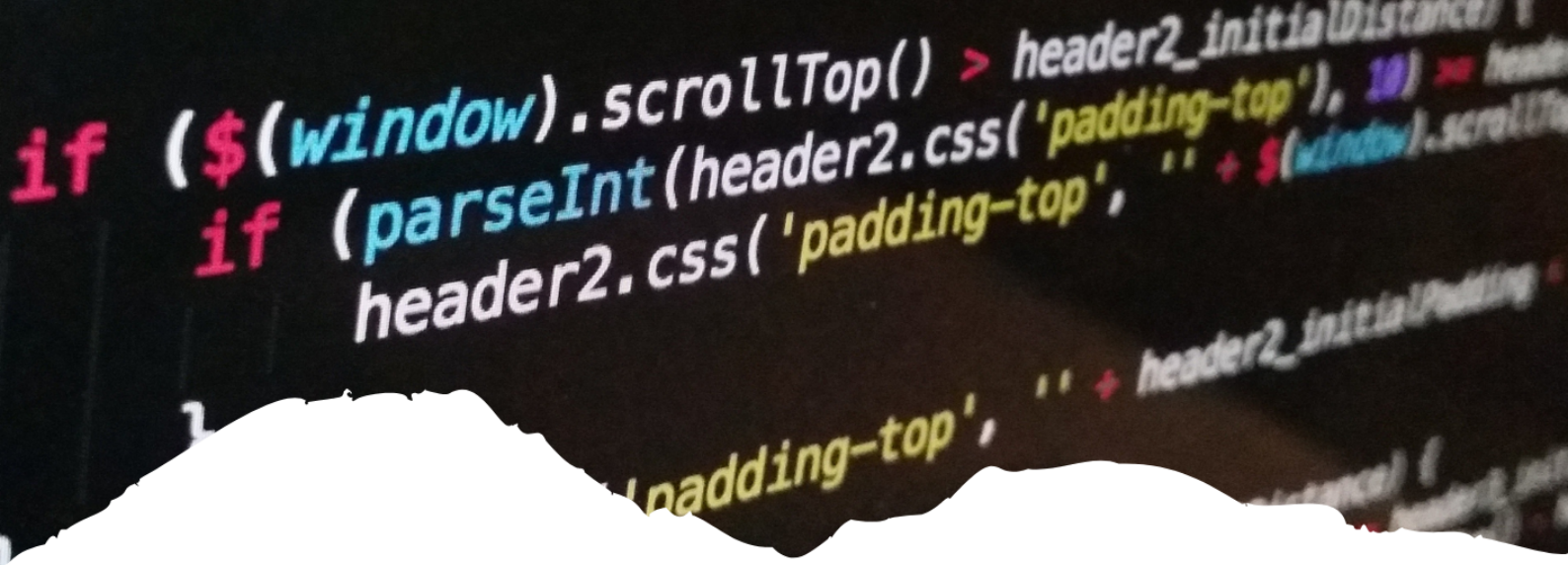
SILVA, J. A. S.; MAIRINK, C. H. P. Inteligência artificial: aliada ou inimiga. LIBERTAS: Rev. Ciência. Soc. Apl., Belo

Horizonte, v. 9, n. 2, p. 64-85, ago. /dez. 2019.

Sociedade Brasileira para o Progresso da Ciência. **SciELO - Scientific Electronic Library Online**. Disponível em: https://www.scielo.org/. Acesso em: 19 mar, 2023.

Veiga, R. A. C., & Pires, C. C. (16, December 2018). **Impacto da inteligência artificial nos locais de trabalho**.

ZILIO, Diego. **Inteligência artificial e pensamento: redefinindo os parâmetros da questão primordial de Turing**. Ciênc. cogn**.**, Rio de Janeiro, v. 14, n. 1, p. 208-218, mar. 2009.



5

A PRÁTICA DA ACESSIBILIDADE NA WEB COMO FORMA DE INCLUSÃO SOCIAL

THE PRACTICE OF ACCESSIBILITY ON THE WEB AS A WAY OF SOCIAL INCLUSION

Matheus Silva Guterres

Catterina Dal Bianco

Resumo

Este trabalho surgiu a partir do interesse em investigar sobre a problemática relacionada a entender a forma a prática de acessibilidade na web pode contribuir para a inclusão social. Dessa forma, o objetivo geral desta pesquisa foi fazer um estudo das principais práticas de acessibilidade na web que estão sendo realizadas como forma de inclusão social. Além disso, de maneira mais específica, pretendeu-se: a) Apresentar o conceito de acessibilidade na web e inclusão social; b) Descrever as principais práticas de acessibilidade na web para proporcionar a inclusão social e c) Apresentar as dificuldades que precisam ser superadas para garantir que a acessibilidade na web proporcione a inclusão social. Sobre a metodologia, neste trabalho realizou-se pesquisa do tipo revisão bibliográfica, qualitativa e descritiva, consultando, para isso, textos e pesquisas de autores que tratam sobre a temática em questão. Percebeu que algumas práticas de acessibilidade vêm sendo importantes para proporcionar a inclusão social, mas que ainda não são suficientes, pois ainda carece de muitas outras para dar conta da necessidade do país.

Palavras-chave: Práticas de acessibilidade, Inclusão social, Web.

Abstract

This work arose from the interest in investigating the problem related to understanding how the practice of accessibility on the web can contribute to social inclusion. Thus, the general objective of this research was to carry out a study of the main accessibility practices on the web that are being carried out as a form of social inclusion. In addition, more specifically, it was intended to: a) Present the concept of accessibility on the web and social inclusion; b) Describe the main accessibility practices on the web to provide social inclusion and c) Present the difficulties that need to be overcome to ensure that accessibility on the web provides social inclusion. About the methodology, in this work, a bibliographical review, qualitative and descriptive research was carried out, consulting, for this, texts and researches of authors that deal with the theme in question. He realized that some accessibility practices have been important to provide social inclusion, but that they are still not enough, as there is still a lack of many others to meet the country's needs.

Keywords: Accessibility practices. Social inclusion. Web.

1. INTRODUÇÃO

Atualmente, algo muito comum e que faz parte da vida de praticamente todos os brasileiros é o uso da internet e da esfera midiática como forma de adquirir conhecimento, compartilhar informações e inserção em um espaço que permite atualizações imediata. Apesar disso, ainda existe uma parcela da sociedade que ainda tem dificuldade de se incluir totalmente nesse acesso, fazendo com que haja uma fragilidade na inclusão social em razão da não acessibilidade na web. É nesse contexto que este trabalho se insere. Nesse sentido, nesta pesquisa busca-se investigar justamente como a prática de acessibilidade na web pode contribuir para a inclusão social.

Nesse sentido, um trabalho que realize um estudo das principais práticas de acessibilidade na web que estão sendo realizadas como forma de inclusão social, sem dúvida, é de suma importância, pois, a partir disso, se poderá ter um panorama do que já vem sendo feito e, também, conhecer as dificuldades para, assim, entender o que precisa ser feito para garantir que de fato a acessibilidade na web ocorra de forma plena garantindo a inclusão social. Dessa forma, este trabalho se justifica pelo fato de poder apresentar resultados com discussões e reflexões sobre a temática em questão e, também, por poder servir como material de consulta para futuras pesquisas acadêmicas e para os demais estudantes e pesquisadores que têm interesse em conhecer mais sobre a acessibilidade na web como forma de inclusão social.

Entende-se que muitas pessoas têm dificuldade em acessar informações e/ou manusear dados e manusear websites. Para amenizar essa realidade, há o que se chama de acessibilidade na web que, desde 2006, é reconhecida como um direito básico humano. A partir disso, surgiu o problema de pesquisa por meio do seguinte questionamento: de que forma a prática de acessibilidade na web pode contribuir para a inclusão social?

Dessa forma, nesta pesquisa buscou-se, como objetivo geral, fazer um estudo das principais práticas de acessibilidade na web que estão sendo realizadas como forma de inclusão social. Além disso, de maneira mais específica, pretendeu-se: a) Apresentar o conceito de acessibilidade na web e inclusão social; b) Descrever as principais práticas de acessibilidade na web para proporcionar a inclusão social e c) Apresentar as dificuldades que precisam ser superadas para garantir que a acessibilidade na web proporcione a inclusão social.

Sobre a metodologia, neste trabalho realizou-se pesquisa do tipo revisão bibliográfica, qualitativa e descritiva. Dessa forma, Dias (2016, p.9) ressalta que essa revisão é “a busca e análise crítica, do que está sendo discutido na literatura sobre determinado tema”. Foram consultados livros, monografias, dissertações e artigos científicos divulgados e publicados em sites de banco de dados. Ademais, para a realização da consulta dos textos, foram utilizadas as respectivas palavras-chave: “Prática de acessibilidade na web” “Inclusão social”.

Este texto encontra-se organizado estruturalmente, além desta introdução, no tópico1, também, consta os tópicos 2, 3 e 4, constando, ainda, a apresentação das referências bibliográficas consultadas.

2. O CONCEITO DE ACESSIBILIDADE NA WEB E INCLUSÃO SOCIAL

Neste tópico será realizada uma explanação acerca do conceito de acessibilidade na web, destacando, também, a inclusão social por meio disso, em consonância com o que foi

proposto no primeiro objetivo específico desta pesquisa.

2.1 A Acessibilidade na web

A acessibilidade na web é algo que muito vem sendo discutido e refletido quando o assunto é inclusão social, pois sabe-se que há um certo distanciamento do que é para acontecer para o que de fato ocorre. Muitas vezes, isso não chega a se tornar uma realidade.

Embora seja um tema que precisa ser cada vez mais discutido, entende-se que acessibilidade é o direito de ir e vir sem barreiras, poder acessar um lugar, serviço, produto ou informação de forma segura e autônoma, sem nenhum tipo de barreira.

Nesse sentido, verifica-se que "encontra-se embutido no próprio conceito de acessibilidade um aspecto que tem sido amplamente utilizado e que se refere a um desenho de espaços urbanos, edificações, transportes e produtos tecnológicos que atendam a todas as pessoas". (TAVARES FILHO, p.26, 2003).

A acessibilidade pode permitir todos os direitos e oportunidades iguais, independente da sua capacidade ou circunstâncias. Sendo completamente desagradável, por exemplo, não ter como receber um cadeirante em um prédio por falta de instalações acessíveis ou não ter acesso a um site da web para pessoas com deficiência visual.

Destaca-se que "a primeira ideia que se tem quando se fala em acessibilidade é a acessibilidade de pessoas com deficiência física, porém significa também acessibilidade de comunicação e atitudinal" (JALVES, 2010. p.21).

> Trata-se do direito de se comunicar - que é diferente do direito à comunicação, à informação e à participação - e não está expresso em nenhuma convenção de direitos humanos. Se uma pessoa surda vai a um evento e este não tem um intérprete de Libras (Língua Brasileira de Sinais), por exemplo, o seu direito de se comunicar está sendo violado. É um problema tão óbvio que ninguém vê. O direito de se comunicar tem a ver com a liberdade de expressão e vem antes dos outros, por isso precisa ser garantido (WERNECK, p.26, 2004).

Nesse sentido, a acessibilidade precisa sempre ser algo que deve ser tema de atenção, visto que:

> Muitas vezes as discussões sobre acessibilidade ficam reduzidas às limitações físicas ou sensoriais dos sujeitos com necessidade especiais, mas esses aspectos podem trazer benefícios a um número bem maior de usuários, permitindo que os conhecimentos disponibilizados na Web possam estar acessíveis a uma audiência muito maior, sem com isso, prejudicar suas características gráficas ou funcionais (CONFORTO; SANTA ROSA, 2002, p. 92-94).

Para Krug, (2001, p.14), "a primeira regra para a navegabilidade é "ser óbvio", quando o usuário olhar para a página ela deve ser direta e autoexplicativa".

> Este é um dos propósitos da internet, uma ferramenta que busca facilitar a comunicação e troca de informações mundiais. Porém nem sempre o percurso feito no meio virtual é fácil. Isso ocorre, pois na maioria dos casos, as regras de padronização para se fazer um ambiente virtual são ignoradas ou nem

> mesmo conhecidas. Isso ocorre para que essa arquitetura, ou layout, chame uma maior atenção dos usuários, dediquem mais tempo naquele ambiente e para suprir as necessidades que cada instituição tem em expor seus serviços (KRUG, 2001, p.20).

A navegabilidade na web precisa ser de fácil acesso para todos, colocando o usuário como personagem principal no desenvolvimento de sites. Nesse sentido, frisa-se que a acessibilidade precisa garantir que, de fato:

> pessoas com deficiência podem usar a web. Mais especificamente, a acessibilidade na web significa que pessoas com deficiência podem perceber, entender, navegar, interagir e contribuir para a web. E mais. Ela também beneficia outras pessoas, incluindo pessoas idosas com capacidades em mudança devido ao envelhecimento (W3C ESCRITÓRIO BRASIL, 2013, p.21).

Dessa forma, o site precisa ser responsivo, em outras palavras, abrir em celulares, tabletes, desktop, evitar páginas com excesso de movimentos e efeitos.

2.2 A inclusão social por meio da acessibilidade na web

O direito de se comunicar é tido como sendo uma medida de controle por parte da sociedade, que visa a integração de pessoas excluídas, garantindo a participação igualitária de todos na sociedade, independente da classe social, condição física, mental, gênero e entre outros. Dessa forma, a inclusão social é oferecer oportunidades iguais de acesso a bens e serviços a todos.

O conceito de inclusão está em convidar para que se aproximem aqueles que estiveram historicamente excluídos ou deixados de lado. A Inclusão digital, da mesma forma que a inclusão social, é empregado em diferentes contextos, sendo raro que alguém defina o conceito em sua positividade. Em outros termos, fala-se de exclusão, a falta de oportunidades diante da sociedade, da falta de recursos computacionais e da rede debilitada de acesso.

> Nossa visão (e a matriz de análise de projetos de inclusão digital daí deriva) parte da premissa de que o processo de 'inclusão' deve ser visto sob os indicadores econômico (ter condições financeiras de acesso às novas tecnologias), cognitivo (estar dotado de uma visão crítica e de capacidade independente de uso e de apropriações dos novos meios digitais) e técnico (possuir conhecimentos operacionais de programas e de acesso à internet) (COSTA; LEMOS, 2005, p.25).

A inclusão enquanto processo social vem crescendo consideravelmente nas últimas décadas. Isso por meio de uma busca de estabelecimento de relação entre inclusão social e digital.

A inclusão digital tem como objetivo garantir que todas as pessoas possam se beneficiar das vantagens que a tecnologia traz. A importância da inclusão digital é essencial para que todos tenham acesso, pessoas com baixa renda, deficiente visuais.

É válido frisar que:

> A ideia de inclusão fundamenta-se numa filosofia que reconhece e aceita a diversidade na vida em sociedade. Isto significa garantia de acesso de todos a todas as oportunidades, independentemente das peculiaridades de cada indivíduo ou grupo social (ARANHA, 2001, p. 35).

Para isso, torna-se de extrema importância a educação inclusiva, a qual:

> constitui um paradigma educacional fundamentado na concepção de direitos humanos, que conjuga igualdade e diferença como valores indissociáveis, e que avança em relação à ideia de equidade formal ao contextualizar as circunstâncias históricas da produção da exclusão dentro e fora da escola (BRASIL, 2008, p. 1).

Enfatiza-se que a acessibilidade na web serve para ter uma inclusão destinado a pessoas com deficiência, facilitando, pois eles podem perceber, entender, navegar, interagir e contribuir para a web.

Assim, a acessibilidade na web tem como objetivo fazer websites para todas as pessoas que tenham deficiência ou não. Dessa forma, construindo uma internet sem barreiras. Para isso, é importante que se tenha:

> Condição para utilização, com segurança e autonomia, total ou assistida, dos espaços, mobiliários e equipamentos urbanos, das edificações, dos serviços de transporte e dos dispositivos, sistemas e meios de comunicação e informação, por pessoa com deficiência ou mobilidade reduzida (BRASÍL, lei 10.048 de 8 de novembro de 2000).

Portanto, a acessibilidade, além de contribuir para a inclusão social, permite que os indivíduos, sobretudo, os que têm alguma necessidade especial, sejam capazes de se vê como um cidadão que pode alcançar seus objetivos de vida, ter uma vida comum como qualquer outra pessoa e se sinta, de fato, integrado na sociedade.

3. AS PRINCIPAIS PRÁTICAS DE ACESSIBILIDADE NA WEB PARA PROPORCIONAR A INCLUSÃO SOCIAL

Neste tópico buscou-se descrever algumas práticas importantes de acessibilidade na web que são importantes para assegurar que a inclusão social ocorra na sociedade.

3.1 Práticas de acessibilidade na web

Primeiramente, é importante o entendimento de que para que para prática da acessibilidade na web ocorra é necessário que o indivíduo/usuário esteja conectado à internet. Para isso, o usuário precisa ter:

> a) algum dispositivo computacional (computador desktop, laptop, tablet celular, dentre outros) que possua softwares3 adequados para o acesso à Internet. b) acesso a algum computador conectado à rede, chamado de provedor,

> responsável por fornecer o acesso de outros computadores à internet. c) uma conexão física entre esses dois computadores, que pode ser através de uma linha telefônica convencional, uma linha de telefone celular ou uma linha de transmissão de dados, com ou sem fio (W3C ESCRITÓRIO BRASIL, 2013, p.17).

Para que a prática de acessibilidade ocorra, alguns pontos precisam ser considerados:

> a) O entendimento da importância, da abrangência e da universalidade da web: Está cada vez mais difícil encontrar um campo da atividade humana em que não haja, de algum modo, influência da web, seja na educação, na formação profissional, no trabalho, na informação, na cultura, nas comunicações, no comércio, nos negócios, na saúde, nos serviços públicos e nos contatos profissionais e pessoais, citando apenas os campos de utilização mais comuns;
>
> b) a reciprocidade: Quanto mais sítios e programas acessíveis estiverem disponíveis, mais efetivamente pessoas com deficiência poderão usar e contribuir com a web;
>
> c) a multiplicidade e a diversidade de fatores envolvidos, considerando, assim, que alguns componentes estejam trabalhando adequadamente em conjunto: Conteúdo, Navegadores e agentes do usuário, Tecnologia assistiva (usada por pessoas com deficiência e mobilidade reduzida, como é o caso dos programas leitores de tela, dos ampliadores de tela, dos teclados alternativos), conhecimento do usuário, Desenvolvedores, designers, codificadores, autores, entre outros, incluindo pessoas com deficiência que são desenvolvedores e usuários que contribuem com conteúdo, Ferramentas de autoria (authoring tools): softwares usados para criar sítios web, Ferramentas de avaliação (W3C ESCRITÓRIO BRASIL, 2013, p.22-24).

Oliveira e Silva (2011) descrevem que, amparando-se às leis inclusivas, há algumas práticas de acessibilidade que promovem o desenvolvimento e emprego de tecnologias acessivas, as quais são, na verdade, justamente as tecnologias “concebidas para contribuir, por exemplo, com pessoas com incapacidades ou deficiências a executarem atividades do cotidiano, como cadeiras de rodas, próteses, cães guias, aparelhos auditivos, bengalas, muletas e balões de oxigênio, por exemplo” (p.4).

Entre as práticas de acessibilidade na web, destacam-se algumas, são elas: uso de códigos mais simples, de validadores automáticos (descrição de imagens, hierarquia de cabeçalho, links e atalhos de navegação, estrutura de formulários, elementos descontinuados, idioma principal usados na página, etc.), boas práticas para conteúdo, validação do código do website, além de considerar também pelo menos esses quatro princípios das Diretrizes de Acessibilidade – Acessível, funcional, compreensível e consistente (OLIVEIRA; SILVA (2011).

Os referidos autores pontuam, ainda, que, quanto uso de computadores/navegação na web, na prática para a acessibilidade, precisa ser feito uso de:

> equipamentos e programas especiais que permitem, ou simplesmente facilitam o acesso por pessoas com deficiência. Entre estes estão os programas ledores de tela, sintetizadores de voz, displays em Braille, ampliadores de tela (para pessoas de baixa visão), programas de comando de voz para cegos e pessoas com dificuldades na digitação; teclados e mouses especiais controlados por um joystick ou pelos movimentos da cabeça, por exemplo, para pessoas com dificuldades motoras (OLIVEIRA; SILVA, 2011, p.4).

Considerando isso, destaca-se que, no Brasil, amparado na iniciativa do Ministério do Planejamento, criou o seu modelo de acessibilidade, o e-MAG, o qual foi planejado considerado como base nas normas adotadas em outros países e, sobretudo, na WCAG, para isso, adequando às necessidades brasileiras (OLIVEIRA e SILVA, 2011).

4. AS DIFICULDADES QUE PRECISAM SER SUPERADAS PARA GARANTIR QUE A ACESSIBILIDADE NA WEB PROPORCIONE A INCLUSÃO SOCIAL

Neste tópico são apresentadas algumas das principais dificuldades verificadas referentes à acessibilidade na web para que, de fato, a inclusão social ocorra da melhor forma.

4.1 As dificuldades de acessibilidade na web que precisam ser superadas para que ocorra a inclusão social

Nesse sentido, se faz necessário ter um acesso que seja facilitado para que todos possam utilizar de forma simples, até mesmo para que se tenha uma inclusão social através da tecnologia, caso contrário, se verificará o que se conhece como como exclusão moderna:

> é um problema social porque abrange a todos: a uns porque os priva do básico para viver com dignidade, como cidadãos; outros porque lhes impõe o terror da incerteza quanto ao próprio destino e ao destino dos filhos e dos próximos. A verdadeira exclusão está na desumanização própria da sociedade contemporânea, que ou nos torna panfletários na mentalidade ou nos torna indiferentes em relação aos seus indícios visíveis no sorriso pálido dos que não têm um teto, não têm trabalho e sobretudo, não têm esperança (MARTINS, 2002. p.21).

Uma das principais dificuldades encontradas no acesso à web é a falta do acesso a uma internet de qualidade, tendo em vista que boa parte da população ainda não tem o privilégio de ter esse acesso ou até mesmo de saber utilizar tais ferramentas. Portanto, é necessário, além da inclusão digital, fazer a capacitação da população, para que aja de fato uma inclusão social, já que "[...] a sociedade que exclui é a mesma sociedade que incluem e integra que cria formas também desumanas de participação, na medida em que delas se faz condição de privilégios e não de direitos (MARTINS, 2002. p.11).

> A partir dessa mudança de enfoque, não se trata mais de resgatar os "desviantes" ou "incapacitados", mas de lutar por formas dignas de inclusão social para o conjunto da população. [...] Uma política realmente cidadã deve procurar "excluí-los da precariedade", protegendo-os do mundo abjeto do ganho e do lucro imediato e possibilitando o desenvolvimento de suas criatividades e potencialidades (POCHMANN, 2004. p.40).

Queiroz (2005) apresenta alguns recursos que, muitas vezes, por não serem contemplados adequadamente na prática, eles podem gerar dificuldades de acessibilidade na web e precisam ser superadas para que ocorra a inclusão social. Os referidos recursos apresentados pelo autor são esses:

- Acesso rápido via teclado: isso para permitir o acesso rápido a conteúdos;
- Equivalente textual: disponibilizar todas as informações da página em texto;

- Cores: assegure-se de que todas as informações fornecidas com cor estejam também disponíveis sem cor;
- CAPTCHA: um tipo comum é aquele onde o usuário deve identificar as letras que são distorcidas em uma imagem. Usar um equivalente não-textual, nesse caso em áudio, é a alternativa mais bem aceita atualmente;
- Resoluções diferentes: é aconselhável a utilização de unidades de medida relativas como porcentagem e pixel para que a página possa se ajustar a resoluções diferentes de tela;
- Skip Links: âncoras para seções da mesma página que podem ser utilizadas para acesso direto a seções ou conteúdos específicos na página;
- Teclas de atalho: podem ser configuradas pelo desenvolvedor para o acesso rápido a determinadas áreas da página, mas sofrem variações em navegadores diferentes;
- Tamanho da fonte: através de javascript pode-se permitir ao usuário controlar o tamanho da fonte dinamicamente de acordo com sua preferência ou necessidade;
- Menu de acessibilidade: pode ser constituído de elementos de acessibilidade como skip links e elementos para alteração do tamanho da fonte (QUEIROZ, 2005).

Nesse sentido, ressalta-se, a importância de melhorar as ferramentas da web para facilitar seu manuseio. Soma-se a isso a necessidade de cursos de formação e aperfeiçoamento aos usuários quanto ao uso adequado de cada um desses recursos e que de fato isso seja garantido ao usuário.

5. CONSIDERAÇÕES FINAIS

Após o trabalho realizado, pôde-se ter uma visão geral acerca do conceito de acessibilidade na web e inclusão social. Ademais, apresentou-se, também, as principais práticas de acessibilidade na web para proporcionar a inclusão social e, ainda, elencou-se algumas dificuldades que precisam ser superadas para garantir que a acessibilidade na web proporcione a inclusão social.

Portanto, pode-se dizer que, com esta pesquisa, foi possível se ter um estudo e visão geral acerca das principais práticas de acessibilidade na web que estão sendo realizadas como forma de inclusão social. Nesse sentido, os objetivos propostos neste trabalho, tanto geral como específicos, foram alcançados.

É importante mencionar, também, que esta pesquisa não se pode se dar como esgotada, ao contrário, ainda há muitas coisas que precisam ser aprofundadas e carecem de mais estudos. Assim, este trabalho inicial poderá, inclusive, servir como material de consulta para acadêmicos que se interessam nesta temática e para demais pesquisadores e estudiosos.

Referências

ARANHA, M.S.F.A. Inclusão social e a municipalização. In: Manzini, E. J.(org.) **Educação Especial**: Temas atuais. Marilia: UNESP Publicações, 2001.

BRASIL. Decreto nº 6.949, de 25 de agosto de 2009. **Promulga a convenção internacional sobre os direitos das pessoas com deficiência e seu protocolo facultativo**, assinados em Nova York, em 30 de março de

2007. Brasília, 2009. Disponível em: Acesso em: 21 fev. 2014.

BRASIL, **Decreto nº 5.296**, de 2004.

CONFORTO, D. e SANTAROSA, L. M. C. **Acessibilidade à Web**: Internet para Todos. Revista de Informática na Educação: Teoria, Prática – PGIE/UFRGS v.5 nº2, 2002.

COSTA, L.; LEMOS, A. Um modelo de inclusão digital: o caso da cidade de Salvador. In: **Revista de Economia Política de las Tecnologias de la Informatión e Comunicación**. Vol. VIII, n. 6, sep.-dic. 2005. Disponível em http://www.eptic.com.br. Acesso em 4 dez. 2006.

COSTELLA, Antonio F. **Comunicação**: Do Grito ao Satélite. Campos do Jordão. Ed. Mantiqueira, 2001.

DIAS, Ana Carolina Esteves. **Guia:** como elaborar uma revisão bibliográfica. Instituto Nacional de Pesquisas Espaciais: São José dos Campos, 2016.

WERNECK, C. (2004). **Acessibilidade**: Uma chave para a inclusão social". Disponível em: Acesso em: 05 mai. 2005.

KRUG, Steve. **Não Me Faça Pensar**. São Paulo. Ed. Market Books, 2001.

MARTINS, Kerley. **Teorias de aprendizagem e avaliação de software educativo.** Monografia (Informática Educativa) Universidade Federal do Ceará. 2002. Disponível em: acesso em: 18 de fevereiro de 2017.

NICÁCIO, Jalves Mendonça. **Técnicas de Acessibilidade**: Criando uma Web para Todos. Maceió. Ed. Edufal, 2010.

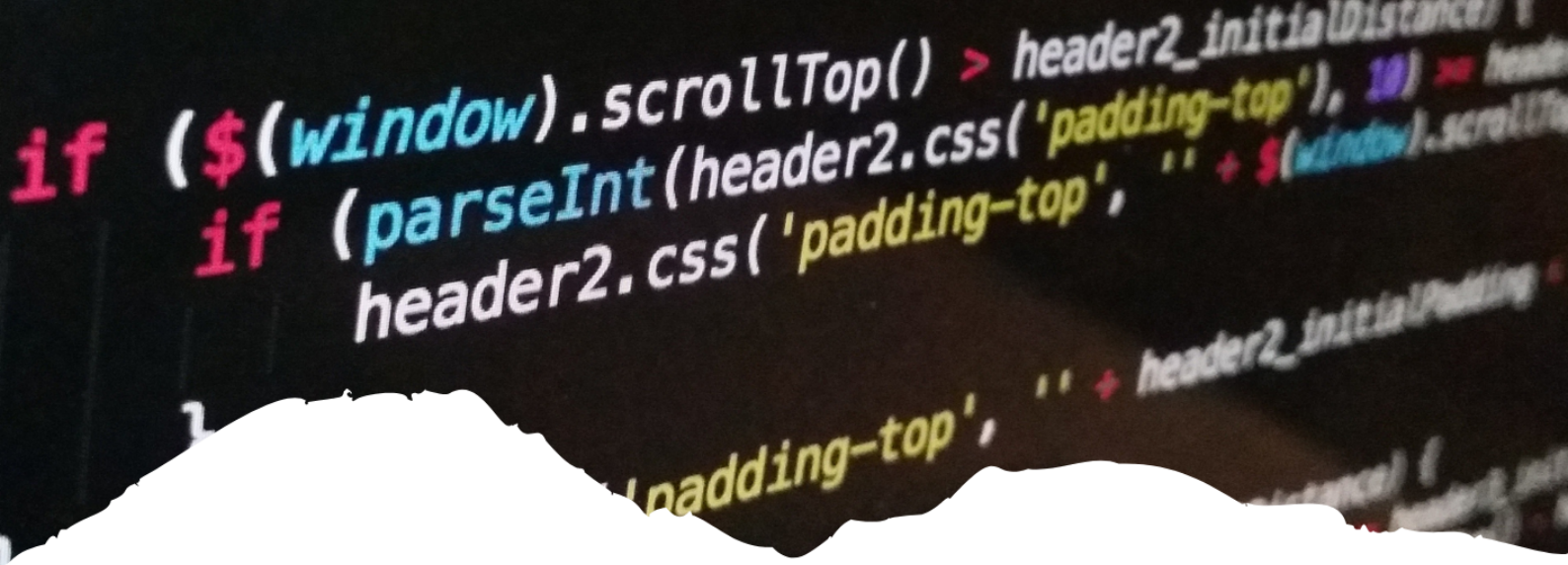
OLIVEIRA, Victor Adriel de Jesus; SILVA, Vânia Cordeiro da. **Acessibilidade em Sites e Sistemas Web:** estudo das tecnologias acessivas e diretrizes de acessibilidade web. 2011. Disponível em: <file:///C:/Users/franciscaiso/Downloads/GD_06_82635_1.pdf>. Acesso em: 1 de novembro de 2022.

POCHMANN, M. **Educação e trabalho**: como desenvolver uma relação virtuosa?. Educ. Soc., Campinas, v. 25, n. 87, 2004.

QUEIROZ, M. A. **Acessibilidade web:** Tudo tem sua Primeira Vez. 2005. Disponível em: <http://www.bengalalegal.com/capitulomaq.php>. Acesso em: 30 de outubro de 2022.

TAVARES FILHO, J. P., MAZZONI, A. A. RODRIGUEZ, A. M. e ALVES, J. B. M. Aspectos ergonômicos da interação com caixas automáticos bancários de usuários com necessidades especiais características de idosos. In: **Congresso Iberolatinoamericano de Informática Educativa Especial**, 3. Anais em CD, Fortaleza - Brasil, 2002.

W3C ESCRITÓRIO BRASIL. **Cartilha Acessibilidade na Web W3C Brasil.** 2013. Disponível em: <https://www.w3c.br/pub/Materiais/PublicacoesW3C/cartilha-w3cbr-acessibilidade-web-fasciculo-I.pdf>. Acesso em: 30 de outubro de 2022.



6

ENGENHARIA SOCIAL E O LADO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

SOCIAL ENGINEERING AND THE WEAKER SIDE OF INFORMATION SECURITY IN SOCIAL NETWORKS

Vinicius Carvalho de Oliveira

Roberto Max Louzeiro Pimentel

Resumo

Com o crescente uso das redes sociais, é comum receber links em seu privado, de marketing ou terceiros, prometendo fornecer determinados produtos, serviços ou ofertas tentadoras. Por tanto, nos seus milhares de e-mails, SMS, links vindos através de redes sociais pode conter alguma tentativa de Phishing. Em outras palavras, pode ser uma tentativa maliciosa de um hacker ou alguém com conhecimento de persuasão afim de manipular uma pessoa aplicando-lhe um golpe. Com base nesta hipótese, o objetivo deste trabalho é mostrar a vulnerabilidade humana, associada às falhas de segurança individual, onde o meio de persuasão funciona através da engenharia social. Portanto, este estudo visa mostrar métodos de Phishing, com objetivo na prevenção dos dados, exibindo como os invasores se comportam na maioria dos casos. Esta monografia procura determinar como a incitação ao inconsciente pode levar a consequências de roubo de dados. Do que foi mencionado acima, pode-se concluir que as boas práticas de segurança nem sempre são suficientes para evitar ataques que se enquadram em características cibernéticas, mas devem abranger a maioria deles a serem evitadas.

Palavras-chave: Engenharia social, Segurança da Informação, Redes sociais

Abstract

With the increasing use of social networks, it is common to receive links in your private, marketing or third party emails promising to provide certain products, services or tempting offers. Therefore, in your thousands of e-mails, SMS, links from social networks may contain some attempt at phishing. In other words, it may be a malicious attempt by a hacker or someone with persuasive knowledge to manipulate a person into a scam. Based on this hypothesis, the goal of this paper is to show human vulnerability, associated with individual security flaws, where the means of persuasion works through social engineering. Therefore, this study aims to show methods of Phishing, with an objective in the prevention of data, showing how the attackers behave in most cases. This monograph seeks to determine how unconscious incitement can lead to data theft consequences. From the above, it can be concluded that good security practices are not always sufficient to prevent attacks that fall under cyber characteristics but should cover most of them to be avoided.

Key-words: Social Engineering, Information Security, Social Networking.

1. INTRODUÇÃO

Quando se trata de segurança da informação, o que vem à sua mente? Um programador digitando vários códigos hackeando um sistema em segundos, ou uma tela cheia de zeros e uns? bem, isso é apenas para filmes. A segurança da informação é uma área da programação que visa estabelecer um ambiente de navegação segura, seja navegado na web ou em sua rede social favorita. No entanto, mesmo com todos os mecanismos de segurança em vigor, as pessoas ainda podem ser enganadas ou persuadidas, isso se deve pela técnica chamada de engenharia social.

O foco dessa pesquisa é tratar como a engenharia social é aplicada nas redes sociais e a importância da segurança da informação. Sobre engenharia social são atos que configura se persuasivo, por se dispor de vários métodos, que em conjunto, lesa e subtraem informações privadas de um indivíduo. Por tanto, para segurança da informação deve-se empregar um pouco mais atenção, visto que, com ela aprimorará as condutas de segurança evitando em clicar ou a repassa informações a terceiros.

Por tanto este trabalho demostra práticas de segurança apontando as fragilidades humanas ao se utilizar a internet e as redes sociais, tento em vista as práticas de engenharia social se demostra eficaz na manipulação de um indivíduo. Essa pesquisa visa responder ao seguinte questionamento. Quais os efeitos da engenharia social e a vulnerabilidade da persuasão humana em ataques que capturam informações pessoais por meio da internet, ou seja, das redes sociais, quais são os meios de segurança para evitar ter dados sensíveis vazados?

Temos como objetivo geral; investigar como são aplicados por meio da ética da engenharia Social os ataques na coletar de informações pessoais através da internet considerado os meios de segurança das informações na prevenção dos dados pessoais nas redes sociais. Na qual para compreende o objetivo geral, temos os objetivos específicos que são; apresentar os conceitos de engenharia social e o PHISHING; avaliar quais métodos de segurança da informação podem ser utilizados na prevenção da não exposição de dados sensíveis; descrever como as redes sociais compactuam com a política de privacidade pessoal e ataques.

O estudo terá uma vertente metodológica de revisão bibliográfica, sendo uma pesquisa qualitativa e descritiva na qual se utilizar livros, trabalhos científicos e repositórios digitais e sites confiáveis. A exploração do tema seguira o critério de qualidade e objetividade, buscando por acervo de até 20 anos e linguagem de fácil compreensão para acolher tanto a esfera acadêmica como a civil.

As informações coletadas por meio de livros, artigos, repositórios e sites, serão de extrema importância para o estudo, pois serão analisadas e julgadas relevantes ou não para o seguimento dessa exploração

2. CONCEITOS DE ENGENHARIA SOCIAL

Segundo Rosa; Silva e Silva (2012, p.4) “A engenharia social tem aplicabilidade em diversas áreas, servindo como ferramenta para exploração de falhas em organizações físicas ou jurídicas”. Ataques por meios de engenharia social trata-se de persuadir alguém a clicar ou fazer uma ação na internet na qual não sabe o risco em potencial de clicar ou baixar um arquivo infectado com malware, segundo, Silva, Araújo e Azevedo (2013, p. 40) “podendo

ser de uso benéfico ou não, protegendo ou atacando um sistema de segurança de informação empresarial ou até mesmo particular". Isso se potencializa quando o alvo é alguma empresa, no qual, qualquer funcionário está sujeito esse tipo de ataque que compromete a segurança de todo o sistema empresarial.

Os funcionários de uma empresa podem receber os melhores treinamentos ter as melhores ferramentas de segurança e trabalhar no lugar mais seguro possível que ainda assim estão sujeitos a destrutibilidade humana (MITNICK; SIMON, 1963).

Um engenheiro social baseia-se o seu ataque analisando os perfis de um certo indivíduo nas redes sociais com o Facebook, Instagram e entre outros, no qual procura analisar diversos aspectos relacionados ao seu ambiente de trabalho e sua vida pessoal traçando informação, como apresentado por Silva, Araújo e Azevedo (2013, p.42):

> Também podem ser caracterizados como uma grande ameaça à privacidade dos seus usuários, pois esses sites possuem/expõem um grande volume de informações pessoais e/ou profissionais, incluindo o ciclo de amizades, fotos, lugares que frequentam, endereço residencial e números de contato, cargo e emprego atual, e ainda, os familiares, aumentando o nível de visibilidade na Internet e as possibilidades de ataques de engenharia Social.

Entre tanto o comportamento dentro e fora do ambiente virtual como as redes sociais é cada vez mais vulnerável, com uma grande necessidade de socialização humana as pessoas naturalmente adicionam individuas que nunca ser conheceram pessoalmente, para Rosa et al. (2012, p.34) "ao simular uma amizade consegue tornar mais fácil a captura de informações, pois a amizade é uma das primeiras técnicas usadas por um engenheiro". Estas ações levam uma falsa confiam de amizades online.

2.1 Phishing

O Phishing é uma estratégia de engenharia social que se conceitua uma pesca de informações. Um exemplo seriam páginas falsas que se parecem com as páginas originais de uma loja ou site, mas são projetadas para fazer a página fake parecer real para enganar, subtraindo informações confidenciais, como nomes de contas e senhas bancárias, números de cartão e guardando inúmeras informações pessoais. "Geralmente, o destinatário é convidado a clicar sobre um link que aparece no corpo da mensagem ou abrir um arquivo anexo e, ao fazê-lo, aciona o download de um programa malicioso que vai penetrar no seu computador e capturar informações [..]". (FILHO, 2008, p. 1). O phishing para ser aplicado com sucesso precisa de alguns fatores cruciais que levem a vítima a cair na armadilha, na qual dois é citado por Santos (2019, p. 32). que é "[...] explorando a relação de confiança e o medo que existe entre as vítimas /utilizadores perante a mensagem, e por outro, na urgência criada para a prática da ação em causa". Por tanto de acordo com Piovesan et al. (2019, p. 50):

> O Phishing é uma técnica baseada em pescaria, ou seja, ela é realizada por meio de e-mails falsos, sites clonados, mensagens em redes sociais ou SMS (Short Message Service, que em português significa Serviço de Mensagens Curtas) é visível que ela apresenta um grande risco à segurança da informação"

2.2 E-mail falso

E-mails falsos são outros meios de manipulação na pretensão de ser obter Informações sigilosas. Essa é uma prática, mas utilizada por cibercriminosos por se de fácil aplicação na qual pode-se ter um boot que dispara vários e-mails para diversas pessoas ao mesmo tempo podendo conter o mesmo conteúdo variando somente os e-mails remetentes. Portanto para se ter uma maior segurança e confiabilidade do conteúdo é preciso verificar E ficar atento a diversas informações Presente no e-mail ou uma delas como destinatário, erros ortográficos e conteúdo generoso. Uma ferramenta que auxiliar a destacar e-mail que se caracteriza falsos ou de cunho duvidosos é os spams. Como explica Taveira et al. (2006, p. 208) “os spams também são usados para difundir programas maliciosos como vírus, vermes e cavalos de tróia”. Na figura a seguir mostra um e-mail na qual configurasse falso.

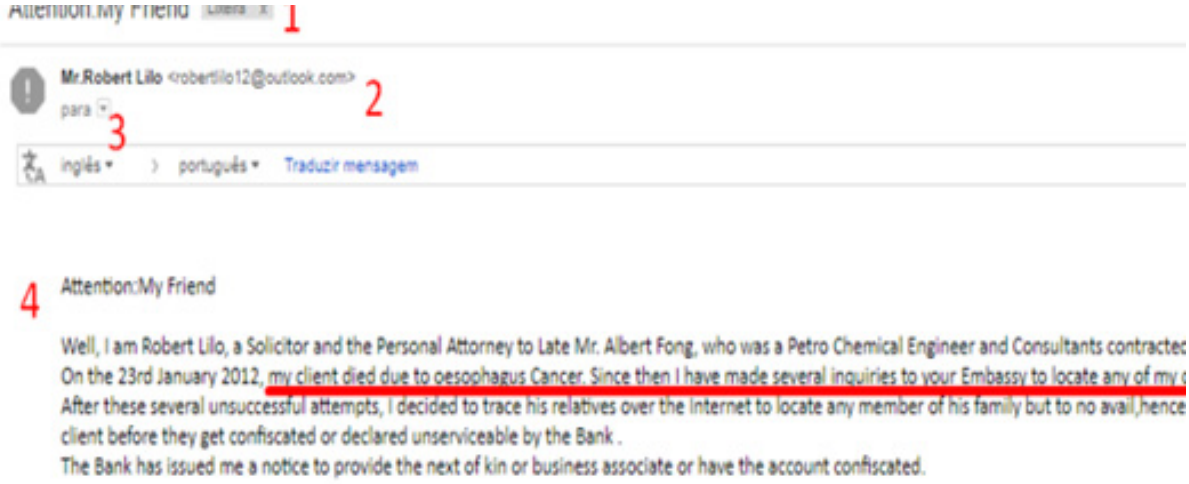


Figura 1 - E-mail Falso

Fonte: Hostinger (2022)

A figura 1 um demonstra uma tentativa de golpe, na qual o cibercriminoso se passa por um advogado representante de um falecido, que deixou uma fortuna milionária para a um tal ente familiar. Esses sublinhados em vermelho são os erros deixado pelo cibercriminoso. Através deles sublinhados é possível identificar diversas evidências de que se trata de um golpe, no qual o e-mail que foi enviado é estrangeiro e desconhecido não possui destinatário, incluir conteúdo de quantia financeira disponível de um parente inexistente. (HOSTINGER, 2022).

Os ataques de Phishing por meio de e-mails falsos são um meio muito eficaz para os cibercriminosos usarem essa técnica para capturar informações pessoais. Todo mundo recebe milhares de e-mails todos os dias, alguns deles de anúncios, cursos ou lojas etc. No entanto, entre os vários e-mails que você recebe todos os dias, alguns deles podem conter armadilhas que, se não observadas cuidadosamente, podem levar a vírus ou à disponibilidade de dados pessoais críticos. (BELCIC, 2020).

2.3 Vishing

Essa estratégia chamada de Vishing consistem quando uma pessoa receber uma suposta ligação para confirmar ou repassar, algumas informações. Essa prática, já possuir um escopo, a qual vai atacar, parte dessas práticas consistem em recolher informação via VoIP, ou seja, por uma ligação telefônica como, senhas bancárias de cartões entre outras

inúmeras credenciais de acessos. Como exemplo, mencionasse um cenário onde um cibercriminoso se passará por um funcionário bancário e falara algo como. Seu cartão foi bloqueado devido a uma compra no valor maior que o seu limite ou precisamos atualizar seu cadastro bancário para se confirma o cliente diga sua senha. Segundo Sá (2020, p.55) “dependendo do quão bem estruturada e convincente estiver a narrativa, a vítima pode retornar à ligação sem verificar se o número telefônico pertence, de fato, à empresa”. A figura 2, ilustra como e a comunicação entre o Cyber criminoso e a vítima.

Figura 2- Ataque Vishing

Fonte: web site security store (2021)

A figura 2 demonstra como é feito o ataque Vishing na qual o Cyber criminoso utiliza ligação VoIP passando se por funcionário bancário, a vítima por sua vez é convencida que se trata de uma ligação bancária e há algum problema na conta, o Cyber criminoso utiliza da confiança da vítima para extra e informações como os dados bancários senhas de cartões e até outros tipos de dados sensíveis.

O vishing é um ataque que demonstra um alto grau de persuasão e domínio das situações, no qual o cibercriminoso manipulam a situação de modo desvantajosa para a vítima, deixando-as em uma situação sem alternativas, empregando a ideia de que a melhor saída para aquela situação é repassar as informações solicitada por pelo cibercriminoso.

2.4 SMishing

O SMishing é um ataque semelhante ao Vishing, mas ao invés de utiliza-se o e-mail como forma de ataque, usa-se o SMS que é em forma de torpedo. O nome SMishing é uma junção das palavras SMS com expressão do inglês Phishing, dando assim origem as termo SMishing. Este tipo de ataque está ligado mais a aparelhos telefônicos por se tratar da utilização do SMS que encontrado só em smartphones. Esse golpe é o mais simples e o mais perigoso na qual normalmente as pessoas não costumo verificar a origem do torpedo, sendo assim o meio de ataque mais fácil de se cair. Esse tipo de ataque todo e qualquer indivíduo está sujeito e vulnerável a essa prática chamada SMishing.

A figura 3 logo abaixo demonstram um exemplo real de uma tentativa de golpe SMishing.

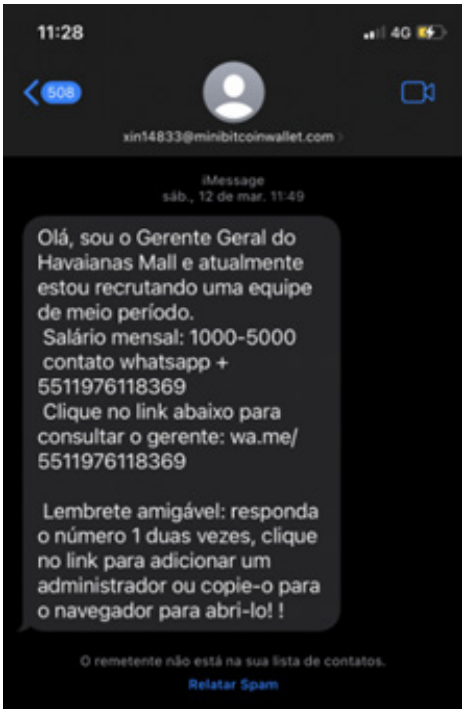


Figura 3 - Tentativa de golpe Smishing

Fonte: Ventura (2022)

Conforme a figura 3, representada acima de monstra uma tela de celular na qual as informações nela é um claro ataque de SMishing no qual o cibercriminoso se passar um tal gerente da empresa Havaianas e que está recrutando uma equipe para uma trabalho de meio período com a proposta salaria de 1000 a 5000 reais, como é possível consta, a imagem possuir a algumas informações com o número e link que deixa uma certa sensação de confiança mas na verdade e uma estratégia que tenta convencer a vítima a cópia e colar link no navegador. Notasse que o SMS possuir um texto argumentativo que tenta empregar uma narrativa bastante convincente. Essa prática de captura de informação torna-se a mais letal na qual é mais fácil uma pessoa clicar no link ou discar o número enviado por SMS, sendo assim mais difícil a verificação do conteúdo ou do remetente. O SMS é o meio de comunicação que traz mais confiança as pessoas, por ser tratar que seu número celular estará fora do alcance de qualquer tipo de ataque cibernético (VENTURA, 2022).

2.5 Pretexting

No Pretexting, um hacker normalmente pode usar vários métodos para convencer um usuário a fornecer informações confidenciais sobre ela ou uma empresa. Pode ser uma pesquisa falsa ou um perfil falso de rede social que constrói uma amizade e usa essa proximidade para extrair alguns dados úteis para uma invasão. Por tanto as técnicas de camuflagem também podem ser usadas por indivíduos disfarçados de colegas, policiais, bancos, autoridades fiscais, especialistas em companhias de seguros ou qualquer outro indivíduo com poder ou autoridade. Um hacker que usa esse truque deve simplesmente preparar as respostas para as perguntas que a vítima pode fazer. Em alguns casos, tudo o que você precisa é de uma voz autoritária, um tom envolvente e a capacidade de reagir rapidamente para moldar a situação (ALAZRI, 2015).

2.6 Tailgating

No tailgating, o infrator aproveita a proximidade de um indivíduo autorizado para invadir algumas áreas restritas na qual ele não possuir acesso, pois ao seguir um funcionário ele pode ter o acesso ao local sem ser barrado por nenhum vigilante ou supervisor do local, ou até criando condições para que ele passe. Uma das diversas práticas do trailing é que ele pode assumir várias formas. Por exemplo, um criminoso pode aparecer em uma entrada com muitas caixas criando assim uma ideia de que não é possível alcançar seu crachá de acesso, e exigir que as catracas sejam liberadas, porque o que está carregando é muito pesado. Ele também pode usar uniforme à vontade e afirmar que é prestador de serviço empregado em qualquer função, mas não está conseguindo entrar em contato com a pessoa que o chama pela recepção (PARALLIS, 2022).

3. SEGURANÇA DA INFORMAÇÃO

Segundo Fontes (2008, p. 32) “quando falamos em segurança da informação, logo nos vem à mente as instituições financeiras, as empresas de transporte aéreo e as organizações virtuais da internet”. Porém esse termo segurança da informação não se trata somente disso. Mas é um pilar bastante importante na vida, no qual com ela aprende-se a proteger e zelar informações essenciais, como fotos ou vídeos familiares por exemplo. Portanto, também isso não se aplica só na vida cotidiana, mas também nas empresas e corporações no qual as informações têm uma grande importância, assim como na vida pessoal não se pode repassar informações crítica para qualquer pessoa. Portanto “Uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor de informações consideradas sensíveis” (MARCIANO, 2006, p.49).

Para Buogo (2017, p. 43) a “segurança da Informação é a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança [...]”. Sendo assim um dos pilares essenciais para manter a confiabilidade e a disponibilidade de um determinado sistema.

3.1 Certificações para profissionais de segurança informação

Os profissionais de segurança da informação devem estar qualificados para realizar as tarefas necessárias. Para (EC-COUNCIL, 2022). Os certificados mais importantes são:

- **CEH** - Certified Ethical Hacker: No português é (Hacker Ético Certificado). Os hackers éticos são profissionais de segurança da informação, normalmente são contratados por empresas ou instituição para fazer uma verificação em seus sistemas. Seu papel é fazer descobertas de vulnerabilidades nas empresas, para isso utilizam as mesmas estratégias de hacking e ferramentas que os hackers podem utilizar para entrar em uma rede ou qualquer máquina física. Isso é necessário para testar a segurança das redes e sistemas apontando ser há e onde está a vulnerabilidade naquela determinada instituição.
- **CHFI** - Computer Hacking Forensic Investigation: Que no português (Investigação Forense de Hacking Computador). É o processo de identificação forense de hacking de computador, ou seja, de ataques hackers, no qual é realizar a coleta

adequada das evidências para diagnosticar os passos do crime cibernético. As ferramentas e técnicas forenses estão sendo cada vez mais aprimoradas, isso se deve ao fato de que profissionais dessa área estão aprimorando cada vez mais as técnicas dando assim ao profissional fornecer maior confiabilidade do diagnóstico nas investigações, seja cibercrime, forense digital ou até mesmo recuperação de dados cibernéticos de um computador.

- **CISSP** - Certified Information System Security Professional: Que no português (Profissional de Segurança de Sistemas de Informação Certificado). É uma das certificações mais procuradas pelos profissionais de segurança da informação. Os CISSP são especialistas em segurança da informação responsáveis por definir a arquitetura, design, gerenciamento ou governança para proteger um ambiente corporativo. Como tal, abrange os principais tópicos de segurança, incluindo tópicos de segurança atuais, como computação em nuvem, segurança móvel, segurança de desenvolvimento de aplicativos, gerenciamento de riscos e muito mais.

Esses são algumas das certificações que o profissional de segurança da informação deve obter para atuar nessas áreas.

3.2 Confidencialidade

A confidencialidade é um dos critérios mais sensíveis há uma instituição ou empresa, pois determina-se a confiança de todas as informações armazenadas na qual constituir a empresa. No em tanto, a segurança é uma questão particularmente humana que vai muito além dos aspectos técnicos ou físicos. Portanto, processos e políticas devem estar sempre em vigor para supervisionar e direcionar todos aqueles que contêm acessos às informações institucionais. Pôs quebra de sigilo das informações por funcionários ou terceiros é considerada um grande risco à segurança da informação, na qual, pode ou não ocorrer de forma intencional. É importante destacar que qualquer tipo divulgação pode feitos com quem tem acesso às informações da instituição ou também ser feitos tanto por partes internas quanto externas (NETWORKS, 2018).

3.3 Disponibilidade

A disponibilidade rege todo um conjunto de normas cujo sua principal função é mante o funcionamento operacionais da rede de uma empresa sempre em funcionamento, a fim de prevenir qualquer instabilidade ou para das operações de uma grande empresa. A parada de qualquer ativo que compõem uma empresa pode ocasionar enormes prejuízos financeiros. Pôs a disponibilidade é algo levado muito a seria pelas instituições. Por tanto para Machado (2014, p. 20) as empresas “devem estar aptos a recuperar quedas de disponibilidade de forma rápida e segura e a garantir que a produtividade das operações da empresa não seja afetada significativamente”.

3.4 Integridade

A integridade da segurança da informação é um ponto que precisa ser feito da forma mais segura possível na hora de ser armazenar os dados ou arquivos. Por tanto a Integridade refere-se à originalidade dos dados, ou seja, essas informações ou documentos não podem conter a probabilidade de serem alteradas, sem as permissões de quem os arma-

zenou. Isto envolve, determinar se as informações não foram alteradas durante o processamento, pois todos os documentos precisam ser preservados desde o primeiro momento de sua criação. (NETWORKS, 2018).

3.5 Ameaças

Segundo Pinheiro (2007 p. 12) “uma ameaça consiste em uma possível violação de um sistema computacional e pode ser acidental ou intencional”. Sendo assim uma ameaça acidental nada mais é que uma falha que envolve o sistema, sendo uma falha de software ou de hardware. Uma ameaça intencional envolve uma ação direta a um sistema feita premeditadamente para encontrar falhas e vulnerabilidade daquele determinado sistema. Estas ações são normalmente exploradas por um hacker que está buscando por alguma fragilidade, podendo assim, ser para fins de exportar os problemas, ou usar a subtrair informação confidenciais.

As ameaças podem ser exploradas de diversas maneiras como uma falha de software ou humana consequentemente as ameaças de software são as mais comuns, por se tratar que, qualquer sistema operacional está sujeito a falhas e bugs, em sua estrutura que pode ser explorada ou manipulada por um cibercriminoso que queira utilizar dessas falhas para a atacar, explorar e roubar determinados dados. Já para as ameaças humanas envolve os ataques Phishing como principal percursor de uma ameaça cibernética (NAKAMURA, 2007).

3.5 Ataques

Segundo Da Silva e Nogueira (2019, p. 45) “os ataques cibernéticos contra a confidencialidade possuem, em geral, o objetivo de conceder, ao atacante, acesso a dados que lhes são negados”. Por isso, configura-se um ataque de hackers em um sistema de negócios ou de um indivíduo específico. A definição de ataque não envolve somente a sistemas.

No entanto, interpreta se que o ataque pode ser feito de várias maneiras com estratégias e métodos diversificados que se emprega o mesmo objetivo de atacar uma rede ou sistema, a ponto de se obter alguma determinada informação que são os dados sensíveis. Por tanto para Gois (2018, p. 46) conclui que “esses ataques são ameaças identificadas tanto pelo Estado quanto pela sociedade, os quais devem ser combatidos”.

3.6 Autenticações de Usuários

Para Fontes (2017, p.52) “a autenticação tem por objetivo garantir que o usuário descrito na identificação é verdadeiramente essa pessoa. Isto é, busca provar que você é você”. Portanto a autenticação é um fator que deve ser levado muito a sério tanto por usuários comuns de serviços web, como por instituição ou empresa, ela irá minimizar as ações de terceiros que se passem por funcionários ou credenciado. As identificações de usuário podem ser feitas de várias maneiras, tanto quanto físicos ou virtuais, como o acesso de um determinado espaço, o credenciado passará por um leitor biométrico para adentrá-lo ou mesmo possuir um cartão de acesso. Já na forma virtual, o método caracteriza-se majoritariamente o acesso de um indivíduo credenciado há uma plataforma virtual que nada mais é um site ou sistema web, alocado na própria rede local. Por tanto “[...] os sistemas informáticos da maioria das organizações utilizam algum tipo de serviço de autenticação

e autorização de forma a impôr [*sic*] políticas [*sic*] de controlo de acesso a diferentes tipos de dados e/ou serviços" (SOUSA, 2010, p. 1).

Sobretudo as autenticações podem ser realizadas através de código enviados via SMS, e-mail, ou aplicativo de autenticação, por tanto o método mais utilizados e as senhas ou perguntas de segurança.

4. REDES SOCIAIS E AS POLÍTICAS DE SEGURANÇA E ATAQUES

As redes sociais como conhecemos atualmente são plataformas desenvolvidas com a finalidade de serem ambientes sociáveis e totalmente interativas. Uma rede social é uma estrutura que conecta pessoas de acordo com seus interesses e valores, e essa estrutura envolve um ambiente online onde o conceito é familiar. Para Recuero (2012, p. 12) as "redes sociais [...], são meios de comunicação emergentes, capazes de difundir informações em uma escala global por causa dessa apropriação, através dos sites de rede social". Em resumo, as redes sociais focam na interação entre as pessoas, enquanto o objetivo principal é compartilhar informações e conteúdo. Por fim, embora você possa interagir com amigos, a plataforma também se beneficia, pois vários anunciantes a utilizam para promover seus negócios.

4.1 Ataques nas redes sociais

Para iniciar um ataque em uma rede, os invasores geralmente seguem uma sequência lógica, desde a coleta dos dados pessoais a características bastantes específicas sobre o alvo, isso é feito para garantir maior precisão no ataque. Portanto um ataque executado nas redes sociais pode deixar rastros que o leve ao responsável que efetuou esse ato. Portanto, as vezes nem sempre é possível identificar um ataque, pois, a ação é tão bem elaborada, que tornar-se impossível, encontra rastros deixado pelo atacante. Para se proteger desses comportamentos, é necessário ter uma compreensão profunda da filosofia dos atacantes, normalmente é impossível uma pessoa comum com pouco conhecimento dessa prática perceber esses ataques, já para um especialista e algum tempo de investigação será possível diagnosticar um ataque malicioso podendo assim encontrar a melhor contramedidas a serem tomadas (SILVA; ARAÚJO E AZEVEDO, 2013).

4.2 Privacidade online

As plataformas que mais adotam as políticas de privacidade e segurança são as redes ou mídias sociais, pois são plataformas com um alto número de usuários que as utilizam diariamente. Uma vulnerabilidade nesses sistemas pode representar sérios riscos aos dados pessoais se compartilhados de forma maliciosa, mas algumas redes sociais tornam transparentes alguns dados que o usuário fornece a eles ao concluir seu cadastro, algumas dessas informações é considerada simples, por exemplo, endereço, sexo etc. Mas por existir uma gama de mídias sociais para Fernandes (2011, p. 1) "[...] no surgimento do Facebook muitas eram as preocupações com a privacidade e segurança, cedo esses receios se esbateram, sobretudo porque a rede crescia de uma forma muito célere e consistente". Isso mostra como uma das maiores redes sociais do mundo prioriza a segurança na privacidade de informações de seus usuários.

4.3 Redes sociais e suas vulnerabilidades

Usamos as redes de mídia social como ferramentas para compartilhar informações pessoais, como fotos e outros dados pessoais. Isso pode parecer inofensivo, mas muitas pessoas não se importam em fornecer suas informações pessoais. No entanto, lamentavelmente, as pessoas de má índole como os hackers acabam usando essas informações com outros propósitos nas quais podem sem para ataques de Phishing e outros. Portanto, é crucial considerar quais informações podemos compartilhar nas mídias sociais e se essa divulgação é realmente necessária. Atualmente disponibilizamos uma parcela significativa de nossa vida profissional e privada através das redes sociais (DIAS, 2011).

4.4 Guerra Cibernética

Hoje em dia há uma preocupação eminente constante em relação as guerras cibernéticas. Por tanto, esse é o termo para definir que se trata de um conflito que ocorrem no âmbito digital, onde ao em vez de armas e soldados são os malware e hackers com objetivos de controlam infraestrutura, redes, telecomunicações e até mesmo computadores e dispositivos que estejam conectados à internet como todo. No entanto ao contrário das ações isoladas de hackers, os ataques normalmente são classificados como as operações de guerra cibernética que visa causar maiores danos reais por meio de ataques hackers, e à disseminação de informações possíveis, interrompendo assim, as vigilâncias de tráfego aéreo e das plataformas que fornecem o controle logístico e das divulgações de produtos e serviços, por tanto, são exemplos de táticas que podem ser orquestradas em conflitos virtuais. Segundo Júnior; Lopes e Freitas, (2017, p. 49) “é possível ainda declarar, em favor da guerra cibernética, que, quanto mais um país estiver ‘plugado’ ao ciberespaço, especialmente no que tange a suas estruturas estratégicas, mais vulnerável estará para ataques originados no ciberespaço”.

4.5 As doenças das mídias Sociais

Segundo Dos Santos Azevêdo, Silva e Reis (2019, p. 59) “redes sociais significativas são redes de apoio que contribuem para o fortalecimento da identidade da pessoa e do seu reconhecimento no grupo inserido”. Por isso, quando usadas incorretamente, as redes sociais trazem diversos transtornos sociais e de saúde, isso se deve ao perfeccionismo das pessoas de que tudo nas redes deve ser o mais perfeito possível, alguns desses transtornos incluir sentimentos de isolamento, ansiedade, exaustão, obsessão com o corpo e o mais preocupante, a depressão. Por tanto, algumas dessas doenças se potencializa com o vício de passar uma boa imagem social, no entanto e possível compreender como as redes de relações sociais afetam o desenvolvimento social e os aspectos psicológicos do indivíduo a saúde.

4.6 Rápida propagação de Fake News

Como o surgimento das redes sociais é notório observar que as informações se propagam de forma instantânea pelo mundo, isso se deve também pelo fácil acesso à internet. Segundo Amaral e Santos, (2019, p.73) “a internet e [...] media [*sic*] sociais alteram significativamente a forma de como a informação é produzida e distribuída.” Tento como perspectiva a rápida disponibilidade de informações em geral é comum ser deparar com

informações falsas. Para Reule (2008, p. 108):

> [...] o boato virtual como falsa informação continua seu curso pela Web, pois mesmo existindo meios de se prevenir contra os rumores ou mesmo de se controlar, em determinados espaços, sua propagação, não há como garantir um fim definitivo ao processo nem prever suas conseqüências [*sic*].

Segundo Alves e Maciel (2020) As fake News é um problema bastante iminente em nossa sociedade, uma vez que as pessoas não estão dispostas a pesquisar se as informações sejam verídicas ou não, mas essas informações podem partir de meio que seja confiável como jornais ou revista, embora seja um pouco menos provável através das mídias jornalísticas, mesmo assim é possível que elas repassem informações falsas uma vez que possa ser notícias de cunho muito recente ou imediatas. Por outro lado, as redes sociais também propagam muita fake News uma vez que é possível criar páginas e perfis fake para fazer este tipo de manipulação e repassar essas informações. Segundo Delmazo (2018, p.166) “um dos caminhos que consideramos promissor é o corte de incentivos financeiros a páginas e perfis que disseminam notícias falsas”.

4.7 Tipos de redes sociais

As redes sociais englobam um nicho muito grande de plataformas online, na qual esses ambientes são bastantes diversificado, nas quais, cada um tem seus propósitos. Para Machado (2022), alguns exemplos de plataformas são:

- **Entretenimento**: estas aplicações estão bastante presentes no dia a dia. Por tanto, são plataformas dedicadas à distribuição de conteúdo que gera um entretenimento para o usuário. Um exemplo desses tipos de rede é o YouTube, Netflix entre outros. Essas plataformas englobam conteúdos com foco, em vídeos que podem ser, engraçados, notícias, filmes, entre outros tipos.
- **Relacionamentos**: as redes de relacionamento são plataformas bastante utilizada para quem está procurando um romance amoroso uma das plataformas mais conhecidas de relacionamento é o Tinder mas também pode-se considerar o Facebook como uma rede social de relacionamento uma vez que é possível conhecer e ter interação com pessoas de vários lugares.
- **Profissionais**: essas são redes voltas para uso mais profissional, ou seja, com elas você pode colocar seus trabalhos, especializações, currículos entre outros mais. Por tanto é possível pôr todo seu perfil profissional a fim de divulgar suas especialidades. Hoje é muito mais fácil aumentar a visibilidade profissional pela Internet e existem redes sociais que focam exclusivamente nisso, como é o caso do LinkedIn, áreas de atuação ou até mesmo atrair novos talentos para suas empresas.

5. CONSIDERAÇÕES FINAIS

É comum expor dados pessoais simples nas redes sociais, o que relativamente não causa nenhum transtorno. No entanto, quando uma violação de dados envolve a divulgação de acesso a contas bancárias, senhas de redes sociais, fotos etc., os dados ficam mais vulnerável a fraudes relacionadas a essas divulgações.

Portanto, essa monografia estuda e apresenta estratégias de segurança para evitar

a exposição de dados pessoais na Internet. Este trabalho trata de analisar como as redes sociais são uns dos pilares na prática de persuasão através da engenharia social, embora apresentar métodos de segurança da informação, desenvolvido com base nas pesquisas bibliográficas.

A pergunta desnorteadora para este trabalho é: será que é possível se sentir seguro ao usar a internet? a resposta é simples, a compreensão desse estudo está em estabelecer e demostrar práticas de engenharia social com o impacto direto na segurança de informações sigilosas. Demonstrar as melhores maneiras de manter uma boa privacidade de dados expostos à Internet em todos os momentos. Por tanto é necessário estabelecer melhores padrões de segurança, visando uma assimilação mais clara de técnicas contra-ataques cibernéticos nas internets e principalmente nas redes sociais online.

Referências

ALAZRI, "A consciência da engenharia social na revolução da informação: Técnicas e desafios," 2015. **10ª Conferência Internacional para Tecnologia da Internet e Transações Seguras (ICITST)**, 2015, pp. 198-201, doi: 10.1109/ICITST.2015.7412088. Disponível em: < https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7412088& />. Acesso em: 13 out. 2022.

ALVES, Marco Antônio Sousa; MACIEL, Emanuella Ribeiro Halfeld. **O fenômeno das fake news: definição, combate e contexto**. N. 1/V. 1. ed. Internet&sociedade, 1 fev. 2020. Disponível em: https://revista.internetlab.org.br/o-fenomeno-das-fake-news-definicao-combate-e-contexto/. Acesso em: 13 out. 2022.

AMARAL, Inês; SANTOS, Sofia José. Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade. **As fake news e a nova ordem (des) informativa na era da pós-verdade**, p. 63-85, 2019.

BELCIC, Ivan. **O guia essencial sobre phishing: Como funciona e como se proteger**. [*S. l.*]: Avast Academy, 5 fev. 2020. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em: 18 out. 2022.

BUOGO, Mateus; YANZER, Anderson; BASSO, Eduardo. Metodologias de gestão do conhecimento considerando melhores práticas para a segurança da informação. In: **Atas da Conferência da Associação Portuguesa de Sistemas de Informação**. 2017. p. 069-083.

DA SILVA, Washington Rodrigues; NOGUEIRA, Jorge Madeira. Ataques cibernéticos e medidas governamentais para combatê-los. **O Comunicante**, v. 9, n. 1, p. 42-57, 2019.

DELMAZO, Caroline; VALENTE, Jonas CL. Fake news nas redes sociais online: propagação e reações à desinformação em busca de cliques. **Media & Jornalismo**, v. 18, n. 32, p. 155-169, 2018

DIAS, Cristiane; COUTO, Olivia Ferreira do. As redes sociais na divulgação e formação do sujeito do conhecimento: compartilhamento e produção através da circulação de ideias. **Linguagem em (Dis) curso**, v. 11, p. 631-648, 2011.

DOS SANTOS AZEVÊDO, Adriano Valério; DA SILVA, Marcos Antônio; REIS, Tomás Collodel Magalhães. Promoção da saúde no contexto das redes sociais significativas. **Nova Perspectiva Sistêmica**, v. 28, n. 63, p. 55-66, 2019.

EC-COUNCIL, **Os incidentes de segurança cibernética estão explodindo.**

Assim como os trabalhos cibernéticos! Disponível em; < https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>. Acesso em: 08 nov. 2022

FERNANDES, Luís. Redes sociais online e educação: contributo do Facebook no contexto das comunidades virtuais de aprendentes. **Universidade Nova de Lisboa, Portugal**, 2011.

FILHO, Demócrito Reinaldo. **A responsabilidade dos bancos pelos prejuízos resultantes do "phishing"**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 13, n. 1836, 11 jul. 2008. Disponível em: https://jus.com.br/artigos/11481. Acesso em: 27 nov. 2022.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

GOIS, Alexsandro Barreto. Segurança Cibernética. **O Comunicante**, v. 8, n. 3, p. 40-47, 2018.

HOSTINGER, **O que é phishing e como se proteger de golpes na internet**, Disponível em: < https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet/> Acesso em: 11 out 2022

JÚNIOR, Augusto Wagner Menezes Teixeira; LOPES, Gills Vilar; FREITAS, Marco Túlio Delgobbo. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Carta Internacional**, v. 12, n. 3, p. 30-53, 2017.

MACHADO, FELIPE NERY RODRIGUES. **Segurança da informação: princípios e controle de ameaças**. Saraiva Educação SA, 2014.

MACHADO, Teca. **Os 4 tipos de redes sociais**. Albatroz|, 17 mar. 2022. Disponível em: https://editoraalbatroz.com.br/os-4-tipos-de-redes-sociais/. Acesso em: 16 out. 2022.

MARCIANO, João Luiz Pereira. **Segurança da Informação: uma abordagem social**. 2006.

MITNICK, D. K.; SIMON, L. W. Mitnick A arte de enganar. **Ataques de Hackers: controlando o fator humano na segurança da informação.Tradução:** Kátia Aparecida Roque. São Paulo: Pearson, 1963. Disponível em: <https://www.docdroid.net/Mq0Edkm/kevin-mitnick-a-arte-de-enganar-pdf#page=3/>. Acesso em: 23 out. 2022.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. Novatec Editora, 2007.

NETWORKS, Telium. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. [*S. l.*], 14 set. 2018. Disponível em: https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 20 out. 2022.

PARALLIS, **Tailgating: um desconhecido, porém perigoso, truque de engenharia social:** Pouco comentado quando falamos sobre a "arte de enganar", o tailgating pode permitir que um ator malicioso entre no perímetro físico de sua empresa. Disponível em: < https://www.perallis.com/news/tailgating-um-desconhecido-porem-perigoso-truque-de-engenharia-social/>. Acesso em: 10 nov. 2022.

PINHEIRO, José Maurício dos Santos et al. Ameaças e ataques aos sistemas de informação: Prevenir e antecipar. **Cadernos UniFOA**, v. 3, n. 5, p. 11-21, 2007.

PIOVESAN, Leonardo Gubert et al. ENGENHARIA SOCIAL: **Uma abordagem sobre Phishing**. REVISTA CIENTÍFICA UNIBALSAS, v. 10, n. 1, p. 45-59, 2019.

RECUERO, Raquel. A rede é a mensagem: Efeitos da Difusão de Informações nos Sites de Rede Social. **Lo que Mcluhan no previó. 1ed. Buenos Aires: Editorial La Crujía**, v. 1, p. 205-223, 2012.

REULE, Danielle Sandri. **A dinâmica dos rumores na rede: a web como espaço de propagação de boatos virtuais**. 2008.

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. **Análise de redes sociais aplicada à engenharia Social**. 2012.

ROSA, Adriano Carlos. Engenharia Social: O elo mais frágil da Segurança nas empresas. **Revista Brasileira de Contabilidade e Gestão**, v. 1, n. 2, p. 29-40, 2012.

SÁ, André Luiz Nery de. **Segurança cibernética de usinas nucleares:** uma análise sobre medidas de mitigação de ataques de engenharia social na central nuclear Almirante Álvaro Alberto. 2020.

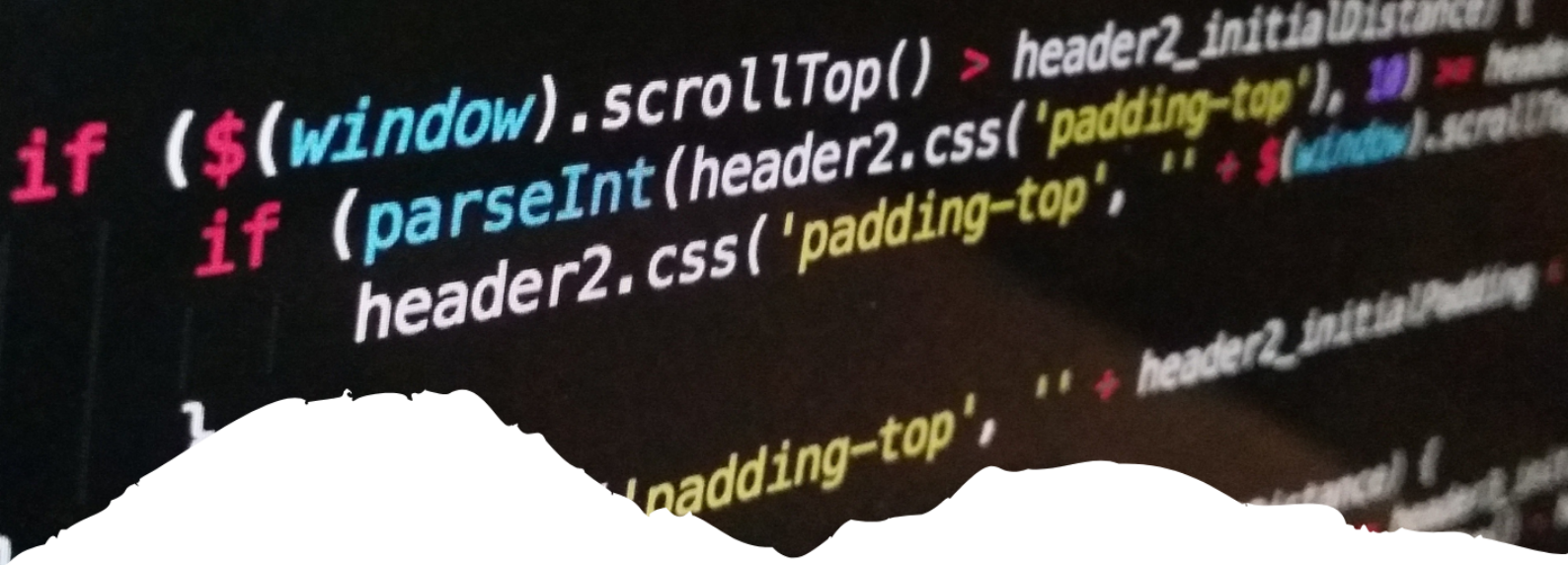
SILVA, Narjara Bárbara Xavier; ARAÚJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Informação**, v. 6, n. 2, 2013.

SOUSA, João Catarino de. **Typhon: um serviço de autenticação e autorização tolerante a intrusões**. 2010. Tese de Doutorado.

TAVEIRA, Danilo Michalczuk et al. **Técnicas de defesa contra spam**. Sociedade Brasileira de Computação, 2006.

VENTURA, Ivan. Smishing: você tem uma nova mensagem (maliciosa): Smishing se tornou um dos principais tipos de golpes para o envio de links maliciosos e, assim, obter dados pessoais. **Entenda**. [*S. l.*], 4 abr. 2022. Disponível em: < https://www.consumidormoderno.com.br/2022/04/04/smishing-mensagem-maliciosa/>. Acesso em: 13 out. 2022.

WEB SITE SECURITY STORE, **O que é um ataque de Vishing? 7 exemplos de phishing de voz**: Disponível em: < https://websitesecuritystore.com/blog/what-is-voice-phishing-and-vishing-attack/> Acesso em: 12 out. 2022.



7

DESENVOLVIMENTO DE UM PROTOTIPO MOBILE PARA GERENCIAMENTO NA CUNICULTURA

DEVELOPMENT OF A MOBILE PROTOTYPE FOR MANAGEMENT IN RABBIT FARMING

Leonardo Farias Dias

Resumo

Este trabalho se propõe a um protótipo para uma aplicação *Mobile*, baseado em sistema híbrido, para armazenar informações oriundas de um centro de cunicultura, onde o produtor irá cadastrar seu animal (coelho) para que faça um controle de sua reprodução. Estes registros serão utilizados para a consulta de informações, com o objetivo de fazer alguns prognósticos a cerca de uma próxima reprodução, que poderão ajudar no gerenciamento do coelho. Para tal foi utilizado o Ionic Framework, nos permite experiências agradáveis na programação, e nos disponibiliza recursos que tornam mais simples, a estrutura necessária para o desenvolvimento da aplicação *Mobile*. O objetivo desta aplicação será guardar informações da produção, onde produtor terá um melhor gerenciamento de sua produção, que serão disponibilizadas através de pesquisa para quem tiver acesso ao sistema.

Palavras-chave: Confiabilidade, Funcionalidade, Usabilidade, Eficiência.

Abstract

This document proposes a prototype of a mobile application based on a hybrid system for the storage of information of a center of rabbits, where the producer will register his animal (rabbit) to make a control of reproduction. These records are used to query information in order to make some predictions about a closed play, which can help in managing the rabbit. For this we use the ionic framework allows us pleasant experiences in programming, and offers features that make it simple, the infrastructure necessary for the development of mobile applications. The purpose of this application will store the production information, where the producer will have a better management of their production, which will be made available by the search of those who have access to the system.

Keywords: Reliability, Functionality, Ease Of Use, Efficiency.

1. INTRODUÇÃO

A utilização de computadores está presente em diversas atividades do nosso cotidiano. Num simples toque no celular para ouvir música ou até mesmo para gerenciamento de hospitais, bancos, escolas, aeroportos. É uma tarefa quase impossível descrever todos os possíveis usos que se pode dar a um computador.

A aplicação mobile surgiu com os dispositivos móveis(smartphone) em 1992 com o Simon da IBM, que tinha como recurso o PDA, tela sensível ao toque. Dez anos depois a empresa Kyocera lançou QCP 6035 que tinha como seu principal recurso mesclar funções de celular e de computador e usava sistema operacional Palm OS, e possuía conexão com a internet no mercado. Com isso trouxe um grande avanço para o desenvolvimento de aplicativos que são software[3] que desempenham objetivos específicos em smartphone ou tablete.

É imprescindível a contribuição de computadores voltados para a área da agropecuária, pois estes são vetores que contribuem para um melhor aproveitamento e aumento da produtividade. Para que possa ser disseminada nesta área, a utilização desta ferramenta deve conseguir ultrapassar as opiniões contrarias ao seu emprego. Segundo Costa (2004), podem ser elas: a aversão por parte dos produtores em aceitar novas tecnologias; e também, está relacionada a dificuldades em possuir capital disponíveis para a obtenção desta tecnologia.

No Brasil, a cunicultura é pouco desenvolvida quando comparada aos demais países. Contudo, está proporciona um retorno financeiro rápido ao investidor, tendo em vista que possuir um curto ciclo financeiro, e possibilita o aproveitamento de diversos produtos oriundos do processo produtivo.

Este trabalho tem como objetivo mostrar as etapas de uma criação de um aplicativo híbrido utilizando framework ionic, para o desenvolvimento de um protótipo na da cunicultura.

Todo e qualquer atividade produtiva, precisa ter controle zootécnico. Na cunicultura, é importante a realização do controle reprodutivo e para realizar melhoramentos genéticos bem como evitar consanguinidade e transmitir transparência ao vender animal e fornecer a árvore genealógica. No entanto, esse controle pode ser realizado pelo próprio produtor através de cadernos e fichas impressas, como é constantemente feita por pequenos produtores, ou em casos mais avançados com ajuda de softwares específicos. Este acompanhamento é fundamental para o processo e otimização da produtividade.

Apesar do grande salto tecnológico observado no setor produtivo como um todo, esse desempenho excepcional da pecuária não tem sido uniforme, pois, vários produtores ainda enfrentam dificuldades em usufruir de soluções tecnológicas para o melhor aproveitamento da criação.

Portanto, em decorrência destas dificuldades em desfrutar de tecnologia, este trabalho tem como objetivo apresentar um protótipo que possa melhorar a organização de dados do Centro de Cunicultura da Universidade Estadual do Maranhão localizada em São Luís.

Tendo como objetivo geral: Desenvolver um protótipo para facilitar o gerenciamento da produção no setor da cunicultura e inovação tecnológica: as necessárias distinções e seus impactos na atualidade. E como objetivos específicos ou secundários: Garantir a consistência de dados; Garantir a consulta de informações com rapidez; Padronização de dados e Realizar melhor controle de desempenho individual.

Como metodologia de pesquisa foi utilizada com o intuito de alcançar o objetivo proposto, a pesquisa utilizada caracteriza-se como exploratória. Desenvolvida através de fundamentos bibliográficos encontrado em dados de artigos publicados, monografias, sites referentes ao tema e livros, pois se trata de um tema pouco difundido no ambiente acadêmico.

2. CUNICULTURA

A cunicultura segundo Garcia (2006) e Rios et al. (2011) é o ramo da Zootecnia que trata da criação racional e econômica de coelhos. Dependendo dos objetivos da criação, a cunicultura pode ser direcionada para a produção de carne, pele (ou pelos) ou ainda para o uso como cobaias em laboratório.

Machado (2012) retrata que a cunicultura se identifica por uma atividade estratégica devido a múltiplas características dentre elas, ser uma atividade sustentável. De acordo com Garcia (2006) e Sordi et al. (2013), esta atividade produz grande quantidade de alimentos de alta qualidade nutricional, elevada produtividade, baixa necessidade de água, baixo impacto ambiental e possibilita o aproveitamento de subprodutos.

Outra vantagem da cunicultura, é que o animal pode ser aproveitado e comercializado quase em sua totalidade. Além da carne, pele e pelos, é possível a comercialização de outras partes, como: cérebro, orelhas, carcaça, esterco e sangue (SILVA, 2006).

Assim, a cunicultura é uma atividade bastante viável ao produtor que pode implantar criações intensivas para gerar uma fonte de renda familiar ou uma pequena criação na propriedade para consumo próprio da carne, que é de ótima qualidade. No entanto, para que se torne uma exploração viável, a criação exige alguns cuidados que devem ser observados pelo cunicultor, principalmente os relacionados às matrizes, aos filhotes e ao controle sanitário (GARCIA, 2006; SIMONATO, 2008).

3. SISTEMAS HÍBRIDOS

3.1 Conceitos e Estrutura

Nesse capítulo será abordado todos os conhecimentos adquiridos para desenvolvimento da aplicação hibrida, sendo eles sistema híbridos, ionic framework e o levantamento de requisito.

Rodrigues (2015) afirma que aplicativos híbridos são construídos como são construídas as páginas web. Ambos usam uma combinação de tecnologias como HTML, CSS e Javascript. Contudo, uma página web será executada no celular, enquanto um aplicativo híbrido será executado dentro de uma WebView que é um componente nativo do sistema operacional, seja ele Android, iOS ou outros.

De acordo com. Rodrigues (2015) hoje em dia a maioria das aplicações utilizam o projeto Cordova uma plataforma que consiste em um conjunto de APIs JavaScript para acessar o hardware do celular através de plugins que são escritos em código nativo.

Umas das vantagens de utilizar uma aplicação hibrida é multiplataforma, tem baixo curva de aprendizado, custo de desenvolvimento mais barato, tempo de desenvolvimento curto e poder ter acesso de recurso nativo (câmera, lanterna e GPS). Porém no aspecto de desempenho não é muito recomendado, pois são utilizadas webviews, que são browsers

embutidos no aplicativo, perdendo a fluidez dos apps nativos.

3.2 Ionic framework

Ionic framework é uma ferramenta Open Source para desenvolvimento de aplicações hibridas para multiplataformas, surgiu em 2012 pela empresa norte americana DriftyCo e que tem como objetivo de permitir que os desenvolvedores criem aplicativos melhores como menor tempo utilizado.

O Ionic é desenvolvido com base em tecnologias controladas e padronizadas da Web: HTML, CSS e JavaScript, usando APIs da Web modernas, como Custom Elements e Shadow DOM. Por causa disso, os componentes Ionic têm uma API estável e não dependem de um único fornecedor de plataforma. Com isso o Ionic foi desenvolvido com a simplicidade em mente, para que a criação de aplicativos seja agradável, fácil de aprender e acessível a praticamente qualquer pessoa com habilidades de desenvolvimento web.

Para que possa utilizar o ionic, devemos instalar uma plataforma de criação web, para isso deve ser feito o download do Node.js como mostra na figura 1.

Figura 1: Página para download do Node.js.

Fonte: O autor (2022)

Depois de instalar do Node.js, o desenvolvedor deverá executar Command Prompt se estiver usando sistema operacional Windows ou Terminal do Linux ou do Mac para instalar o pacote do Cordova e o NPM gerenciador de pacotes do Node.js como mostraremos na figura 2.

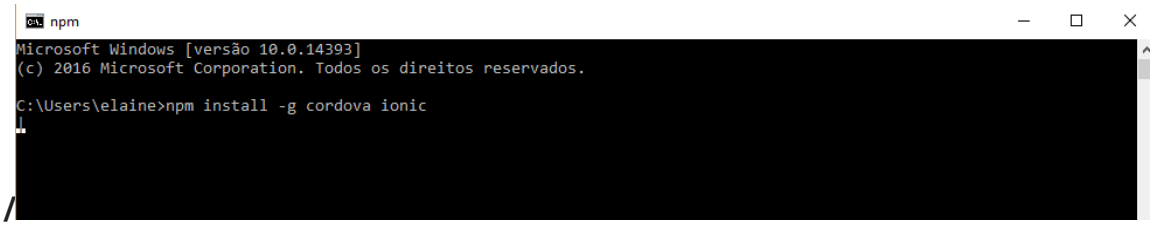


Figura 2: Instalação do gerenciador NPM e pacote Cordova.

Fonte: O autor (2022).

Na figura 3 será mostrado como criar uma aplicação hibrida já utilizando ionic. O comando ionic start criará uma pasta chamada MeuPrimeiroApp contendo o projeto, o sidemenu será o template do aplicativo. É importante salientar que é necessário ter conexão com a internet, pois o ionic vai baixar e instalar os recursos necessários para a nossa aplicação (FELQUIS, 2016).

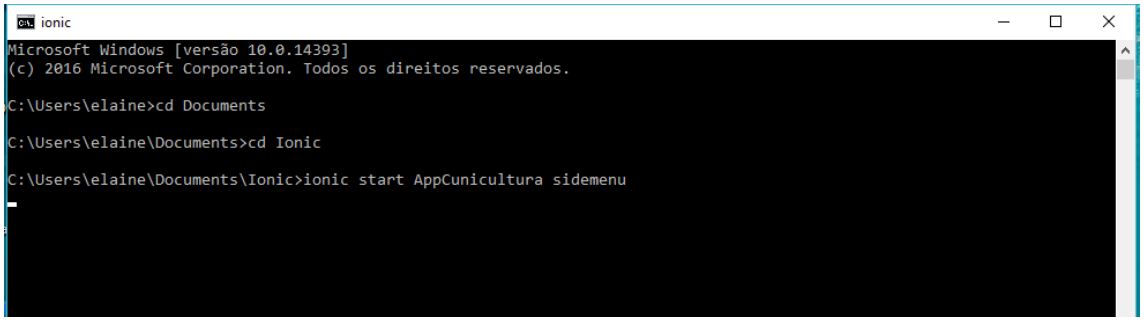


Figura 3: Criando o aplicativo AppCunicultura.

Fonte: O autor (2022).

4. LEVANTAMENTO DE REQUISITO E ESTRUTURA DO PROTÓTIPO DA CUNICULTURA

O levantamento de requisito tem como objetivo o desenvolvimento de software é a criar sistemas que correspondam às necessidades de cliente e usuários. Uma especificação correta dos requisitos do software é essencial para o sucesso do desenvolvimento. Mesmo tenha sido bem projetado e codificado, se ele foi mal especificado, certamente irá desapontar o usuário e causar desconforto à equipe de desenvolvimento, que terá de modificá-lo para se adequar às necessidades do cliente (VASCONCELOS, 2006).

Segundo Sommervill (2011, p.83) sugere que o requisito é tratado como “funcional quando descreve um serviço ou função que o sistema deve realizar”. Paralelamente pode haver requisitos não funcionais, que são restrições impostas tanto ao sistema quanto ao seu desenvolvimento, sendo as ferramentas utilizadas: uml e diagrama de caso de uso.

4.2 Diagrama de caso de uso

Analisando o projeto sobre expectativa do diagrama de caso de uso observa-se uma maior interação com usuário e desenvolvedor, pois possibilita demostrar a funcionalidade da aplicação. Na primeira interação entre usuário e sistema será incluído um controle de acesso feito por uma tela de *login*, onde apenas os que tiverem acesso ao sistema por meio de usuário e senha poderão utilizar o mesmo, possibilitando cadastrar, atualizar e excluir o animal no banco de dados, fazer consulta dos dados do animal e por fim cadastrar as informações da sua reprodução, como demostrado na figura 5.

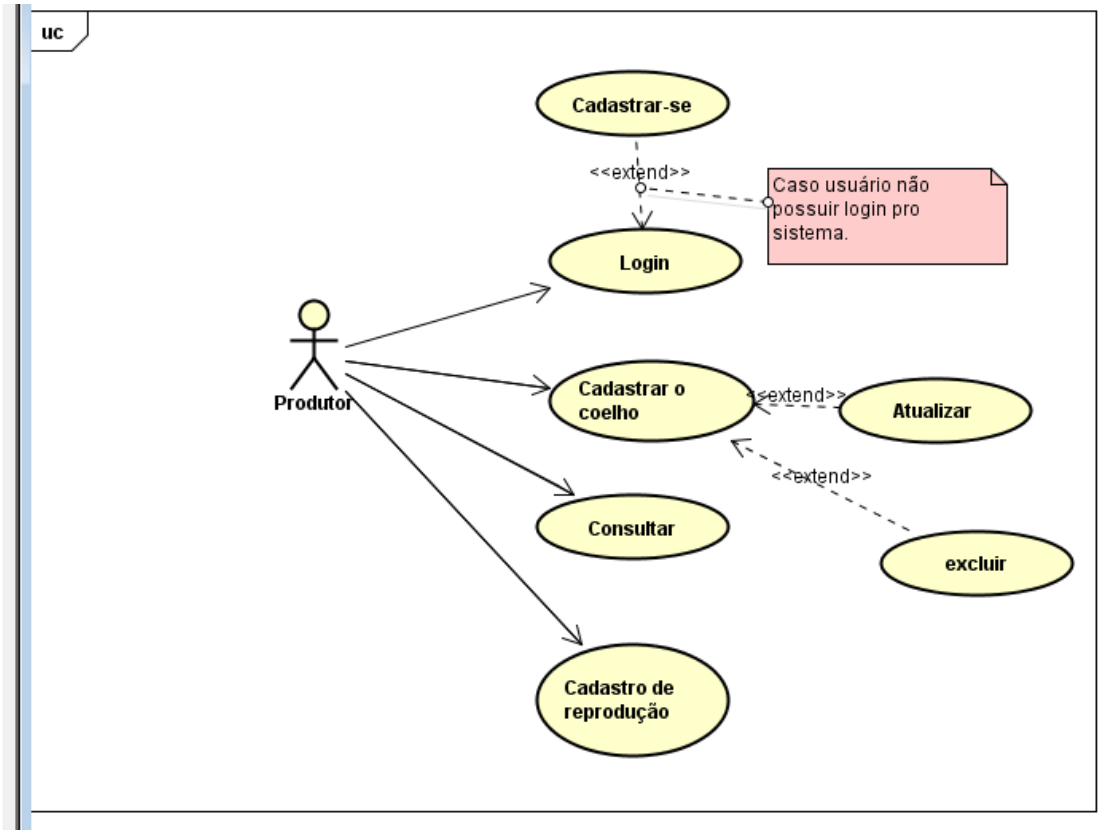


Figura 5: Diagrama de Caso de Uso

Fonte: O autor (2022)

4.3 Protótipo

A seguir serão mostradas algumas imagens ilustrativas dos protótipos do sistema, começando pela tela de login. Tela que é responsável pelo controle de acesso da aplicação. Procuramos aplicar um *layout* bem intuitivo para que não canse seus usuários e mais didático.

Aqui o usuário (Produtor) vai informar seu login para acessar o sistema, caso não tenha ainda irá na opção de se cadastrar, onde vai informar seus dados pessoais.

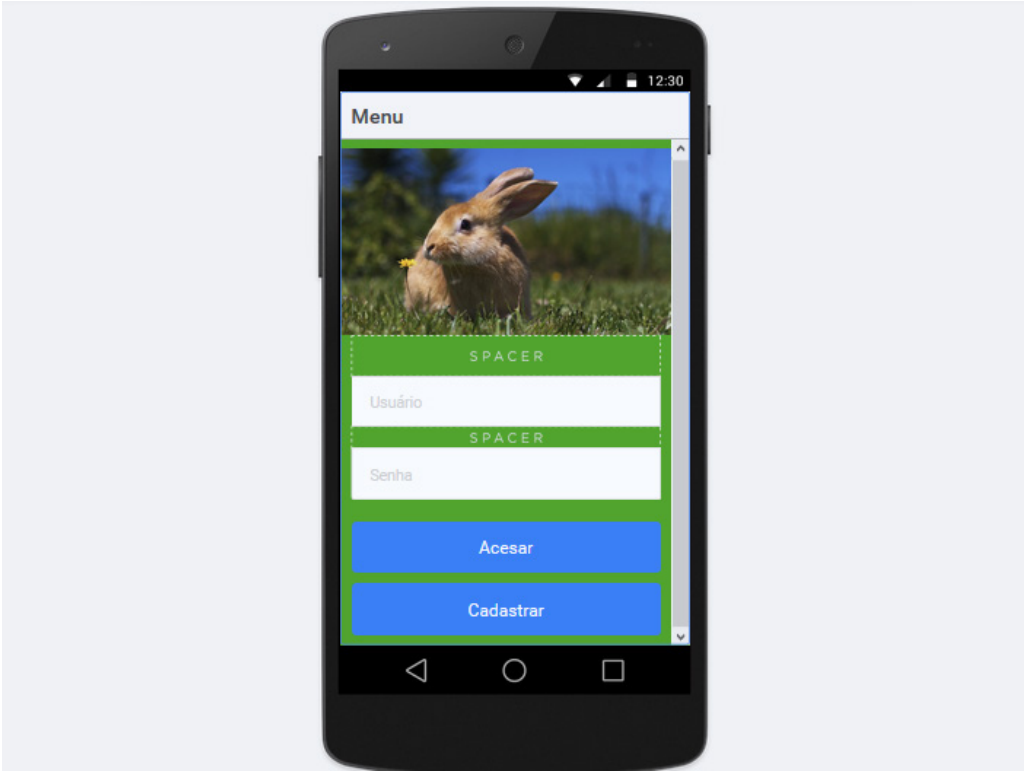


Figura 6: Imagem ilustrativa para acesso ao sistema.

Fonte: O autor (2022)

Na figura 7 demostra uma tela de cadastro do animal (coelho), onde o usuário vai ter umas opções de escolher raças, sexo, pelagem, e em seguida vai informar a data de nascimento do animal. Após informar as características irá salvar os dados no banco de dado.

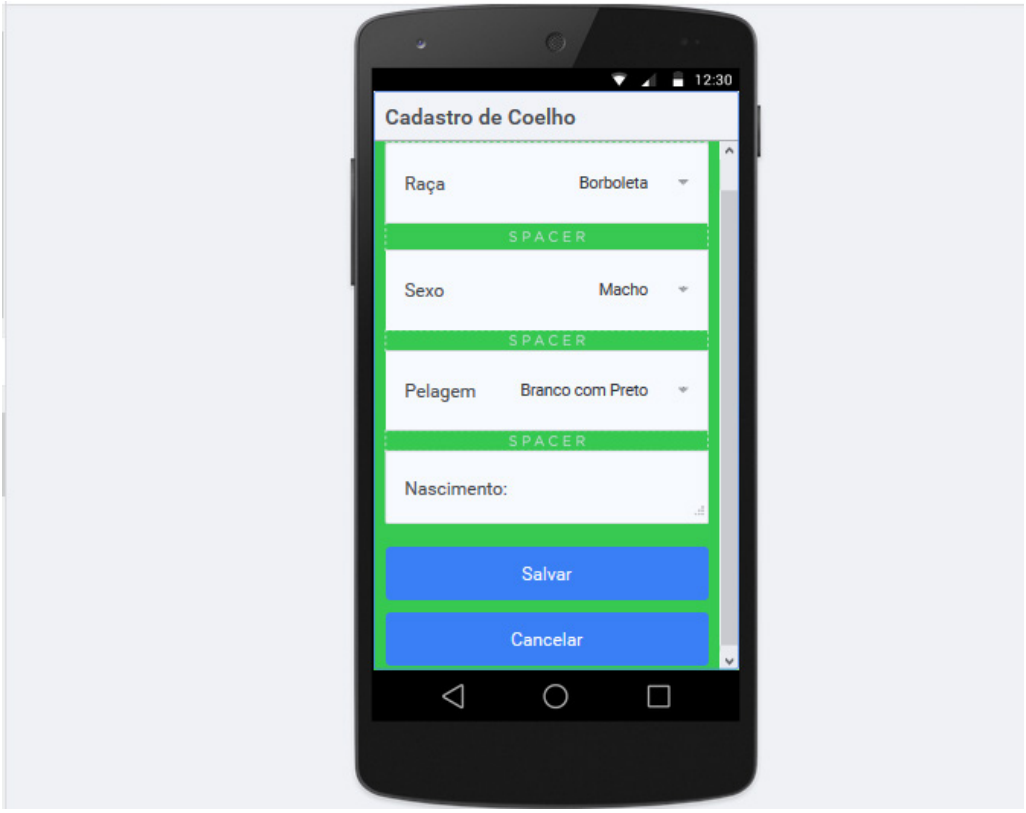


Figura 7: Imagem ilustrativa para o cadastramento do animal no sistema.

Fonte: O autor (2022)

Os dados da reprodução serão escritos nos campos informando os dias de cobertura (acasalamento), o horário e o reprodutor a ser usado. Onde o produtor obterá dados específicos para facilitar o manejo durante a vida produtiva dos animais. Já o campo parição é destinado a informações sobre o dia em que haverá (ou não) a parição da matriz como é apresentado na figura 8.

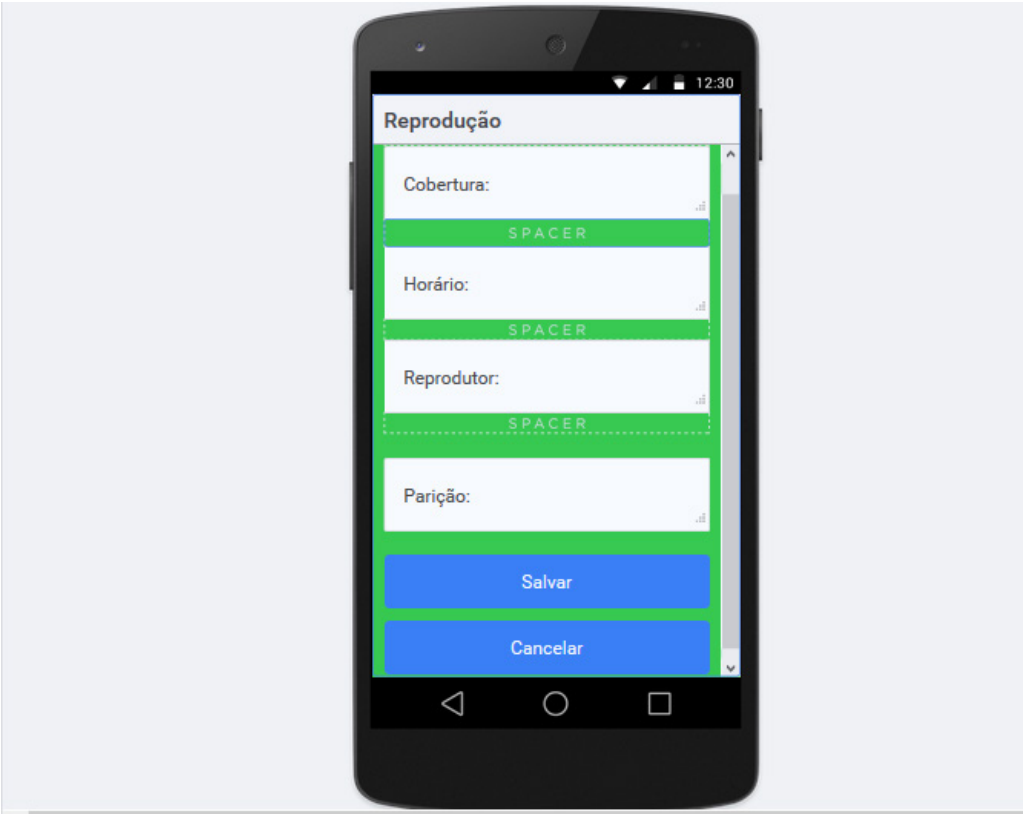


Figura 8: Imagem ilustrativa para reprodução do animal no sistema.

Fonte: O autor (2022)

5. CONSIDERAÇÕES FINAIS

O objetivo do protótipo é desenvolver uma aplicação para controle de reprodução de coelhos, é melhorar e facilitar o gerenciamento de reprodução uma cunicultura, visando a prosperidade na geração de coelhos, coletando suas informações especificas para estudos e diagnósticos futuros.

A importância de uma aplicação voltada para cunicultura é trazer mais a tecnologia para agropecuária, aprimora ainda mais os avanços em laboratórios que utilizam os coelhos como cobaia, ou até mesmo para estudos sobre sua biodiversidade, além da ajuda para organização de um produtor de coelhos, tendo assim uma forma mais detalhada sobre as características de cada coelho.

Portanto, com a utilização desses recursos desenvolvidos pela aplicação, terá rapidez nos procedimentos, uma estatística dos dados coletados muitos mais elaborados e organizados, um controle muito mais eficiente, além de colaborar com a biodiversidade para que não haja impacto na diminuição da espécie, e estudo com mais exatidão a um prazo bem menor.

Resumidamente, o foco é agilizar e aprimorar de forma mais precisa o controle de reprodução do mesmo, e pensando posteriormente em possíveis estudos utilizando esta

aplicação para tratamentos de doenças humanas com base de estudo nos coelhos utilizados como cobaias, ou até mesmo, procedimentos de mutação genética.

Referências

COSTA, Grin Miranda. **A Informática na Agricultura**, 2004. Disponível em: <http://www.zemoleza.com.br/trabalho-academico/exatas/informatica/a-informatica-na-agricultura/>. Acesso em 17 de agosto de 2022.

FERREIRA, R. C.; SILVA, R. A.; VIANA, E. P. T.; FILHO, N. T. A. Alimentação alternativa para coelhos à base de rami (*Boehmeria nivea*) e palma (*Opuntia* fícus). **Revista Verde de Agroecologia e Desenvolvimento Sustentável.;** Mossoró, v.4, n.3 p.61 – 69, jul/set, 2009.

GARCIA, Edson Marcelo Gonçalves. **O que é cunicultura**. [S.l.], [200-?]. Disponível em: http://pessoal.portoweb.com.br/clanalcateia/artigos/Cunicultura/cunicultura.htm. Acesso em: 10 set. 2022.

GÓMEZ, E. Producción industrial de gazapos: algunos puntos críticos. **XXXI Symposium de Cunicultura,** Espanha, Lorca, v.1, n.1, p.201-214, 2006.

MACHADO, L. **Opinião: Panorama da cunicultura Brasileira.** Revista Brasileira de Cunicultura, v.2, n. 1, Setembro de 2012. Disponível em <http://www.rbc.acbc.org.br/index.php?option=com_content&view=article&id=63&Itemid=71>. Acesso em 17 de set. 2022.

RIOS, Daniel Macedo *et al***. Manual de cunicultura**. 2011. 46 f. Trabalho acadêmico (Graduação em Engenharia Agronômica) – Universidade do Estado da Bahia, Barreiras, 2011. Disponível em: <http://pt.scribd.com/doc/49387002/cunicultura>. Acesso em: 19 jul. 2022.

RODRIGUES, Paulo André Alves. **Cunicultura: um estudo sobre a aplicação da contabilidade de custos voltada aos pequenos empresários.** 2007. 67 f. Trabalho de conclusão de curso (Graduação em Ciências Contábeis) – Faculdade de Economia, Administração, Contabilidade e Atuária, Pontifícia Universidade Católica de São Paulo, São Paulo, 2007. Disponível em: http://www.coelhoecia.com.br/Zootecnia/Cunicultura%20um%20Estudo%20Sobre%20a%20Aplicacao%20da%20Contabilidade%20de%20Custos%20Voltada%20aos%20Pequenos%20Empresarios.pdf> Acesso em: 16 jun. 2022.

RODRIGUES, PAULO, **Arquitetura de uma aplicação híbrida,** 2015, Disponível em:< http://legendas-z.com/arquitetura-aplicacao-hibrida/>. Acesso em 01 de nov. 2022.

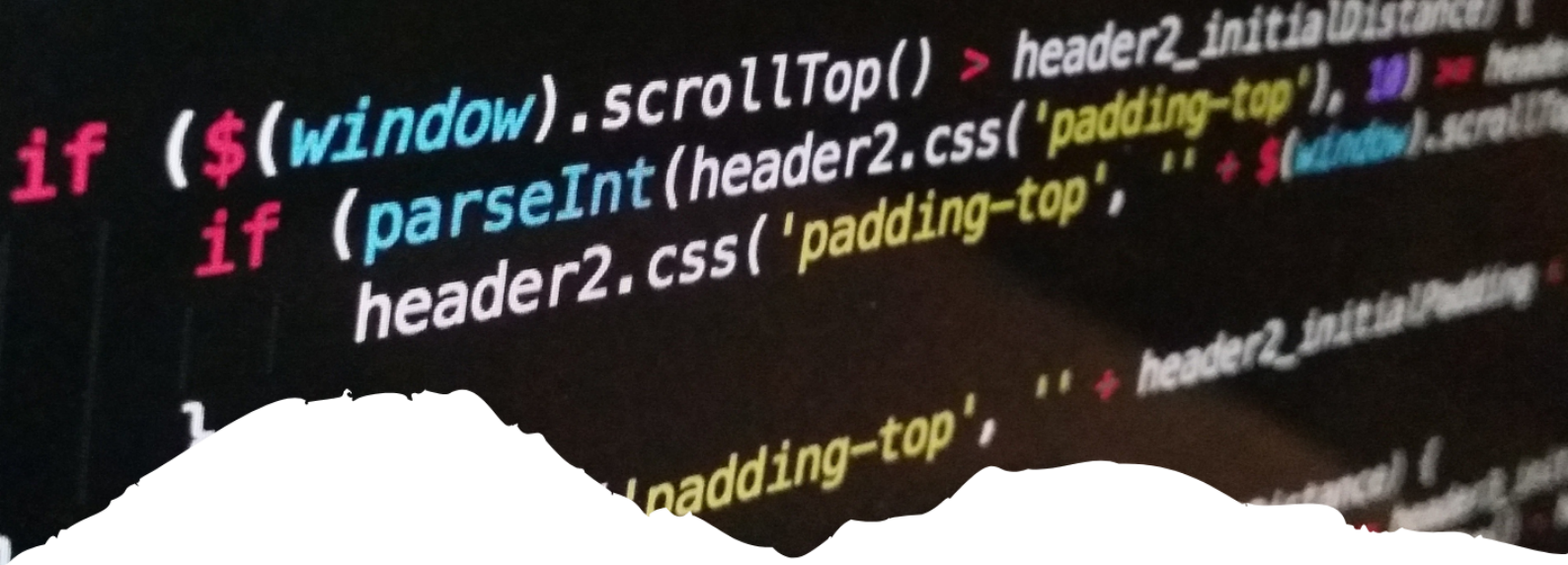
SCAPINELLO, C.; FALCO, J. E.; FURLAN, A. C.; FARIA, H. G. de. Desempenho de coelhos em crescimento alimentados com diferentes níveis de feno da rama da mandioca (Manihot esculenta Crantz). **Ciência Rural**, Santas Maria, v.30, n.3, p.493-497, 2000.

SILVA, Roberto de Andrade. **Cunicultura**. Curitiba: Secretaria de Estado da Agricultura e do Abastecimento, 2006. Disponível em: <http://www.agricultura.pr.gov.br/modules/qas/uploads/143/coelhos_julho2006.pdf>. Acesso em: 25 jul. 2022.

SORDI, V. F.; ROSA, C. O.; MARTINS, V. N. A cunicultura na estratégia de diversificação em propriedades rurais. **I Simpósio de Redes de Suprementos e Logísticas.** Universidade Federal da Grande Dourados, 2013.

SOMMERVILLE, Ian. **Engenharia de *Software***. 11. ed. São Paulo – SP: Pearson Addison Wesley, 2011.

WAGNER, FRANCIS, **Ionic Framework**,2015, Disponível em:<http://netcoders.com.br/blog/criando-aplicativos-hibridos-com-ionic-framework> Acesso em 01 de nov.2022.



8

A INCLUSÃO DA I.A NO DESENVOLVIMENTO DA APRENDIZAGEM DOS EDUCANDOS

THE INCLUSION OF AI IN THE DEVELOPMENT OF STUDENTS' LEARNING

Thamyres Mikaelly dos Santos Conceição

Resumo

O presente trabalho mostrar a importância da implantação da tecnologia no ambiente escolar e como ele pode auxiliar na aprendizagem dos educandos, mostrando seus benefícios e como deve ser utilizada para criar um ambiente de ensino mais eficaz e com maior taxa de aprendizado entre os alunos utilizando as tendências tecnológicas que o mundo globalizado fornece para uso em salas de aulas, auxiliando os professores na sua didática de ensino e preparação de atividades com o propósito de ministrarem aulas em que os educandos tenham a possibilidade de maior interação com os assuntos abordados. Identificar as áreas da inteligência artificial que podem ser implementadas dentro do ambiente escolar se torna essencial para o ambiente escolar, pois desta forma, todo o corpo docente da escola pode se qualificar para iniciar as práticas de ensino com auxílio da inteligência artificial, de forma a proporcionar melhores qualidades de ensino com um ambiente inovador e interessante para os alunos.

Palavras-chave: Inteligência Artificial. Educação. Aprendizagem. Inclusão. Crianças.

Abstract

The present work shows the importance of implementing technology in the school environment and how it can help students learn, showing its benefits and how it should be used to create a more effective teaching environment with a higher rate of learning among students using the technological trends that the globalized world provides for use in classrooms, helping teachers in their teaching didactics and preparation of activities with the purpose of teaching classes in which students have the possibility of greater interaction with the subjects covered. Identifying the areas of artificial intelligence that can be implemented within the school environment becomes essential for the school environment, because in this way, the entire school faculty can qualify to start teaching practices with the aid of artificial intelligence, in order to provide better teaching qualities with an innovative and interesting environment for students.

Keywords: Artificial intelligence. Education. Learning. Inclusion. Children.

1. INTRODUÇÃO

Com a utilização do computador na educação dos alunos no decorrer dos últimos anos foi possível observar-se que o mesmo tem se demonstrado ser um grande aliado ao aprendizado dos educandos, pois, desta forma o interesse dos alunos tem aumentado com relação aos estudos desenvolvidos em sala de aula juntamente aplicado ao uso das novas tecnologias de aprendizagem, e consequentemente o rendimento das crianças tem acompanhado o mesmo ritmo de desenvolvimento.

O aumento significativo das tecnologias no mundo tem chamado grande atenção para a área associada a educação, visando apresentar como a inclusão das aplicações da Inteligência Artificial na educação é capaz de auxiliar de forma significativa o aumento dos níveis de aprendizagem do ensino ministrado pelos professores no ambiente escolar.

O ensino é de fundamental importância na formação do indivíduo em sociedade, mas sua ausência é maléfica. Tendo em vista a relevância do ensino não apenas para os educandos, mas também para a sociedade é indispensável garantir um ensino de qualidade. A falta de acesso a uma educação de qualidade fortalece o ciclo da desigualdade social.

No presente trabalho concluiu-se que houve a estimulação da aprendizagem das crianças na fase inicial, com o auxílio das novas tecnologias inclusivas e interativas de forma com que os educandos obtiveram resultados de aprendizagem significativas e ao mesmo tempo prazerosa, os alunos também foram capazes de desenvolver suas competências e habilidades de forma mais rápida. Assim a presente pesquisa visa responder a seguinte questão: Quais tecnologias são capazes de proporcionar ao educando uma forma mais eficiente e dinâmica de absorção do conteúdo abordado?

O objetivo principal desta monografia é de destacar que através da utilização da IA as práticas de ensino se tornam mais eficientes e capazes de auxiliar na aprendizagem os alunos, suas vantagens e contribuições na educação, de forma que as tecnologias foram capazes de proporcionar aos alunos melhor qualidade e absorção dos conteúdos e aumentando os seus níveis de aprendizagem e ainda sendo capaz de auxiliar os professores nas suas práticas de ensino de modo personalizado, focando no aprendizado individual de cada criança de modo eficiente e dinâmico.

O tipo de pesquisa que será realizado nesse trabalho é a revisão de literatura. Serão apresentados os conceitos necessários para uma melhor compreensão do tema abordado, visando alcançar reflexões para compreender como a inteligência artificial contribui de forma significativa para melhorar a educação. Desta forma, serão discutidos, os Conceitos de inteligência artificial, as Vantagens da utilização da inteligência artificial na educação e, por fim, serão expostas as Práticas de ensino no ambiente intuitivo

2. O QUE É INTELIGÊNCIA ARTIFICIAL?

A definição de inteligência artificial é um conceito muito aberto e que os cientistas ainda não conseguiram entrar em consenso, pelo fato de suas vastas aplicabilidades e inovações em diversas áreas do dia a dia das pessoas, tais como a área da saúde como os softwares de auxílio a diagnósticos médicos, na área industrial com softwares que auxiliam na verificação de gastos de produtos e lucros, na área educacional com os tutores inteligentes, entre outras. Ainda assim o conceito mais concreto que temos é que a inteligência artificial tem a capacidade de assemelha ou “imitar” o comportamento que um ser huma-

no teria, como citado por Silva e Mairink (2019, p. 65):

> A Inteligência artificial, resumidamente, é a possibilidade de uma máquina, através de algoritmos, possuir capacidade cognitiva semelhantes ao de um ser humano; com isso pode realizar atividades que antes apenas o homem era capaz. Aplicado ao direito, pode desempenhar todo o trabalho repetitivo e maçante de forma ininterrupta.

O termo inteligência artificial ou I.A, como estamos acostumados a ouvir faz referência principal a função de uma máquina imitar ou se assemelhar ao comportamento que um ser humano teria, de modo que, a máquina consiga realizar tarefas de maneira considerável inteligente, e tão bem ou até mesmo melhor que o próprio ser humano. Como citado por Silva e Mairink (2019, p. 67):

> A Inteligência artificial, também conhecida como IA, é um ramo da ciência que visa, por meios tecnológicos, ser capaz de simular a inteligência humana; podendo resolver problemas, criar soluções e até mesmo tomar decisões no lugar do ser humano, como um auxílio que facilitaria em diversas áreas do cotidiano.

Uma solução de I.A engloba várias tecnologias, como por exemplo as redes neurais artificiais, os algoritmos e sistemas de aprendizados, simulando capacidades humanas ligadas à inteligência. A rede neural é treinada com as bases de dados que o usuário insere, deste modo é realizado o reconhecimento das informações, onde ela consegue aprender de acordo com os dados que foram inseridos na máquina, por exemplo, a rede neural consegue reconhecer um cachorro e um gato de acordo com as suas características, após a realização de algumas análises que foram capazes de apontar diferenças entre os dois animais (OLIVEIRA, 2022). Tudo teve início antes de 1949, quando os primeiros computadores já eram capazes de realizar comandos simples com auxílio de um usuário, mas, por conta de a máquina não ter como armazenar aqueles comandos ela não conseguia lembrar a tarefa que havia acabado de realizar, mostrando um grande problema aos cientistas. Como citado por Oliveira (2022, p. 177):

> Em 1990 uma revolução transformou a metodologia da IA. Uma nova abordagem baseada em redes neurais permitiu a construção de programas capazes de aprender. As redes neurais, inventadas na década de 1950 e inspiradas no funcionamento dos neurônios biológicos, tiveram um renascimento após terem sido esquecidas no período da IA simbólica. Curiosamente foram os chips desenvolvidos para processamento de videogames que permitiram a construção de redes neurais com milhares de componentes interligados. Novos algoritmos matemáticos utilizando essas unidades de processamento gráfico consolidaram a abordagem que passou a ser conhecida como machine learning – aprendizado de máquina.

No ano de 1950, o grande matemático e considerado pai da computação Alan Turing levantou o questionamento sobre como criar máquinas inteligentes e testar esta inteligência em seu estudo COMPUTING MACHINERY AND INTELLIGENCE (Máquinas computacionais e inteligência), como mencionado por Baranauskas (1999, p. 45):

> Os primeiros usos do computador em Educação surgiram ainda no final da década de 50 e representavam as possibilidades tecnológicas da época. Ao

mesmo tempo, devemos observar que os paradigmas de aprendizado embutidos nesses sistemas, isto é, a maneira de entender o ensino/aprendizado, refletem e situam o contexto educacional vigente na época.

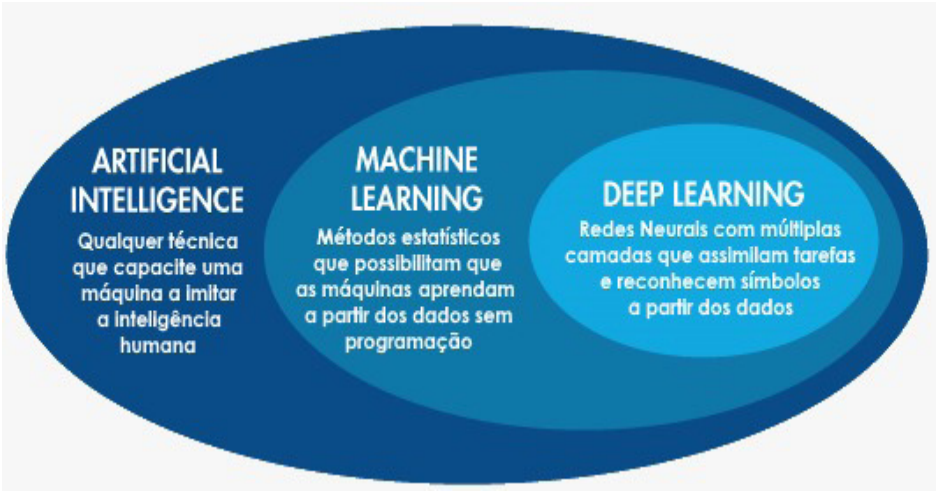


Figura 1– Definição de Inteligência artificial, Machine learning, Deep learning

Fonte: Lavagnoli (2019).

O machine leargin são criações da ia que estão dedicadas na criação de algoritmos que são capazes de permitir que os sistemas consigam aprender sem a intervenção humana, ou seja, de maneira autônoma. O Deep Leargin tem seu foco na criação de sistemas que imitam o cérebro humano de maneira artificial, um grande exemplo são as redes neurais artificiais que são capazes de se adaptar e aprender com grandes volumes de dados. Como citado por Damaceno e Vasconcelos (2018, p. 13):

> Estudos atuais na área de Inteligência Artificial, Machine Learning e Deep Learning andam de mãos dadas e podem ser categorizados em esferas. No centro está o Deep Learning, abrangendo esta, a esfera do Machine Learning e por fim a camada da Inteligência Artificial englobando-as. A relação entre Deep Learning e Machine Learning pode ser entendida com o Deep Learning, substituindo a intervenção humana, como já citado, para prover dados de entrada para o Machine Learning. Isso torna expressamente claro que o conceito de Deep Learning é herdado do Machine Learning.

Os conceitos de machine learning são especificados de acordo com Bertozzo (2019, p. 22):

> Sistemas de machine learning ou aprendizado de máquina são sistemas que aprendem a partir dos dados e que pretende tomar decisão com o mínimo de intervenção humana, uma opção muito interessante e que na última década o uso do aprendizado de máquina se espalhou rapidamente por toda a ciência da computação e além. Machine learning é usado em diferentes áreas, em pesquisa na web, filtro de spam de e-mails, sistemas de recomendação, anúncios, detecção de fraude, classificação de imagens e muitas outras aplicações.

O machine leargin são criações da ia que estão dedicadas na criação de algoritmos que são capazes de permitir que sistemas aprendam sem a intervenção humana, ou seja, de maneira autônoma. Já o deep learning é explicado por Chagas (2019):

> O Deep Learning trabalha o sistema do computador para realizar tarefas como reconhecimento de fala, identificação de imagem e realizar projeções. Ao invés de organizar as informações para atuarem através de equações predeterminadas, esse aprendizado determina padrões básicos dessas informações e ensina os computadores a desenvolver-se através da identificação dos padrões em camadas de processamento.

O Deep Leargin tem seu foco na criação de sistemas que imitam o cérebro humano de maneira artificial, um grande exemplo são as redes neurais artificiais que são capazes de se adaptar e aprender com grandes volumes de dados.

A resolução de problemas define-se como a capacidade de realizar uma tarefa de modo que ela seja julgada como eficiente, dentro da inteligência artificial a resolução de problemas funciona com intervenção, ou seja, o usuário ainda tem que exercer algum tipo ação para que ela possa realizar a tarefa, o que para muitos da área indica que este tipo de ação não designa inteligência como deveria ser (OLIVEIRA, 2018).

As tecnologias precisavam ter uma interação com os seres humanos, de forma que o computador e homem fossem capazes de se comunicar, propondo um método para que a máquina entendesse e processasse informações sobre o que o usuário necessitava, para que ele agisse de maneira eficiente e seu uso fosse indispensável.

De acordo com essa necessidade o Processamento de Linguagem Natural (PLN) existe para que seja possível que ocorra essa interação da inteligência artificial com o mundo real e seus usuários no dia a dia, de forma que a máquina fosse capaz de entender a linguagem humana de modo eficaz e objetiva, a fim de trazer soluções para as indagações do ser humano (OLIVEIRA, 2018).

O avanço na área da inteligência artificial nos mostra que as criações e investimentos estão se destacando cada vez mais, e ainda sendo capaz de demonstrar o seu uso no dia a dia, desde aplicações mais simples como chatbots que são programas de conversação, até as mais complexas como é o caso das redes neurais artificiais.

3. A INFLUÊNCIA POSITIVA DA IMPLEMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA EDUCAÇÃO

A inteligência artificial (IA) não é mais uma realidade distante ou limitada à ficção científica como se era costumado ver, e está se tornando cada vez mais presente na vida das pessoas, inclusive na educação. O assunto não é novo e, começou a ser colocado em discussões na década de 1930, o pai da computação e matemático Alan Turing formalizou o termo algoritmo em um artigo sobre máquinas de Turing. O algoritmo é um componente fundamental da inteligência artificial, termo este, que foi proposto pelos pesquisadores John McCarthy, Marvin Minsky e Claude Shannon em uma conferência de 1956.

De acordo com Gomes (2010, p. 7) “a inteligência artificial é um ramo da Ciência da Computação cujo interesse é fazer com que os computadores pensem ou se comportem de forma inteligente”. A forma inteligente mencionada se refere a capacidade das máquinas agirem com o mínimo de interferência humana possível, já que, este é o seu objetivo principal.

A inteligência artificial possui uma capacidade de armazenamento e processamento de linguagem natural muito poderosa, se mostrando deste modo ser uma grande aliada da educação, pois com seu alto poder de processamento se torna eficiente e adequada o

seu uso no ambiente escolar.

Assim, foi mencionado por Gomes (2010, p.11) “existem três níveis para o reconhecimento: comandos (reconhece de dezenas a centenas de palavras), discreto (reconhece fala ditada e com pausas entre as palavras) e contínuo (reconhece a fala natural)”. A linguagem natural se refere a linguagem usada pelos seres humanos, o processamento da linguagem natural é imprescindível, pois, se trata da capacidade da máquina entender e responder de forma ágil as necessidades do usuário.

Com a implantação das tecnologias inclusivas foi observado como principal ponto forte comprovado que é possível motivar os alunos através da utilização das tecnologias, em especial os educandos que apresentam dificuldades de aprendizado e na realização das tarefas que são propostas pelos professores dentro e fora das salas de aula.

De acordo com Melo (2019, p. 27):

> Desse modo, é importante que o professor conheça métodos e abordagens diferentes, para que possa aprimorar e alcançar os objetivos de ensinar em diferentes contextos, sejam eles nas modalidades presencial ou online, de forma significativa para o aluno.

As práticas de ensino com a utilização das tecnologias podem ser adaptadas com o ensino que o professor pretende repassá-las aos seus alunos, de forma que a I.A será capaz de apresentar um ensino mais didático, intuitivo e divertido para os alunos, despertando neles a vontade e desejo de indagar, saber mais sobre o assunto que o professor está repassando a eles.

Segundo Melo (2019, p. 27) “o bom ensino é aquele com que o professor se identifica, em que aluno e professor estejam envolvidos”. Para os educandos obterem maior taxa de aprendizados dos conteúdos precisa-se desde envolvimento mais dinâmico entre aluno e professor, onde o educador possa se questionar mais sobre os seus métodos de ensino abordados, para que se preciso sejam aprimorados com o auxílio da IA.

O ambiente e como o ensino é repassado aos educandos diz muito sobre como ele irá de fato absorver aquele conhecimento, a inteligência artificial proporciona aos alunos a possibilidades de vivenciar novas experiências de ensino, facilita a comunicação em sala de aula entre professor, aluno e o conhecimento.

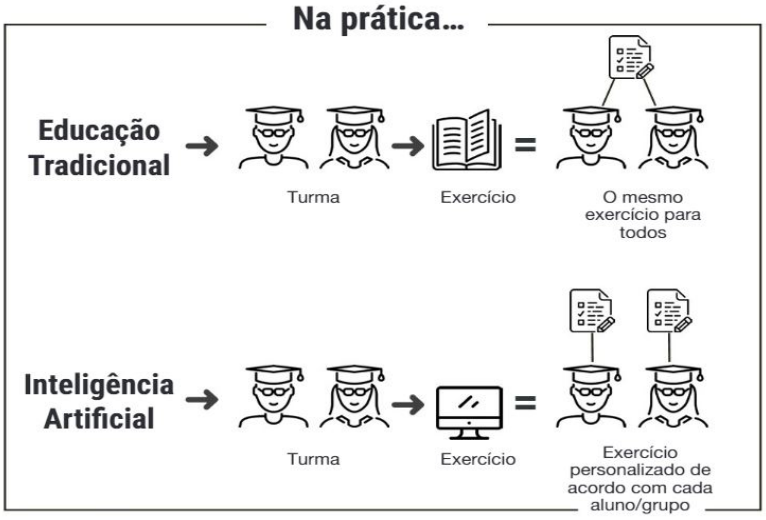


Figura 2 - Modelos de ensino.

Revista Appai Educar: Inteligência Artificial não é o futuro, é o presente! (2018)

Na figura 2, tendo em vista que ninguém aprende de maneira igualitária este modo de ensino atinge de maneira negativa os alunos que não conseguem ter o mesmo nível de aprendizagem dos outros, gerando um déficit de aprendizagem e dificultando seu desenvolvimento de conhecimento para os anos que seguem, sendo este, um dos grandes problemas que a educação brasileira enfrenta nos dias atuais.

Lastória e Campos (2020, p. 4) afirmam que "de acordo com essa visão, permeada de elementos de marketing, máquinas não só seriam melhores aprendizes como possibilitariam um ensino mais efetivo, delimitando individualmente as defasagens e os modos de aprender de cada estudante".

Com a utilização das ferramentas de inteligência artificial é possível ter uma proposta de ensino e atividades personalizadas de acordo com cada aluno, levando em conta as suas dificuldades no decorrer do seu aprendizado e sendo capaz de identificá-las para adaptar um plano de estudo para aquele indivíduo atendendo as necessidades de aprendizagem deles.

O professor Saiji Isotani assim citado por Casatti (2018) defende que ao utilizar as ferramentas da Inteligência Artificial é possível ampliar a inteligência dos seres humanos, "A gente já consegue verificar, por exemplo, para conjuntos de milhares de alunos, abordagens de ensino que têm maior potencial de auxiliar a aprendizagem e, assim, apoiar o professor na tomada de decisão pedagógica."

De acordo com por Casatti (2018) sobre a fala do professor Saiji Isotani, podemos observar que com a aplicação das tecnologias é possível realizar a adaptação dos métodos de ensino que serão aplicados aos alunos, e decorrente destas aplicações é gerado outra grande influência, que é a facilidade na absorção do conteúdo, pois é repassado a eles de modo inovador e atrativo através das utilizações de tecnologias como o computador, aumentando as chances do aprendizado dos mesmos.

Sistemas computadorizados que ajudam à tomada decisão já existem há décadas, mas com a revolução industrial e principalmente da internet causando assim o aumento da velocidade de processamento e de armazenamento de informação dos computadores, permitiu quem em segundos analisar um grande volume de dados para tomar decisões mais rápidas, orientando a proposta e tomada de decisões, realizando tarefas sem receber instruções diretas de humanos. (LOBO, 2018).

Segundo Soares Ibrahim e Morcos (2002) citado por Pimentel, Queiroz, Lima e Sampaio (2018, p. 494) "definem IA como a automação de atividades associadas ao pensamento humano, como tomadas de decisão, resolução de problemas, aprendizado, percepção e raciocínio".

Com a utilização dos computadores juntamente com a implementação da Inteligência Artificial dentro do âmbito escolar os educandos têm a oportunidade de estudar de qualquer lugar e não apenas dentro do ambiente escolar, ampliando as possibilidades de estudos e aumentando o tempo de estudo dos alunos.

O computador pode ser visto como uma ferramenta pedagógica para criar um ambiente interativo que proporcione ao aluno, investigar, levantar hipóteses, pesquisar, criar e assim construir seu próprio conhecimento (MATTEI, 2011).

Em resumo, é de grande importância a inteligência artificial assim explicado por Gonçalo, Carvalho e Araújo (2022, p.1):

> A Inteligência Artificial inserido no setor educacional proporciona ao deficiente um aprendizado diferenciado, o ajudando a aumentar o engajamento do

> aluno. Isso porque são diferentes recursos de tecnologia disponibilizados a qualquer momento, como a gamificação, que elevam o interesse do estudante pela educação, dessa essa estratégia transforma os alunos em protagonistas com habilidades fundamentais e mais conhecimento.

As tecnologias dentro do âmbito escolar proporcionam ao aluno uma nova perspectiva de mundo e recursos que estão disponíveis, familiarizando os mesmos desde cedo para o seu futuro mais próximo com os equipamentos tecnológicos dentro e fora do ambiente escolar.

4. AS PRÁTICAS DE ENSINO COM A INTELIGÊNCIA ARTIFICIAL

Com a implantação da inteligência artificial na educação foi possível que ocorresse a mudança de parâmetros de ensino para os educandos, de maneira que proporcionou mudanças significativas no seu aprendizado de modo dinâmico, com que a utilização das tecnologias foi possível que os alunos com mais dificuldade de aprendizagem conseguissem assimilar o conteúdo mais rápido e ajudando a solucionar o problema do déficit de compreensão do conteúdo. Assim explicado por Kenski (2003, p.5):

> Os atributos das novas tecnologias digitais tornam possíveis o uso das capacidades humanas em processos diferenciados de aprendizagem. A interação proporcionada por softwares especiais e pela Internet, por exemplo, permite a articulação das redes pessoais de conhecimentos com objetos técnicos, instituições, pessoas e múltiplas realidades... para a construção de espaços de inteligência pessoal e coletiva.

Esta é uma área que tem sido cada vez mais presente no dia a dia da sociedade, desde as casas inteligentes nas quais são controladas por meio de aplicativos de celulares, nos atendimentos de sites de forma que eles utilizam chatbot, que é um atendimento online no qual é feito através de robôs que conversam com o cliente, como por exemplo podemos citar a Lu da Magazine Luiza, os e-mails também utilizam a inteligência artificial, e está aplicação pode ser observada quando automaticamente um e-mail é classificado como spam na caixa de correio eletrônico, essa revolução da tecnologia é citado por Rosa (2019, p. 7):

> Destaca-se, portanto, que esta nova fase do direito, a digital, será impulsionada por um conjunto de tecnologias disruptivas como robótica, inteligência artificial, realidade aumentada, big data (análise de volumes massivos de dados), nanotecnologia, impressão 3D, biologia sintética e a chamada internet das coisas, em que cada vez mais dispositivos, equipamentos e objetos serão conectados uns aos outros por meio da internet. Algumas dessas inovações estão em sua fase de “infância” e ainda não mostraram todo o seu potencial.

A aplicações da I.A também podem ser observadas de forma positiva na sua participação na educação, de maneira que vem aumentando a chance de aprendizado dos educandos e também disponibilizando aos professores dados sobre a aprendizagem dos seus alunos de forma individual, desta maneira é possível adaptar os estudos com as necessidades de cada aluno. Segundo Vicari (2018), a utilização dos meios tecnológicos nos ambientes educacionais promove que os educandos tenham a capacidade de se desenvolver melhor para as exigências que estão sendo impostas pelo mundo globalizado em

que tudo envolve a tecnologia, se preparando desde pequenos para enfrentar a exigências e competitividades atuais.

Podemos ressaltar que é fortemente desejável que os jovens possam compreender as tecnologias e os fundamentos da inteligência artificial que a contemporaneidade vem proporcionando a eles, e de maneira mais simples a I.A pode ser compreendida como a referência de sistemas ou máquinas que possuem a finalidade de imitar a inteligência humana para a realização de tarefas, e ainda com o tempo aprimorar essas tarefas de acordo com os dados que são coletados durante seu uso. Sendo assim, de acordo com Lobo (2018, p. 3):

> Inteligência artificial (IA) é um ramo da ciência da computação que usando algoritmos definidos por especialistas é capaz de reconhecer um problema, ou uma tarefa a ser realizada, analisar dados e tomar decisões, simulando a capacidade humana.

Tendo em vista estas duas principais características da Inteligência Artificial pode proporcionar ajuda aos professores na criação de ambientes de aprendizagem colaborativas, atendendo as necessidades dos alunos por meio das chamadas técnicas de mineração de dados educacionais para “rastrear” o comportamento dos educandos com relação a aprendizagem. De acordo com Russel e Norvig (2020) citado por Camada e Durães (2020, p. 4):

> As aplicações modernas apontam para um conceito de I.A voltados para duas principais características: Autonomia e adaptabilidade. Autonomia é a habilidade de executar tarefas em contextos complexos sem constante intervenção do ser humano, e a adaptabilidade é a habilidade de melhorar seu desempenho aprendendo com a experiência.

Considerando que as novas tecnologias auxiliam o professor no conteúdo que será transmitido é possível realizar a automatização das atividades que virão a ser passadas aos alunos, atividades estas que a I.A disponibilizará de maneira individualizada de modo que venha atender a necessidade de cada aluno em específico, segundo Taurion (2020):

> A principal aplicação da IA não será em robôs físicos substituindo humanos, mas em robôs de software, exemplificados em sistemas e assistentes virtuais controlados por voz, no apoio às tarefas educacionais, como agentes pedagógicos, auxiliando e complementando as atividades dos professores.

A Inteligência Artificial possui uma área chamada de gamificação, na qual é atrelada a associação dos jogos educacionais como metodologia de ensino eficiente, de acordo com Dutra (2020) “A gamificação colabora com o desenvolvimento e participação do aluno, além de oferecer estímulos externos que ajudam no processo de aquisição de conhecimento e no reforço escolar”.

Associar os jogos ao ensino é uma abordagem inovadora e prazerosa aos alunos, pois, os mesmos aprendem brincando, com a utilização dos jogos os educandos demonstram seus conhecimentos à medida que vão jogando e avançando nas fases dos games, a I.A possui a funcionalidade de se adaptar de forma automática ao nível de dificuldade dos problemas que serão propostos para que os alunos achem meios de soluções para a resolução dos problemas apresentados. Assim, explicado por Andrade et al. (2013, p. 1455):

> Gamificação é um conceito que pode ser entendido erroneamente como "aprender por meio de jogos". Contudo, o uso correto deste termo refere-se à utilização de elementos e técnicas de design de jogos em situações fora do contexto de jogos, a fim de obter maior participação e envolvimento das pessoas em um determinado assunto ou contexto. Essa abordagem pode ser aplicada em ambientes empresariais, escolas, administração pública e até em atividades do cotidiano.

O avanço em disparada dos equipamentos tecnológicos é notório, vivemos em um mundo globalizado onde a implantação da tecnologia se mostra indispensável em todas as suas áreas de aplicações no nosso dia a dia, desde a comunicação das pessoas através do aplicativo WhatsApp até aos métodos de ensino em salas de aula, facilitando seu aprendizado. Assim explicado por Giordan (2005, p.292):

> É evidente que a interação do aluno com os aplicativos de simulação ou com sistemas tutoriais não esgota as formas de uso do computador na Educação em Ciências. Uma forma de se contrapor ao realismo da visualização molecular é fomentar o diálogo dos alunos entre si, de modo a realçar a busca do consenso como um dos propósitos das atividades que se realizam diante do computador.

O primeiro benefício que a ia mostrar para nós na educação, é a sua capacidade de personalização do ensino para cada aluno de forma individual, com suas análises de dados a inteligência artificial consegue "aprender", por exemplo a ia é capaz de mostrar em quais matérias os alunos têm mais dificuldades e quais matérias chamam mais atenção deles e com base nesses dados é possível adaptar um plano de ensino adequado. Desta maneira a instituição educacional é capaz de extrair o potencial máximo do aluno de maneira diferente do que no ensino tradicional. Assim reforçado por Portela e Isotani (2017, p.5):

> O grande potencial da IA aplicada ao ensino é promover a personalização do percurso de aprendizagem, de maneira que a pessoa tenha a sensação de que aquele percurso parece ter sido planejado especialmente para si. Embora essa promoção seja executada por ou com o auxílio de softwares, sente-se que o percurso está sendo desenhado e gerido por uma inteligência humana.

4.1 As tendências tecnologias na educação

Podemos afirmar que a Realidade Aumentada trata do mundo real como ponto de partida para uma experiência que leva o usuário a experimentar o mundo virtual. A RA prevê que não seja retirada do usuário a consciência de que ele está em seu ambiente real, mas traz para ali (o ambiente real) os objetos tridimensionais necessários para que a interação ocorra (FORTE; KIRNER, 2019). O uso da realidade aumentada (RA) nas salas de aula chama muita atenção dos alunos pelo fato de misturar o mundo virtual com o mundo real.

Visando melhores aplicabilidades do ensino os cientistas criaram os tutores inteligentes, que é uma ferramenta com a finalidade de proporcionar um ensino adaptativo e individual ao aluno, de modo que o educando tenha um sistema que assemelha o seu comportamento ao de um professor, sendo capaz de aplicar tarefas com maior precisão, visando explorar o potencial máximo dos alunos. Sengundo Pozzebon, Frigo e Bittencourt (2009, p.3):

> Dentre as principais deficiências identificadas, pode-se citar a rigidez pedagógica, a falta de capacidade de adaptação às características dos diferentes aprendizes e a pobreza de recursos didáticos. Com o objetivo de solucionar estas deficiências foram incorporadas técnicas de Inteligência Artificial, dando origem aos Sistemas Tutores Inteligentes. Estas técnicas permitem a modelagem das características do aprendiz e a flexibilização do comportamento do sistema.

Sabemos que os professores armazenam grandes volumes de dados com relação a planos de ensino e atividades propostas para seus alunos, uma solução prática para esta problemática é o armazenamento dos dados na nuvem. Por meio do Cloud Computing, os educadores podem armazenar seus arquivos de forma remota, e ainda podem compartilhar com outros usuários através da internet q qualquer lugar e hora. Sengundo Oliveira e Mozzaquatroa (2011, p.4):

> Nuvem computacional oferece uma nova maneira de trabalhar com Ambientes Virtuais de Aprendizagem por permitir utilizações diversas e processamento de aplicações pesadas. Podem ser disponibilizados desde ambientes simples até plataformas envolvendo cálculos complexos e processamento intenso. Através do acesso móvel o usuário teria todo seu material disponível independente de plataforma utilizada ou sua localização, ainda poderia acompanhar datas, anotações, contatos de maneira mais ativa.

O método da gamificação é outro que vem se destacando com seu uso em sala de aula, pois esta estratégia busca trazer a utilização de jogos para repassar os conteúdos abordados em sala de aula, como perguntas, desafios e rankings. Esta aplicação ajuda a desenvolver as habilidades dos alunos e os estimula a superarem cada novo desafio proposto. Assim citado por Tolomei (2017, p. 149):

> Dessa forma, a ideia de que o uso de games ou atividades gamificadas favorece o engajamento dos estudantes em atividades escolares tidas por eles como enfadonhas é inevitável, porque o uso dos games pode aproximar o processo de aprendizagem do estudante à sua própria realidade. Primeiramente por estimular o cumprimento de tarefas para o avanço no curso com o objetivo de alcançar as recompensas, e segundo por ser de fácil acessibilidade, tendo em vista que sua utilização pode ocorrer com celulares, tablets e computadores.

Mesmo diante de todos os avanços da ia na área educacional, ainda devemos voltar nossa atenção para as barreiras de desigualdade ao redor que ainda precisam ser rompidas, barreiras estás que ainda impossibilitam a avaliação a fundo do real impacto do processo de aprendizagem com a utilização da Inteligência artificial.

3. CONCLUSÃO

O presente estudo trouxe à tona o tema sobre o uso da inteligência artificial na educação. Justificou-se o tema escolhido por tratar de instrumentos que podem proporcionar melhores qualidades de ensino e aprendizagem do conteúdo para os educandos, uma vez que tal torna-se importante o tema escolhido por se mostrar ser eficiente o uso da inteligência artificial no ambiente escolar.

Nessa perspectiva a presente pesquisa buscou respostas para o seguinte problema:

Quais tecnologias são capazes de proporcionar ao educando uma forma mais dinâmica e eficiente de absorção do conteúdo abordado? Teve como objetivo identificar as aplicações da inteligência artificial disponíveis que podem ser incluídas na educação escolar. Para tanto, três capítulos descreveram um pouco sobre o que é inteligência artificial, a influência positiva da implantação da Inteligência artificial na educação e as práticas de ensino com a Inteligência artificial.

Sobre o que é inteligência artificial, observa-se que foi explicado e exemplificado o seu contexto histórico, de modo que veio a sanar qualquer tipo de dúvidas sobre o assunto abordado.

Em relação a influência positiva da implantação da inteligência artificial, a discussão propõe que o seu uso no ambiente escolar proporciona melhores qualidade de ensino aos alunos, de maneira que contribuem a aumentar o seu grau de aprendizagem de forma eficientes com o uso das tecnologias existentes.

A respeito das práticas de ensino com a inteligência artificial torna-se importante vale salientar que é possível ter um maior nível de internação dos alunos com os conteúdos apresentados pelos professores em sala de aula, de modo que os educandos mantêm mais atenção as aulas e com a implantação deste modelo de ensino inovador.

Diante da realização do estudo, é ressaltado que a integração das tecnologias no ambiente escolar é eficiente na vida educacional dos alunos, lhes proporcionando um ensino de qualidade com recursos tecnológicos. À luz das teorias, exploradas na fundamentação teórica desta pesquisa bibliográfica, torna-se possível afirmar que os objetivos específicos em geral foram alcançados neste estudo científico.

Referências

ANDRADE, Fernando R. H; et al. Desafio do Uso de Gamificação em Sistemas Tutores Inteligentes Baseados em Web Semântica. In: WORKSHOP DE DESAFIOS DA COMPUTAÇÃO APLICADA À EDUCAÇÃO (DESAFIE!), 2, 2013, Maceió. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2013. p. 1453-1462.

BARANAUSKAS, Maria Cecília Calani et al. **Uma taxonomia para ambientes de aprendizado baseados no computador. O computador na sociedade do conhecimento**, v. 45, 1999. Disponível em: https://sites.icmc.usp.br/sisotani/aulas/SLC0610/livroMEC.pdf#page=45. Acesso em: 22 out. 2022.

BERTOZZO, Richard Junior. **APLICAÇÃO DE MACHINE LEARNING EM DATASET DE CONSULTAS MÉDICAS DO SUS**. 2019. 100 f. TCC (Graduação) - Curso de Sistemas de Informação, Informática e Estatística, Universidade Federal de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/202663/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 23 out. 2022.

CAMADA, Marcos Yuzuru; DURÃES, Gilvan Martins. **Ensino da Inteligência Artificial na Educação Básica: um novo horizonte para as pesquisas brasileiras**. In: SIMPÓSIO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO, 31. , 2020, Online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020 . p. 1553-1562. Disponível em: https://doi.org/10.5753/cbie.sbie.2020.1553. Acesso em: 27 mai. 2022.

CAMPOS, Luis Fernando Altenfelder de Arruda; LASTÓRIA, Luiz Antônio Calmon Nabuco. Semiformação e inteligência artificial no ensino. Pro-Posições, Campinas, v. 31, n. 1, p. 1-18, jan. 2020. Disponível em: https://doi.org/10.1590/1980-6248-2018-0105. Acesso em: 19 out. 2022.

CASATTI, Denise. Na sala de aula do futuro, somos todos inteligentes. 2018. Assessoria de Comunicação do ICMC/USP. Disponível em: https://icmc.usp.br/noticias/3942-na-sala-de-aula-do-futuro-somos-todos-inteligentes. Acesso em: 19 out. 2022.

CHAGAS, Edgar Thiago de Oliveira. Deep Learning e suas aplicações na atualidade. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, [S.L.], v. 04, n. 05, p. 05-26, 8 maio 2019. Revista Cientifica Multidisciplinar Nucleo Do Conhecimento. http://dx.doi.org/10.32749/nucleodoconhecimento.com.br/administracao/deep-learning. Disponível em: https://www.nucleodoconhecimento.com.br/administracao/deep-learning. Acesso em: 23 out. 2022.

DAMACENO, S. S.; VASCONCELOS, R. O. INTELIGÊNCIA ARTIFICIAL: UMA BREVE ABORDAGEM SOBRE SEU CONCEITO REAL E O CONHECIMENTO POPULAR. **Caderno de Graduação - Ciências Exatas e Tecnológicas** - UNIT - SERGIPE, [S. l.], v. 5, n. 1, p. 11, 2018. Disponível em: https://periodicos.set.edu.br/cadernoexatas/article/view/5729. Acesso em: 23 out. 2022.

Disponível em: https://sol.sbc.org.br/index.php/desafie/article/view/16915. Acesso em: 23 out. 2022

DUTRA. **Gamificação na educação: como aumentar o interesse dos alunos.** Disponível: https://www.google.com/amp/s/tutormundi.com/blog/gamificacao-na-educacao/%3famp Acesso: 18 de maio de 2022.

FORTE, Cleberson E.; KIRNER, Cláudio. Usando realidade aumentada no desenvolvimento de ferramenta para aprendizagem de física e matemática. In: 6º Workshop de Realidade Virtual e Aumentada, Santos-SP: UNISANTA. 2009. p. 1-6. Disponível: https://sites.unisanta.br/wrva/st%5C62200.pdf. Acesso em: 29 out. 2022.

GIORDAN, Marcelo. O computador na Educação em Ciências: breve revisão crítica acerca de algumas formas de utilização. **Ciência & Educação (Bauru)**, [S.L.], v. 11, n. 2, p. 279-304, ago. 2005. Disponível em: https://doi.org/10.1590/S1516-73132005000200010. Acesso em: 29 out. 2022.

GOMES, Dennis dos Santos. Inteligência Artificial: Conceitos e Aplicações. Revista Olhar Científico, Ariquemes, v. 1, n. 2, p. 234-246, dez. 2010. Disponível em: https://www.professores.uff.br/screspo/wp-content/uploads/sites/127/2017/09/ia_intro.pdf. Acesso em: 19 out. 2022.

GONÇALO, C. V. de S. .; CARVALHO, A. dos S. M. de .; ARAÚJO, A. M. de . Artificial Intelligence in favor of learning disabled students . **Research, Society and Development**, *[S. l.]*, v. 11, n. 11, p. e449111133271, 2022. DOI: 10.33448/rsd-v11i11.33271. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/33271. Acesso em: 19 oct. 2022.

http://polouabufrgspsicotic.pbworks.com/w/file/fetch/97258851/Informatica%20na%20educa%C3%83%C2%A7%C3%83%C2%A3o%20infantil.pdf . Acesso: 03 out. 2022.

KENSKI, Vani Moreira. APRENDIZAGEM MEDIADA PELA TECNOLOGIA. Revista Diálogo Educacional, Paraná, v. 4, n. 10, p. 47-56, 2003. Disponível em: https://www.redalyc.org/comocitar.oa?id=189118047005. Acesso em: 28 out. 2022.

LAVAGNOLI, Silvia. Machine Learning ou Deep Learning? 2019. OPENCADD. Disponível em: https://opencadd.com.br/machine-learning-ou-deep-learning/. Acesso em: 21 out. 2022.

LOBO, Luiz Carlos. Inteligência artificial, o Futuro da Medicina e a Educação Médica. **Revista Brasileira de Educação Médica**, v. 42, p. 3-8, 2018. Disponível em: https://www.scielo.br/j/rbem/a/PyRJrW4vzDhZKzZW47wddQy/?format=pdf&lang=pt . Acesso em 08 abril 2022.

MATTEI, Claudinéia**. O prazer de aprender com a informática na educação infantil**. Instituto Catarinense de Pós-Graduação, Associação Educacional Leonardo da Vinci, 2011. Disponível em:

MELO, Maria Aparecida Viegas de. Inteligência Artificial e ensino de inglês como língua estrangeira: inovação tecnológica e metodológica/de abordagem? 2019. 156 f. Dissertação (Mestrado) - Curso de Estudos em Linguística, Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26726. Acesso em: 19 out. 2022.

OLIVEIRA, A. C. B. de. Inteligência Artificial: riscos e oportunidades. **CEBRI-Revista: Brazilian Journal of International Affairs**, [S. l.], n. 3, p. 175–181, 2022. Disponível em: https://cebri-revista.emnuvens.com.br/revista/article/view/58. Acesso em: 22 out. 2022.

PIMENTEL, Charles Soares; QUEIROZ, Rubens Lacerda; LIMA, Priscila Machado Vieira; SAMPAIO, Fábio Ferrentini. Projeto Frankie: uma proposta para o ensino de Inteligência Artificial na Educação Básica. Nuevas Ideas En Informática Educativa, Santiago de Chile, v. 14, n. 1, p. 493-498, jan. 2018. Disponível em: http://www.tise.cl/Volumen14/TISE2018/493.pdf. Acesso em: 19 out. 2022.

PORTELA, Samuel Santos; ISOTANI, Seiji. **A aplicação da Inteligência Artificial na personalização de itinerários de aprendizagem em ambientes virtuais**. 2017. Disponível em: https://especializacao.icmc.usp.br/documentos/posters/samuel_portela.pdf. Acesso em: 29 out. 2022.

POZZEBON, Eliane; FRIGO, Luciana Bolan; BITTENCOURT, Guilherme. Inteligência artificial na educação universitária: quais as contribuições. Revista do Centro de Ciências da Economia e Informática da Universidade da Região da Campanha Urcamp, Editora da URCAMP-EDIURCAMP, v. 8, n. 13, p. 34-41, 2004. Disponível em: https://www.researchgate.net/publication/242091111_INTELIGENCIA_ARTIFICIAL_NA_EDUCACAO_UNIVERSITARIA_QUAIS_AS_CONTRIBUICOES. Acesso em: 29 out. 2022.

ROSA, Alexandre Morais da. Questão digital. Revista de Direito da Faculdade Guanambi, [S.L.], v. 6, n. 02, p. 259, 26 set. 2019. Centro de Educação Superior de Guanambi (CESG). http://dx.doi.org/10.29293/rdfg.v6i02.259.

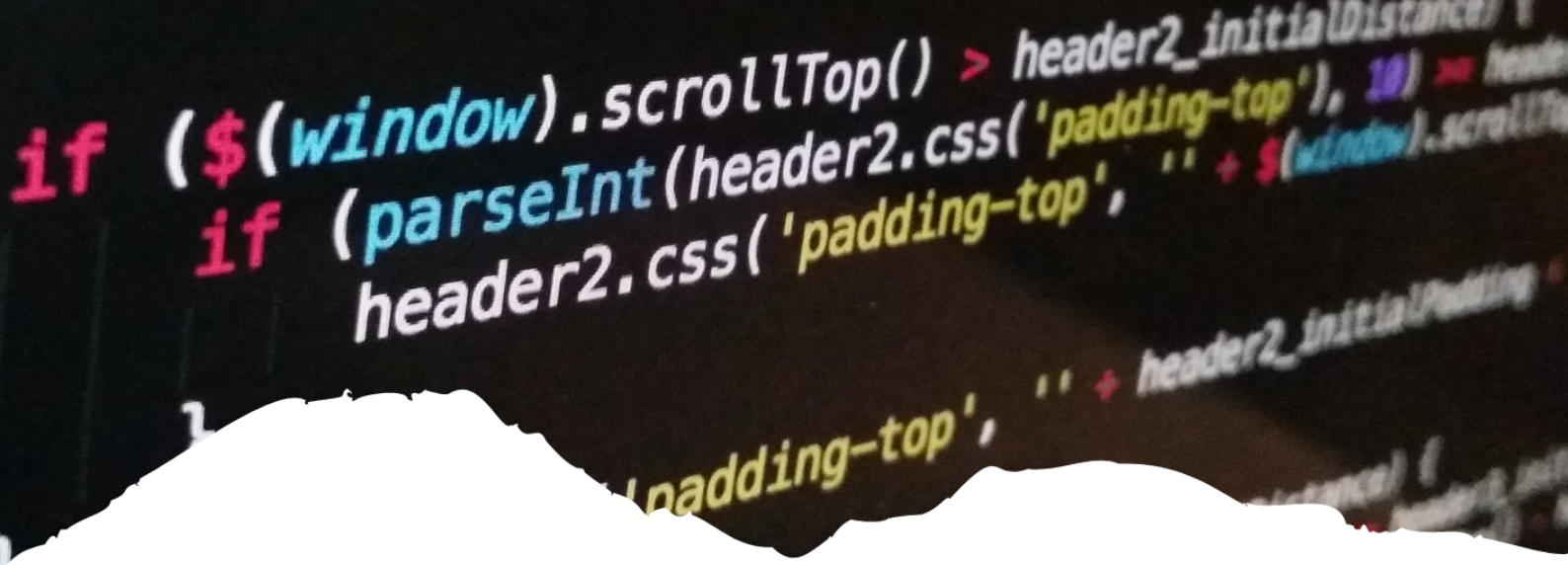
Disponível em: https://portaldeperiodicos.animaeducacao.com.br/index.php/RDFG/article/view/13928. Acesso em: 29 out. 2022.

SILVA, J. A. S. DA; MAIRINK, C. H. P. Inteligência artificial. **LIBERTAS: Revista de Ciências Sociais Aplicadas**, v. 9, n. 2, p. 64-85, 13 dez. 2019. Disponível em: http://famigvirtual.com.br/famig-libertas/index.php/libertas/article/view/247. Acessado: 22 outubro 2022.

TAURION, Cezar. O futuro da educação em um mundo de IA. 2020. Disponível em: https://revistatecnologia360.com.br/o-futuro-da-educacao-em-um-mundo-de-ia/. Acesso em: 28 maio 2022.

TOLOMEI, Bianca Vargas. A gamificação como estratégia de engajamento e motivação na educação. EAD em foco, v. 7, n. 2, 2017. Disponível em: https://eademfoco.cecierj.edu.br/index.php/Revista/article/view/440. Acesso em: 29 out. 2022.

VICARI, Rosa Maria. Tendências em inteligência artificial na educação no período de 2017 a 2030: sumário excutivo. 2018. Disponível em: https://acervodigital.sistemaindustria.org.br/handle/uniepro/259. Acesso em: 29 out. 2022.



9

INTELIGÊNCIA ARTIFICIAL NO DESENVOLVIMENTO WEB

ARTIFICIAL INTELLIGENCE IN WEB DEVELOPMENT

Vandeilson Correia Fernandes

Resumo

Este estudo tem como objetivo demonstrar e a ponta os benefícios da IA na web através de exemplos já existentes no mundo onde vivemos, e conta das tecnologias projetadas pela história da humanidade que caminharam de forma voluntária e involuntária para as tecnologias existentes hoje. Analisar a junção de outras tecnologias para maior benefício humano em empresas e a vida pessoal. Utilizar de uma linguagem moderna para criar um IA e analisar o processo de alta aprendizagem.

Palavras-chave: Tecnologias. Aprendizagem. Processo. Linguagem. Mundo.

Abstract

This study aims to demonstrate the benefits of AI on the web through examples that already exist in the world where we live, and tells of the technologies designed by the history of humanity that voluntarily and involuntarily walked towards the technologies that exist today. Analyze the combination of other technologies for greater human benefit in companies and personal life.Use a modern language to create an AI and analyze the high learning processes.

Keywords: Technologies. Learning. Processes. Language. World.

1. INTRODUÇÃO

A tecnologia da IA pode ser utilizada de várias formas na *Web* como *Chatbots* para simular uma conversar com um ser humano junto a algum usuário, pode fazer pesquisas e conversas interativa utilizando o comando de voz do usuário, pode estabelecer a melhor rota para um usuário através de mapas, pode capturar e definir gesto de usuários utilizando câmeras, pode capturar informações de usuários em outras sites para captura de *leads*, pesquisas ou propagandas, pode melhorar a qualidade de imagens borradas, pode simular componentes em jogos *online* tanto como o suporte do jogo, alguns processos de aperfeiçoamento de *skins* e as simulações de um modo geral.

Em outras palavras, o futuro da IA em alguns setores está bem definido e abreviado com boas atualizações e novas pesquisas de desenvolvimento, em outros está em busca da ficção tão vista nos cinemas. Mas existem benefícios da Inteligência Artificial na *Web* que possam alcançar a todos que possuem acesso a um dispositivo com acesso à *internet*.

Então em objetivo foi pesquisado os benefícios da Inteligência Artificial na *Web* que pode alcançar a todos que possuem acesso a um dispositivo com acesso à internet, através de fonte de pesquisas confiáveis em artigos, livros e sites, visando atender aplicações no setor e possíveis melhorias em aspectos de *design* até às leis constituídas para a Inteligência Artificial e foi apontado as ferramentas que estão utilizando de forma indiscreta e vigentes a tecnologia de Inteligência Artificial voltada para a *Web*, e foi utilizou uma linguagem moderna para o desenvolvimento de uma ferramenta de Inteligência Artificial buscando entender seu processo de autoaprendizagem.

A grande quantidade de inovações aponta que este século será definitivo para essa tecnologia, muitas poucas pessoas sabem hoje em dia, mas os nossos celulares são puro Sistema Artificial no propósito de interpretar cada gesto que o ser humano faz a fim de conseguir a informação desejada, muitas das vezes pela internet através de comandos.

Em busca do maior benefício no desenvolvimento foi apontado o comportamento do sistema até a saída da eventual resposta, explicar porque de fato cada comportamento acontece e assim trazer mais entendimento da tecnologia para uma melhor compreensão da mesma.

Esta pesquisa teve como finalidade falar dos benefícios e todas as possibilidades de uso da Inteligência Artificial tanto como nos dias atuais e futuramente no “mundo da *Web*”, visando ferramentas já utilizadas atualmente e visa futuros relatórios de acordo com um desenvolvimento de aplicação com essa tecnologia. Sempre destacando as funções e aplicações utilizadas nos dias atuais e seus comportamentos.

2. HISTÓRIA, PROCESSO E O FUTURO DA INTELIGÊNCIA ARTIFICIAL

A 2.000 anos atrás o estudo de mecanismo capaz de imitar a performance funcional humana vem sendo tratados e evoluídos para eventuais substituições em trabalho braçais ou inovações que possam servir no dia-a-dia da vida do homem. No desenvolvimento voltado para a internet hoje em dia grandes empresas vêm trazendo essa inovação. Em visar uma maior facilitação do uso de sites e melhor eficiência na saída de dados para o usuário, a tecnologia de Inteligência Artificial (IA) vem sendo vista como uma solução de eficiência necessária para a velocidade desta saída de resultados.

Ocupação	Ranking n. de trab.	Número de trabalhadores	% do total de trabalho.	Ranking P(Auto)
Assistência Administrativa	1	2.081.339	4.5%	4
Auxiliar de Escritório, Em Geral	2	2.036.571	4.4%	4
Vendedor de Comércio Varejista	3	2.007.042	4.4%	8
Faxineiro	4	1.344.939	2.9%	34
Motorista de Caminhão (Rotas Regionais e Internacionais)	5	877.081	1.9%	20
Alimentador de Linha de Produção	6	860.740	1.9%	7
Operador de Caixa	7	823.476	1.8%	3
Professor de nível médio no Ensino Médio	8	749.667	1.6%	42
Vigilante	9	630.663	1.4%	16
Servente de Obras	10	571.663	1.2%	12
TOTAL	-	11.983.505	26%	100

Tabela 1 – Ocupações com mais trabalhadores no Brasil e suas probabilidades de automação

Fonte: Relatório Técnico "O Futuro do Emprego no Brasil: estimando o impacto da automação" (2019).

2.1 Empresas

Grandes empresas vêm investindo muito desde 2010 com muitos resultados e várias pesquisas, hoje tornou-se obrigatório um site ter a Inteligência Artificial em algumas funcionalidades. E de acordo com Estatísticas (que é uma empresa alemã especializada em dados e consumidores) através de um relatório é esperado em 2025 um aumento de US $126 bilhões. De acordo com Helton Simões (2017, p.1) o *Facebook* criou um Sistema Artificial no qual podiam interagir entre si e fazer novas aprendizagens por conta própria. Esse sistema eram *Chatbots* desenvolvidos para simular conversas entre humanos por meio da internet, então, foram colocados dois *Chatbots* para conversarem entre si chamados Alice e Bob e em poucos momentos os dois começaram a agir de forma estranha. Mais tarde, a *Digital Journal* disse que os programadores descobriram que os *Chatbots* desenvolveram uma nova forma de comunicação por padrões e repetições de palavras do idioma inglês por conclusão foram desligados rapidamente pelos desenvolvedores. E uma chuva de críticas foi posta ao *Facebook*, a maioria delas ressaltando que o *Facebook* não necessita desse tipo de aplicação.

2.2 Bibliotecas e ferramentas

A uma série de bibliotecas e programas que são usados para gerenciar vários tipos de tarefas e fazer os mais diversos trabalhos usando com base a rede *web* para ter uma vasta possibilidade de conhecimento gerenciáveis ou não gerenciáveis, segundo Somanath Balakrishnan (2018, p.1) entre as ferramentas mais famosas estão aquelas que são projetos

iniciados por grandes empresas como a *TesorFlow* que uma biblioteca que foi inicializada por programadores e engenheiros do *Google Brain Team*. E ela consiste no fornecimento de muitas *APIs* de nível baixo e as de nível superior, ela é usada em alguns programas do *Google* como o *RankBrain* e o *SmartReply*. Existem ferramentas que são muito utilizadas quando se fala em aprendizagem que máquina, que é a possibilidade de uma máquina apreender com seus dados consultados, evitando ao máximo a interferência humana para executar uma tarefa. Entre as várias ferramentas existentes hoje existem aquelas usadas por uma grande quantidade de usuários ou por grandes empresas, como o *SystemML* que foi criado na *IBM* e que é um projeto de nível superior e, considerado hoje como um sistema flexível e escalonável.

3. APRENDIZAGEM DE MÁQUINA

Como muitos já sabem a aprendizagem de máquina também tem como base as redes neurais artificiais, que são baseadas em sistemas nervosos centrais de animais e assim facilita muito o reconhecimento de padrões. Entre as ferramentas mais bem vistas no mercado está a *Neuroph* que é um *framework* da linguagem *Java* de programação. E trás as possibilidades da criação de um sistema artificial com classes que auxiliam na programação que trazem regras de aprendizado, conexões de neurônios, função de transferência, função de entrada e muitas outras possibilidades para a criação da IA.

3.1 Futuro dos setores

Segundo Ricardo de Freitas (2019, p.1) alguns empregos serão substituídos pelas IA e que a cada dia vem se tornando um fato por conta das inovações da última década. Na Medicina, Advocacia, Telemarketing, Analistas de RH, Correios e até o pessoal que faz suporte em computadores.

De acordo com a pesquisa de Alanis Meira (2022) editada por André Lucena (2022, p.1) um concurso de arte que aconteceu no estado do Colorado, nos Estados Unidos o ganhador foi um software de criação de imagens chamado *Midjourney* por Inteligência Artificial, mas claro com fator inicial a imagem foi criada por um americano chamado Jason Allen que fez algumas etapas até conseguir imprimir a imagem premiada. Ele usou o *Midjourney* que assim como o *Dalle*, é um sistema que gera imagens através de pesquisas por palavras chaves escritas nos servidores do programa *Discord*, lá ele usava de comando iniciais e em seguida palavras chaves gerando teste até chegar na imagem desejada e, além disso, ele usa o *Photoshop* nas suas três imagens favorita e uso também o software *Gigapixel AI* e aumentou a resolução da imagem para melhor visualização. Ainda com esses sistemas muitas outras pessoas que criaram imagens através deles tentaram vendê-las com suas assinaturas pela internet como no *Getty Images*.

Muitos acontecimentos como esse vem acontecendo e muitos programadores correm para aprender uma linguagem de programação que é voltada para sistemas artificiais e automação e até mesmo pessoas de outros setores buscam aprender alguma linguagem de programação pelo motivo dessa eventual substituição.

4. POR TRÁS DE UMA INTELIGÊNCIA ARTIFICIAL

Existem muitas aplicações que levam a inteligência artificial em seus códigos com

uma variação grande de processos passando a montar como objetivo determinado a fim de solucionar um problema corriqueiro ou inovar em um setor para facilitar a vida de vários trabalhadores trazendo mais perfeições em execuções sem estar à mercê de erros humanos. Mas isso não aponta 100% que não haverá erros em aplicações e ferramentas modernas que trazem a inteligência artificial.

Das tecnologias que levam inteligência artificial existem aquelas que são mais relevantes e utilizadas tanto no ambiente corporativo quanto no ambiente doméstico usando uma mescla de ferramentas para determinado fim. A quatro anos a Inteligência artificial representava apenas 10% das empresas que haviam implementado ela, mas em 2019 cresceu para 37% segundo Chris Howard (2019).

Na produção de linguagem natural existem ferramentas que traduzem texto e identifica erros em muitas línguas do mundo, o reconhecimento de fala que traduz automaticamente a fala humana, Agende Virtuais que fazem interação com o consumidor como os *Chatbots*, fornecedores de aprendizagem de máquina com *APIs* e ferramentas de treinamento.

A tecnologia da Inteligência Artificial pode ser utilizada de várias formas na *Web* como pode estabelecer a melhor rota para um usuário através de mapas, pode capturar e definir gesto de usuários utilizando câmeras, pode capturar informações de usuários em outras sites para captura de *leads*, pesquisas ou propagandas, pode melhorar a qualidade de imagens borradas, pode simular componentes em jogos *online* tanto como o suporte jogo, alguns processos de aperfeiçoamento de *skins* e as simulações de um modo geral.

Figura 1 - Inteligência artificial faz imagens borradas ficarem 60x mais nítidas

Fonte: Meet the authors: Sachit Menon, Alex Damian, McCourt Hu, Nikhil Ravi and Cynthia Rudin. From a single blurred image PULSE can generate uncannily lifelike portraits, which might differ subtly from the real person but are much sharper than previous methods. Credit: Duke University

4.1 Linguagens de programação

Em relevância disso existem linguagens que são mais apropriadas para a criação de ferramentas e softwares desse tipo trazendo *frameworks* e biblioteca para facilitar na criação das mesmas, como a linguagem *Java, R, Python, C, C++* e o *JavaScript*.

A linguagem *Java* de acordo com Jones Granatyr (2018, p.1) é a mais popular do mundo segundo o *ranking* da *TIOBE* é muito utilizada no desenvolvimento web, sendo possível utilizar inteligência artificial nas suas plataformas, as suas bibliotecas como a possibilidade do *pipeline* trazem uma facilidade para processos de linguagem natural. Ela está sendo muito importante para o aprendizado profundo acelerado *deep learning* com *APIs*, umas das mais utilizadas é a é o *TensorFlow* do *Google* que fornece uma *API* em *Java*.

O *R* por exemplo possui uma biblioteca que trabalha diretamente com aprendizagem de máquina que é a *ForIA*, para a aprendizagem profunda existe a biblioteca *MXNet*. No exterior essa linguagem vem ganhado bastante relevância no mundo da inteligência artificial, no brasil vem sendo mais utilizada para processos de estatísticas (GRANATYR, 2018, p.1).

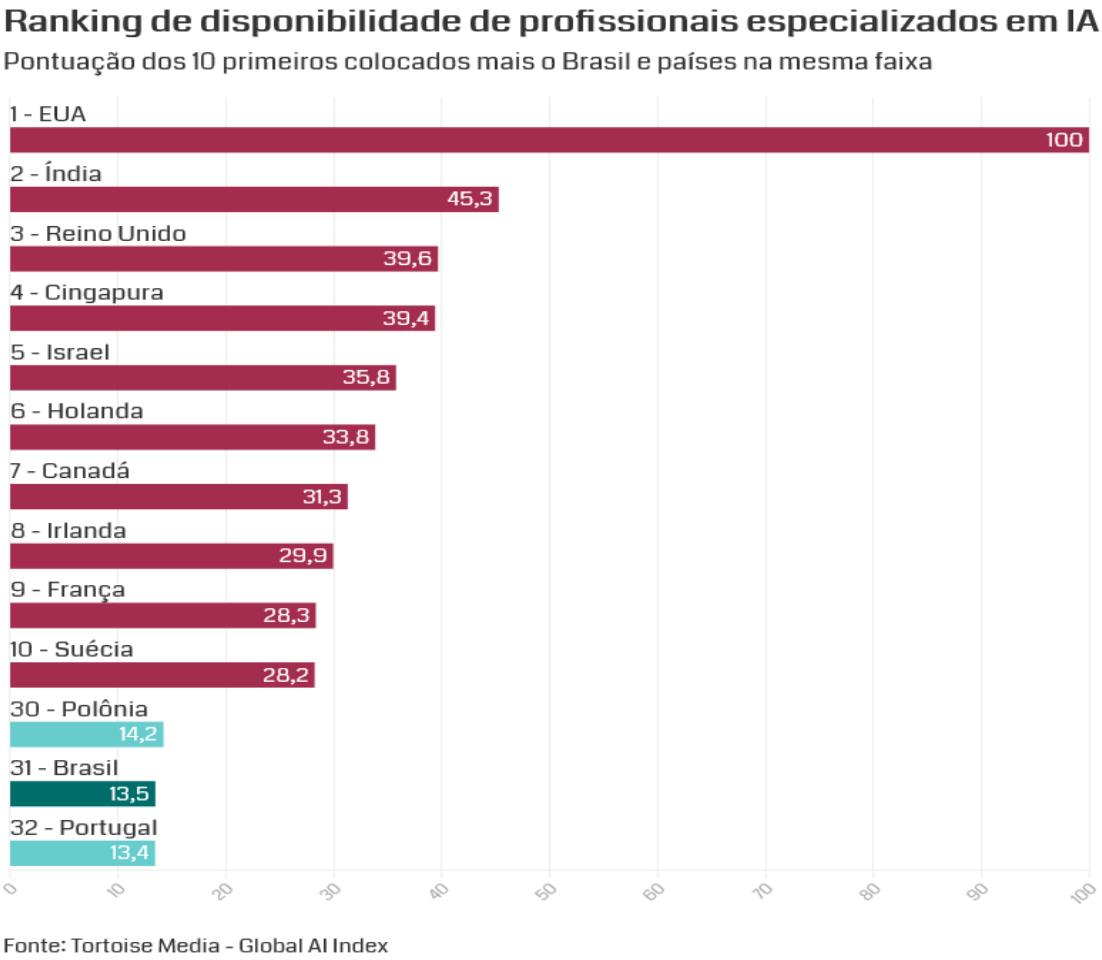


Figura 2 - Profissionais especializados em IA por país

Fonte: Tortoise Media - Global AI Index

O *Python* é uma linguagem que vem crescendo muito nos últimos por muitas empresas e é umas das linguagens mais utilizadas para o desenvolvimento artificial tanto na *web* como fora dele. Por sua simplicidade e a facilidade de criação de protótipos em poucas linhas de código. Por causa das suas bibliotecas únicas vem sendo cada vez comum falar de inteligência artifical e relacionar logo essa linguagem, para o processamento de linguagem natural existe as bibliotecas *NLTK* e *SpaCy* (O *NLTK* por sua popularidade chegou a se tornar uma *API*. aprendizado de máquina), para aprendizagem profunda os mais populares são *TensorFlow, Chainer, PyTorch, Theano, Apache MXNet*. E lembrando que para o desenvolvimento *web* o *framework* mais utilizado é o *Django* (GRANATYR, 2018, p.1).

4.2 Detalhando o código por trás de uma inteligência artificial

Para melhor compreensão dos códigos que compõem uma inteligência artificial foi desenvolvido um pequeno algoritmo através da linguagem *JavaScript* de programação, passando assim a detalhar padrões e coisas comuns que podem ser apresentadas em outros projetos independente da linguagem, biblioteca ou *API*.

Todas as ferramentas para esse fim buscam reconhecimento de padrões que a partir da análise de um conjunto de dados que resultam em uma organização desses dados transformando-os em padrões que serão utilizados e normalmente são grupos de medidas ou observações que definem pontos em um espaço multidimensional apropriado.

BIBLIOTECAS	**DESCRIÇÃO**
TensorFlow	O TensorFlow é uma biblioteca open source para computação numérica usando gráficos de fluxo de dados. Foi desenvolvida por pesquisadores e engenheiros do Google Brain Team e rapidamente se tornou uma das principais ferramentas para machine learning e deep learning e inteligência artificial.
Caffe	Caffe é um poderoso framework muito rápido e eficiente para pesquisa de aprendizado profundo.
Keras	Keras é uma biblioteca de rede neural de código aberto escrita em Python.
Torch	MLPack é uma biblioteca de machine learning (aprendizado de máquina) escalável implementada em C++. Por estar em C++, você pode adivinhar que é ótimo para gerenciamento de memória.
Scikit-learn	Scikit learn é uma biblioteca Python muito poderosa para machine learning (aprendizado de máquina) que é usada principalmente na construção de modelos.
Spark MLlib	O Spark MLlib do Apache é uma biblioteca de machine learning (aprendizado de máquina) muito escalável.
MLPack	MLPack é uma biblioteca de machine learning (aprendizado de máquina) escalável implementada em C++. Por estar em C++, você pode adivinhar que é ótimo para gerenciamento de memória.

Quadro 1: Bibliotecas e *frameworks* mais utilizadas para o desenvolvimento de Inteligências Artificiais

Fonte: BrasilCode - Robson dos Santos

Segundo Machine Learning (2022, p.1) nos algoritmos de aprendizagem tem várias técnicas que possam ser usadas buscando a melhor criação de Inteligência artificial em termos de complexidade com “Aprendizagem Supervisionada” e “Aprendizagem sem Supervisão”. Para tais fins existem diversas técnicas como Árvore de Decisão, Classificação *Naive Bayes*, Regressão Logística, *Clustering*, *PCA* (Análise de Componentes Principais) e *ICA* (Análise de Componentes Independentes).

A árvore de decisão é uma tabela de decisão em forma de árvore e usa a mesma lógica quando se usa uma tabela.Chamado também como método da árvore ela mapeia as decisões dentro de um sistema e suas possíveis consequências.

Baseada na descoberta de Thomas Bayes a Classificação *Naive Bayes* é um algoritmo que faz predições em aprendizagem de máquina é construída como classificadores probabilísticos com fortes suposições de independência entre os recursos e é bastante utilizado em reconhecimento facial.

A Regressão Logística também faz parte da aprendizagem supervisionada e é uma técnica estatística que a partir de um conjunto de observações cria predições com uma série de variáveis explicativas contínuas e/ou binárias.

> O *Clustering* é um conjunto de técnicas que faz agrupamento de dados automaticamente a partir de um grau de semelhança, ou seja, objetos que possuem características comuns. Ele faz parte dos algoritmos de aprendizagem não supervisionada (LEARMING, 2022, p.1).

Também é importante ressaltar que entre os padrões mais conhecidos em termos de algoritmos trazidos muitas vezes por bibliotecas onde se encontra como por exemplo o *pipeline* que é um operador que é nada mais do que execuções de funções sequenciais, ou seja a função ou expressão é passado para a próxima execução, então através do algoritmo vai-se pegando essas expressões ou funções anteriores até serem apresentadas no último processo de execução, ou seja até o resultado final. Esse padrão de processos é apresentado em muitas outras linguagens sendo mais conhecida no *Python*.

5. UM XADREZ DE POSSIBILIDADES

Foi detalhado de acordo com o artigo do Daniel Rosa (2022, p.1) de uma forma explicativa uma pequena aplicação que leva Inteligência Artificial criada na Linguagem *JavaScript* representada em um jogo de xadrez onde o usuário joga contra a Inteligência Artificial e onde a primeira jogada é sempre do usuário. As tecnicas utilizadas para a criação do jogo foi a geração de movimento, avaliação do conselho, a *minimax* e o poda alfa-beta, e cada técnica afeta o estilo de jogo executado.

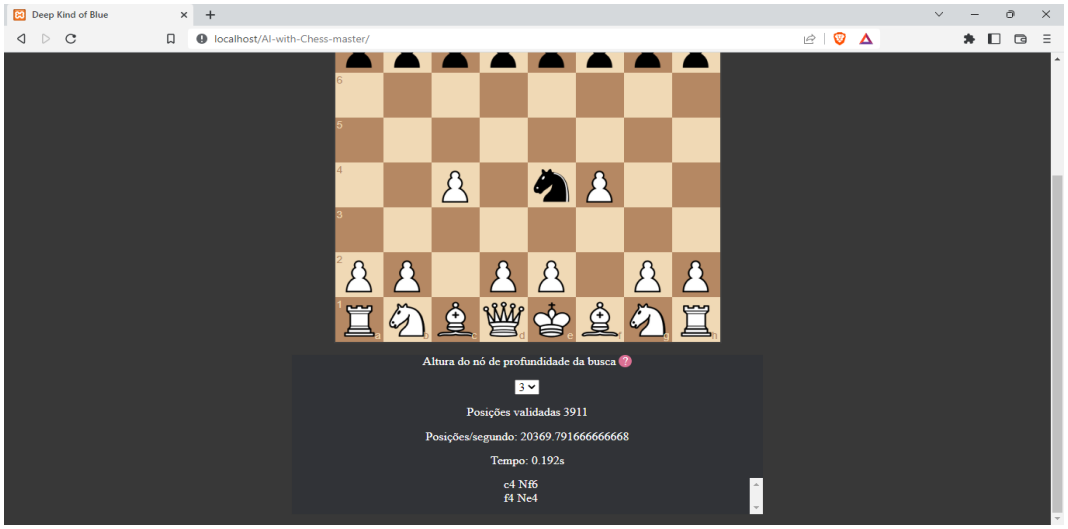


Figura 3 - Jogo de Xadrez com JavaScript

Fonte: Vandeilson Fernandes - Tela de Computador

Figura 3.1 - Jogo de Xadrez com JavaScript

Fonte: Vandeilson Fernandes - Tela de Computador

Para a geração de movimento foram usadas as bibliotecas *Chess* e *Chessboard*, elas por si só implementam regras de xadrez nos movimentos executados no tabuleiro, então consequentemente foi possível calcular todos os movimentos legais para um jogo de tabuleiro (ROSA, 2022, p.4).

A avaliação de posição foi a lógica usada para que uma peça do tabuleiro executasse a maior jogada possível naquele momento, visando que a peça de xadrez com o valor maior de prioridade pudesse se sobrepor por outra que tivesse um valor menor. E assim foi possível criar um algoritmo que também executasse a maior avaliação.

Foi utilizado também uma árvore de busca usando o *Minimax* que utilizada da busca em profundidade na teoria dos grafos a partir de um arvore de dados, então tomando a árvore recursiva de todos os movimentos possíveis que é explorado até determinada profundidade no algoritmo e a posição avaliada é dada nas folhas finais dessa árvore (ROSA, 2022, p.6).

A poda *alfa-beta* permite acrescenta velocidade nas buscas por profundidade utilizada pelo *Minimax* e permite concluir os melhores caminhos nas árvores melhorando ainda mais a execução da busca fazendo distinções dos caminhos avaliados e resultado no melhor e possuiu maior eficiência na ida de caminhos levam bons movimento no jogo (ROSA, 2022, p.8).

Buscando a melhoria da avaliação lógica inicial foi colocado também a avaliação aprimorada que levou possíveis posições das peças de xadrez dando exemplo que em busca da vitória a inteligência artificial buscou colocar sua peça na melhor posição possível no tabuleiro (ROSA, 2022, p.12).

Assim o jogo foi criado e determinado como o jogo básico de xadrez, mas ainda sim para um certo entendimento estratégico é necessárias algumas melhorias com um determinado números de implementações no código que pode ser até mesmo com algumas outras técnicas ou algoritmos para inteligência artificial.

5. CONSIDERAÇÕES FINAIS

Em finalidade de conseguir demonstrar alguns aspectos que possam beneficiar as

pessoas e buscar um maior entendimento em relação a Inteligência Artificial na *Web* foi descrito um pouco sobre sua história e algumas estruturas que a levam dentro de organizações e de algoritmos com a conclusão do apontamento do futuro de vários setores.

Buscando ainda um entendimento maior para demonstrar que a Inteligência Artificial na *Internet* é uma tecnologia benéfica, foi detalhado as linguagens, bibliotecas e algoritmos por trás dela buscando um maior entendimento naquilo que se transformam em ferramentas com a finalidade e o objetivo de melhorar trabalhos do cotidiano.

Em vista que alguns possíveis comportamentos a criação de um jogo com várias técnicas e bibliotecas que constituir uma Inteligência Artificial voltada para *Web* se tornou possível e plausível com a proposta da pesquisa, demonstrando ainda mais o ocorrer por trás de um sistema assim é que como todo sistema com variáveis tecnologias e linguagens pode estar sujeitos a erros e acertos, mas com uma aprendizagem contínua.

Pode-se dizer que sempre existem aspectos a mais que poderiam ser apontados e aspectos que poderiam ser ressaltados, mas como forma direta e esclarecedora o objetivo da pesquisa foi alcançado e detalhado entre os capítulos e tópicos.

Referências

CARVALHO, Castro. André Carlos Ponce de Leon Ferreira de Carvalho: **Inteligência Artificial:** riscos, benefícios e uso responsável**,** 2021. Disponível em: https://www.scielo.br/j/ea/a/ZnKyrcrLVqzhZbXGgXTwDtn/?format=pdf&lang=pt. Acesso em: 3 mar. 2021.

MIT Tech Review.TecMundo, 2021. **Nova IA da Google identifica em que parte do mundo uma foto foi tirada**. Disponível em: https://www.tecmundo.com.br/inteligencia-artificial/101252-nova-ia-google-consegue-identificar-onde-mundo-foto-tirada.htm**.** Acesso em**:** 7 out. 2021.

Positivo Tecnologia. **Conheça as 5 melhores linguagens de programação para Inteligência Artificial.** Disponível em: https://www.meupositivo.com.br/panoramapositivo/inteligencia-artificial-corporativo/. Acesso em: 14 ago. 2002.

Equipe Runrun.it.**Software de inteligência artificial: conheça mais de 30 ferramentas para adotar na sua gestão.**. Disponível em: https://blog.runrun.it/software-de-inteligencia-artificial/. Acesso em: 6 ago. 2002.

Jones Granatyr. **3 Linguagens para Inteligência Artificial.**. Disponível em: https://iaexpert.academy/2017/04/05/3-linguagens-para-inteligencia-artificial/ . Acesso em: 16 set. 2002.

Lucas Santos. **Pipeline operators no JavaScrip**t **.**. Disponível em: https://blog.lsantos.dev/pipeline-operators-javascript/ . Acesso em: 11 ago. 2002.

ADTsys. **Saiba quais são os algoritmos de aprendizagem usados na IA.**. Disponível em: https://www.adtsys.com.br/saiba-quais-sao-os-algoritmos-de-aprendizagem-usados-na-ia/ . Acesso em: 11 out. 2002.

Allan Valin. **A step-by-step guide to building a simple chess AI.** Disponível em: https://www.tecmundo.com.br/seguranca/3014-inteligencia-artificial-reconhecimento-de-padroes.htm/. Acesso em: 26 ago. 2002.

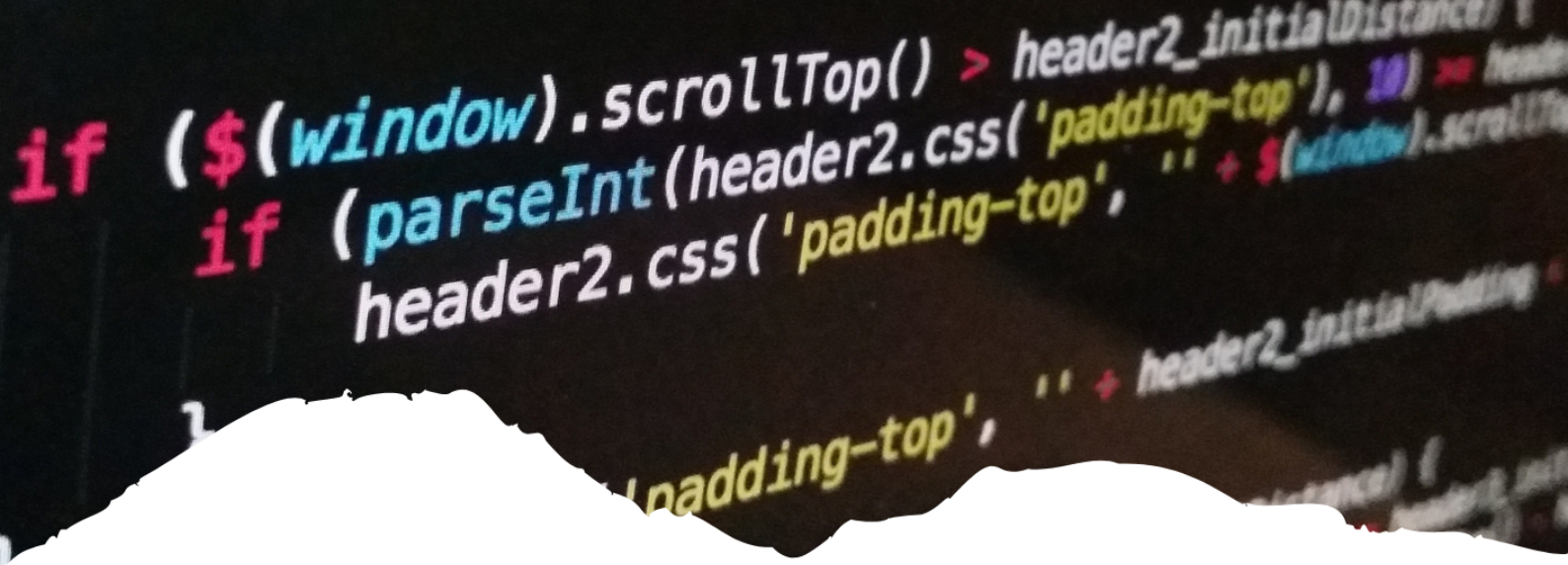
MARCH . **Conheça as 5 melhores linguagens de programação para Inteligência Artificial.**. Disponível em: https://www.freecodecamp.org/news/simple-chess-ai-step-by-step-1d55a9266977/ . Acesso em: 5 out. 2002.

Somanath Balakrishnan. **110 Open-Source Tools/Frameworks for Artificial Intelligence.**. Disponível em: https://dzone.com/articles/10-opensource-toolsframeworks-for-artificial-intel/. Acesso em: 14 ago. 2002.

Nick Ellisa. **Como usar o Midjourney para produzir artes feitas com inteligência artificial.**. Disponível em: https://olhardigital.com.br/2022/08/05/reviews/como-usar-o-midjourney-para-produzir-proprias-artes-com-inteligencia-artificial/. Acesso em: 17 out. 2002.

Alanis Meira. **Sites removem imagens geradas por inteligência artificial; entenda**. Disponível em: https://olhardigital.com.br/2022/09/22/internet-e-redes-sociais/sites-removem-imagens-geradas-por-inteligencia-artificial-entenda/. Acesso em: 17 out. 2002.

Santo Digital. **4 ferramentas de inteligência artificial que empresas já utilizam**. Disponível em: https://santodigital.com.br/4-ferramentas-de-inteligencia-artificial-que-empresas-ja-utilizam/. Acesso em: 25 out. 2002.



10

A EFICIÊNCIA DA INTELIGÊNCIA HUMANA NA EFICÁCIA DA INTELIGÊNCIA ARTIFICIAL: UM ESTUDO SOBRE A "COGNIÇÃO DAS MÁQUINAS" A FAVOR DAS PESSOAS

THE EFFICIENCY OF HUMAN INTELLIGENCE IN THE EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE: A STUDY ON "MACHINES COGNITION" IN FAVOR OF PEOPLE

Rafael Oliveira de Sousa

Mirian Nunes de Carvalho Nunes

Resumo

As últimas décadas foram decisivas na alteração das reações dos seres humanos com as ferramentas tecnológicas operadas pelas inteligências artificiais, até então havia apenas especulações e imaginação em torno de como se dariam as relações sociais entre seres humanos e "máquinas", contudo o que se observa são interações alicerçadas em conformidade com as diferentes necessidades humanas e tecnológicas/científicas. Dito isto, este trabalho tem como objetivo principal apontar as variadas formas de aplicabilidade da inteligência cognitiva na efetividade da inteligência artificial para o ser humano. Na busca desse objetivo utilizou-se como metodologia um levantamento bibliográfico em produções especializadas que pudessem corroborar e/ou abrir possibilidade de discursão quanto ao objetivo gerador. Dessa forma, ao se tratar das aplicabilidades da inteligência cognitiva em consonância com a inteligência artificial pode-se traçar um paralelo compreendendo as múltiplas inteligências enquanto faces eficazes na elaboração de novas tecnologias a serviço das necessidades humanas, ao passo disso chegou-se à compreensão de que ainda há um leque de possibilidades no que tange os estudos das Ciências Cognitivas considerando o campo das Inteligências artificiais a serviço dos seres humanos.

Palavras-chave: Ciência. Eficácia. Inteligências. Tecnologia.

Abstract

The last decades were decisive in changing the reactions of human beings with the technological tools operated by artificial intelligences, until then there was only speculation and imagination around how the social relations between human beings and "machines" would take place, however what is observed they are interactions based on different human and technological/scientific needs. That said, this work has as main objective to point out the various forms of applicability of cognitive intelligence in the effectiveness of artificial intelligence for humans. In pursuit of this objective, a bibliographic survey was used as a methodology in specialized productions that could corroborate and/or open up the possibility of discussion regarding the generating objective. In this way, when dealing with the applicability of cognitive intelligence in line with artificial intelligence, a parallel can be drawn, understanding the multiple intelligences as effective faces in the elaboration of new technologies at the service of human needs, at the same time we reached the understanding of that there is still a range of possibilities regarding the studies of Cognitive Sciences considering the field of Artificial Intelligences at the service of human beings.

Keywords: Science. Efficiency. Intelligences. Technology.

1. INTRODUÇÃO

As diversas ferramentas tecnológicas e digitais as quais utiliza-se no cotidiano são de um longo e exponencial salto qualitativo em pesquisas de produção e aprimoramento das técnicas e tecnologias do pós-segunda guerra mundial. A esse momento se convencionou chamar de quarta revolução industrial e nesse interim pudemos assistir à passagem de um mundo analógico para um mundo conectado pelas ligações digitais.

É interessante frisar que esse processo ocorre em um momento histórico de profundas transformações sociais, econômicas, culturais e políticas. Esses contornos ajudam a delinear as políticas voltadas para o desenvolvimento tecnológico que passamos a utilizar mais à frente. A inteligência artificial (IA) ganhou dimensões que não se imaginava, e ainda que se imaginasse, as reflexões ocasionadas por ela transformaram as percepções de outras ciências sobre o uso de máquinas que pensam.

Assim, a IA pode ser definida como um concatenar da inteligência humana e da inteligência cognitiva. Dessa correlação de inteligências surgem diferentes expressões sobre o estudo da mente, aplicabilidade da robótica e das IA a serviço dos seres humanos, questionamentos filosóficos sobre ética na produção e reprodução de seres pensam.

Nesse sentindo, ao refletir-se sobre as possibilidades de aplicabilidades da inteligência artificial em nosso cotidiano e que possa estar passo a passo com as necessidades sociais e humanas, levou-se ao seguinte questionamento gerador: de que forma a inteligência cognitiva aplicada à inteligência artificial pode trazer resultados assertivos, e, ser benéfica ao ser humano?

Na tentativa de trazer elementos que possam nos ajudar em nossa reflexão problematizadora lança-se em um árduo trabalho de revisão bibliográfica, buscando nas literaturas especializadas caminhos que pudessem trazer as respostas. Nessa senda caminhamos tendo como objetivo geral: apontar as variadas formas de aplicabilidade da inteligência cognitiva na efetividade da inteligência artificial para o ser humano.

Para auxiliar na busca do objetivo geral traçou-se os seguintes objetivos específicos: relacionar o conceito de eficiência, eficácia e efetividade com a inteligência humana, artificial e cognitiva; descrever a importância do estudo da inteligência humana para o desenvolvimento de novas tecnologias; entender como a inteligência cognitiva pode ser usada para melhorar a inteligência artificial; demonstrar as diversas aplicabilidades da inteligência cognitiva e sua relação com a efetividade da inteligência artificial.

Para fins metodológicos, este trabalho está dividido em três capítulos. O primeiro capítulo dedica-se a explicar as diferenças entre eficácia, eficiência e efetividade, assim como a relacionar esses conceitos a Inteligência Artificial e cognitiva demonstrando com as IA's podem de maneira efetiva trazer benéficos no cotidiano das pessoas, assim com chegar a um ponto onde a eficiência seja a máxima possível.

O segundo capítulo se deterá a demostrar e entender como a inteligência humana e cognitiva podem auxiliar na inovação tecnológica. Da mesma forma, apontamos as contribuições da inteligência cognitiva na formulação de uma inteligência artificial com fins de estabelecer relações tecnológicas com fins sociais, econômicos e humanos.

No terceiro e último capítulo são apresentados os elementos substanciais para se compreender a importância da aplicabilidade da inteligência cognitiva traçando um panorama comparativo com a inteligência humana e sua efetividade. Aqui se traz alguns elementos de fundo filosófico para dar corpo a essa compreensão.

Por fim, em nossa guisa de considerações finais apontando para a necessidade e importância de entendermos em fins tecnológicos e filosóficos da importância as múltiplas inteligências no coser de redes que possam demonstrar a aplicabilidade, ética, das IA's concatenada as necessidades humanas.

2. EFICÁCIA, EFICIÊNCIA, EFETIVIDADE E AS MÚLTIPLAS INTELIGÊNCIAS

No capítulo as seguir é posto a tarefa de relacionar o conceito de eficiência, eficácia e efetividade com a inteligência artificial e cognitiva. O intuito é poder estabelecer as bases para a compreensão da aplicabilidade da inteligência cognitiva à inteligência artificial, compreendendo que a ciência da cognição está assentada em um processo interdisciplinar, e por possuir essas estruturas disciplinares diversas, se configura como uma ciência que busca nas diferentes dimensões a compreensão da formação do aprender e do ensinar humano e não-humano (LIMA, 2003).

Em (1985) Donna Haraway lança o famoso "Manifesto Ciborgue" (2009), um ensaio sobre a necessidade da compreensão da relação que os seres humanos estabeleciam com outros seres e coisas não-humanas, essas relações estavam diretamente conectadas com as necessidades que se desenvolvem cotidianamente entre seres humanos e máquinas, a relação cotidiana com os corpos, modelagens das lutas, o feminismo, a luta política e a transformação do mundo do trabalho através dos saltos tecnológicos. A *priore* para ser algo não conveniente ao tratar da correlação entre as dimensões da eficácia no conjunto da aplicabilidade da inteligência cognitiva com a inteligência artificial, porém é necessário lembrar que essas relações são e se estabelecem quando refletimos a necessidade e construção destas nas interações cotidianas entre os seres humanos e os não-humanos.

Eficácia, eficiência e efetividade em primeiro momento se apresentam como sinônimos, ou mesmo com sentidos correlatos, mas é importante destacar que não o são, em seus radicais. A primeira trata da segurança de uma boa operação, a segunda traz o poder de ser efetivo como o mínimo de erros possíveis, e a última a capacidade de funcionar normalmente. Destacar essas diferenças é importante para pensar como a aplicabilidade na inteligência artificial pode se dar de forma efetiva, considerando o pensamento (a cognição) como algo que se aprende a partir das informações e dados que coletamos cotidianamente e como as máquinas, processadores, entre outros, podem desenvolver essa efetividade nos trabalhos cotidianos (READS, 2017).

Nesse sentindo é importante entender o que é inteligência artificial e inteligência cognitiva. A inteligência artificial tem suas raízes históricas com o desenvolvimento da Ciência da Cognição e é graças a ideia de IA que há um impulsionamento dessa ciência, segundo (GARNER, 2003 *apud* SARAIVA; ARGIMON, 2011) poderia até existir Ciência Cognitiva sem os computadores e a IA, mas é graças a Ciência da Computação que essa primeira ganha força.

2.1 Inteligência artificial e inteligência cognitiva

A inteligência artificial no decorrer do tempo sofreu diversas conceituações, para fins didáticos as dividiremos em duas grandes áreas: uma que busca a partir do pensamento e da racionalidade definir o que é uma inteligência artificial e outra que busca a partir da concepção comportamental traçar a ideia de uma IA. Porém, as primeiras ideias do que seria uma IA surge com Warrem Macculloch e Walter Pitts (1943). Eles buscaram através

de uma analogia às conexões neurais estabelecer uma relação entre um mecanismo que respondia de acordo com os estímulos entre “ligado” e “desligado” (MACCULLOCH; PITTS, 1943).

Alan Turing (1950) será o primeiro a articular uma concepção mais robusta sobre a inteligência artificial ao apresentar um teste onde o computador passaria no teste de um interrogador, humano, o questionasse e as respostas chegariam a um ponto onde o interlocutor já não pudesse mais distinguir se as respostas eram elaboradas por um mecanismo artificial ou humano. Nesse sentido, a ideia de inteligência tem como base a noção de cognição da inteligência humana.

Segundo Camargo (1999, p. 57):

> A Inteligência Artificial é o ramo da ciência da Computação que pesquisa a criação de sistemas inteligentes. A IA possui duas abordagens: uma científica, voltada ao estudo da psicologia cognitiva, para compreender os processos envolvidos na inteligência, e outra tecnológica, que lida com a representação destes processos através da máquina.

Nesse sentido, ao se tratar da I.A. está se abordando seus usos tanto em um contexto psicológico quanto sua dimensão tecnológica. A inteligência artificial ocupa espaços bastante comuns no cotidiano das pessoas. De acordo com Teixeira (1998, p. 13):

> Foi a partir do desenvolvimento da IA, nas últimas décadas, que toda a ideia de uma ciência da mente se desenvolveu. A IA proporcionou o passo fundamental para se tentar relacionar mentes e computadores e estabelecer o que passamos a chamar de “modelo computacional da mente”. Não fossem os desenvolvimentos e realizações da IA nas últimas décadas: suas máquinas de jogar xadrez, demonstrar teoremas matemáticos, realizar diagnósticos médicos, toda uma polêmica sobre a natureza da mente e da inteligência não teria surgido.

A inteligência artificial proporcionou um salto qualitativo nas ciências da computação e colocou em questões várias problematizações próprias de outras ciências, tais como a Antropologia, a Psicologia (uma ciência da mente?), da Linguagem e das teorias sobre aprendizado tais como as que estavam em choque como o behaviorismo e as concepções de Skinner.

A inteligência cognitiva está relacionada com a capacidade de relacionar habilidades e informações para melhorar o desempenho de aprendizado e raciocínio lógico. A ideia de construção dessas habilidades possui uma ligação com o pedagogo e psicólogo Alfred Binet (1857-1911) ao propor testes que pudessem quantificar e qualificar as diferentes dificuldades que as crianças possuíam, não somente a partir dos acertos, mas também dos erros nos testes. Contudo é com Jean Piaget (1896-1980) que esses estudos sobre Inteligência cognitiva ganham impulso, Piaget vai elaborar um quadro evolutivo sobre o desenvolvimento de múltiplas inteligências e inteligência cognitiva, porém não nos determos nessa questão agora.

Segundo Lemos *et al.* (2008, p. 85) seja nos testes de inteligência seja nas aprendizagens curriculares, apela-se ao exercício de funções cognitivas básicas (atenção, percepção, memória de trabalho) e de funções cognitivas superiores (compreensão, raciocínio, avaliação, resolução de problemas) comuns.

Nesse sentido, ao se tratar dessas inteligências enquanto elementos fundamentais

na construção da IA traz-se à baila a compreensão de que a inteligência humana é fator constitutivo em sua formulação, mas ao mesmo tempo compreende-se que o debate não se esgota aqui. O entendimento de quando um ser, seja ele da forma que for constituído, ganha habilidades próprias de entendimento e racionalização de si, temos uma cruzada filosófica sobre *self* e a vida (AFONSO, 2007; MIRANDA, 2002).

2.2 Eficácia, eficiência e efetiva e suas correlações com as inteligências

É indiscutível que o cérebro humano possui uma capacidade de processar informações e responder a elas de maneira efetiva, a inteligência humana é capaz de dar respostas a questões problemáticas de maneira eficiente quando consegue desenvolver as habilidades superiores da chamada inteligência cognitiva. É partindo dessa premissa que surgiram diversos estudos sobre o funcionamento dele para entender como algumas habilidades são trabalhadas (LEMOS *et al.* 2008).

O estudo da inteligência cognitiva viabilizou a possibilidade de melhorá-las. Partindo dessa premissa, a Inteligência Artificial (IA) surgiu do projeto de estudiosos de várias áreas como um braço da inteligência cognitiva dentro da área de estudo chamada de Ciência Cognitiva, para compreender e replicar os comportamentos humanos considerados inteligentes (TIBERIUS, 2016).

Observa-se que existe uma importante relação direta entre a eficiência da inteligência humana para que haja então a eficácia da inteligência artificial, uma vez que, resumidamente a eficiência se refere ao custo, meio de estudo e de resolução de problemas – no caso a própria inteligência humana; e, eficácia nada mais é que o resultado, o que precisa ser feito para maximizar as soluções – a inteligência artificial. Se a inteligência humana não for empregada de forma assertiva e com todo seu potencial a inteligência artificial não obtém os resultados esperados e não atinge seu objetivo (READS, 2017).

Tiberius (2016 p. 16) afirma que na comparação das características de psicologia cognitiva entre o cérebro e os computadores modernos é muito para efeitos expositivos dos conceitos básicos de memória, inteligência e requisitos de funcionamento do sistema. Esse contexto vai de encontro a visão de Reads (2017) que cita que a maior dúvida das pessoas é pensar que as máquinas estão a substituir as tarefas humanas, em termos laborais, fazendo o ser humano perder espaço, todavia, não podemos ter a real certeza, visto que a IA permanece auxiliando pessoas em suas rotinas, trazendo comodidades e aperfeiçoando técnicas, até certo ponto as máquinas ainda dependem da intervenção humana para tomadas de decisões, esse é o fundo do debate filosófico no que tange a autonomia e a ideia de vida.

Diversos tipos de dispositivos dos mais variados possíveis aprendem a utilizar o conhecimento e a cognição, incluindo entonação de voz por meio da I.A, algo que cresce rapidamente cada vez mais, esse processo de aprendizado se dá com base na concepção da efetividade da cognição humana e busca em um paralelo desenvolver a inteligência artificial construindo o máximo de eficiência. Toda essa desenvoltura acontece por meio da simulação dos pensamentos e das ações do ser humano, e é compreendida por um campo específico da ciência chamado de aprendizado de máquina ou *Machine learning* (PACHECO; PEREIRA, 2018).

O termo *Machine learning* é parte do conceito de inteligência artificial é a área da computação que estuda e viabiliza as possibilidades de as máquinas realizarem tarefas que poderiam ser feitas pelos seres humanos. Sendo assim, a programação utilizada nos

computadores é baseada em algoritmos, que são sequências definidas e compostas de informações, dados e instruções para serem seguidas pela máquina. Com essas sequências, o sistema da máquina consegue tomar decisões a respeito de determinada situação (SAMUEL, 1959).

Como um subcampo do aprendizado da máquina, tem-se a *deep learning* que é um tipo de *machine learning*, uma prática inteligente que possui os algoritmos com uma funcionalidade diferente, a própria máquina gera automaticamente propriedades que não variam mesmo quando aplicadas a um conjunto de transformações, sem precisar de ajuda humana. Neste caso, o computador aprende sozinho a reconhecer padrões de dados em várias camadas de processamento realizando tarefas como seres humanos (PACHECO; PEREIRA, 2018).

A aplicabilidade da inteligência cognitiva para a efetividade da inteligência artificial está cada vez mais acessível por meio do uso da *machine landing e deep learning,* uma vez que a efetividade se refere à transformação obtida do resultado da eficiência da inteligência humana na eficácia da inteligência artificial, ou seja, a efetividade aqui é o impacto.

Dado a importância do aprendizado de máquina e seu imenso potencial, aplicações do tema em segmentos distintos, já são muito utilizadas trazendo grandes benefícios nas áreas pública e privada. Segundo Nivio Ziviani, cofundador da empresa Kunumi e professor emérito da Universidade Federal de Minas Gerais (UFMG), em entrevista à 17ª edição da revista Fonte (2017, p.8) afirmou que:

> Uma maneira de se avaliar onde o aprendizado de máquina é útil é pensar que o que é fácil para os seres humanos processarem é geralmente difícil para se programar em computadores, tais como problemas que resolvemos intuitivamente, que sentimos automaticamente, como reconhecer palavras faladas ou faces em imagens. Mas o que é penoso ou repetitivo para os humanos, é mais fácil programar para as máquinas, como dirigir veículos ou emitir um diagnóstico médico a partir de uma imagem.

A inteligência artificial aplicada no setor médico, tem sido crucial para crescer o número de salvamento de vidas quando o assunto é Sepse. A Laura, o primeiro robô cognitivo gerenciador de risco do mundo, pôde comprovar essa tese, utilizando seus algoritmos para comprovar a existência de uma infecção generalizada, possibilitando diagnósticos precoces (PACHECO; PEREIRA, 2018).

O campo de aplicabilidade da IA tem crescido e se desenvolvido cada vez mais, são várias as áreas onde a Inteligência Artificial tem sido empregada, e sua eficácia está sempre em paralelo com as capacidades e habilidades de efetividade da inteligência humana, ao mesmo tempo que as IA's também estão ganhando autonomia no processo de dados e informações mais robustas, sendo assim é notório que há uma real eficiência dessas nas atividades humanas das mais simples as mais complexas (READS, 2017).

Nesse sentido, é importante que se pense como se constroem as relações entre as diferentes inteligências, considerando a interações entra a inteligência cognitiva, humana e artificial tendo como horizonte a formulação de novas tecnologias que tragam facilidades e na criação de outras habilidades para os seres humanos. O capítulo a seguir vai se dedicar a traçar esses paralelos considerando entre as interações e diferenças das múltiplas inteligências (PACHECO; PEREIRA, 2018).

3. INTERAÇÃO DA INTELIGÊNCIA HUMANA, COGNITIVA E ARTIFICIAL E AS NOVAS TECNOLOGIAS

De acordo com Binet & Simon (1905), compreender os meandros da inteligência humana se configura como uma tarefa árdua e extremamente complexa, há diversos fatores, e questões de fundo epistemológico que influenciam na compreensão, uma vez que, essas questões (como no aspecto analítico e comportamental) podem dar um direcionamento diferente na compreensão do que podemos entender enquanto inteligência humana.

No fundo psicológico a inteligência humana possui vieses que nos levam a entendimentos distintos, nesse sentido, e compreendendo a inteligência humana numa perspectiva holística de múltiplas configurações e operacionalidades, lança-se no capítulo seguinte a descrever com os estudos da inteligência humana causam um impacto significativo na formulação de novas técnicas e tecnologias (MIRANDA, 2002).

3.1 A inteligência humana em quatro visões paradigmáticas

No interim da compressão do que podemos definir como inteligência humana ao menos 4 visões paradigmáticas vã dominar as concepções de inteligência humana ao longo da história, nos interessa essas construção temporal-histórica, na medida em que, podemos traçar os paralelos da construção de tecnologias e seus impactos na história e ciência.

A primeira visão paradigmática a dominar o entendimento de inteligência humana é o paradigma biológico que possui suas origens ainda na Grécia antiga com Hipócrates (460- 377 a.c.), e assim vai ganhando mais adeptos como Frantz Joseph Gall (1758-1828) já no iluminismo até D. Hebb (1949) e Cattel (1987), onde a questão biológica, no caso do cérebro, é a questão central que faz girar a ciranda da criação da inteligência humana. Esses autores dão um enfoque na formação do crânio, do estudo da massa encefálica, assim como uma valorização dos estudos das atividades cerebrais. Os estudos dessas atividades acionam outras ciências como neurobiologia, e buscam o entendimento da formação da inteligência e da cognição em uma explicação biológica.

Segundo Maria Miranda (2002, p. 22):

> Os estudos da atividade cerebral têm examinado a relação entre a estrutura e o funcionamento do cérebro e o processamento da informação: velocidade da condução neuronal, potenciais evocados, metabolismo da glucose, especialização hemisférica. (...) Na área da neurobiologia, os trabalhos do cientista português Antônio Damásio na Universidade de Iowa constituem uma referência incontornável do final do último milênio. O conceito básico da obra mundialmente famosa (Damásio, 1994) é relativamente simples: na terminologia cartesiana, não há *res cogitans* sem *res extensa* = não há *cogito* sem corpo = não há pensamento sem o substrato neurobiológico.

Podemos perceber que há uma discussão de fundo epistemológico para o autor citado por Maria Miranda (2002), pois ao destacar a concepção de existir na perspectiva cartesiana o corpo enquanto um substrato não está alocado dentro desse ser, é algo alheio, dessa forma, por se tratar de um paradigma biológico não se pode escamotear os estudos neurológicos da formação do pensamento, ou da inteligência humana.

O paradigma diferencial se alicerça na premissa da individualidade de cada sujeito. Nessa perspectiva o construto da inteligência humana faz parte de uma dimensão maior,

mas que se delimitam pelos limites que há em cada dimensão. Segundo (MIRANDA, 2002, p. 22) para o paradigma da diferença o foco está centrado no entendimento avaliativo, “a avaliação é o ponto de partida (averiguação da variabilidade do desempenho), a avaliação é o ponto de chegada (indicadores de competência (s) e partilha da informação favorecedora do autoconhecimento).”

Para Afonso (2007, p. 121-122):

> As teorias tradicionais da inteligência, designadamente as originárias do paradigma diferencial de investigação, tenderam a sobrevalorizar a caracterização da inteligência em termos de estrutura interna (g, aptidões, estrutura das condutas cognitivas, perfil das aptidões) e a negligenciar a relação com o contexto como aspecto definidor da inteligência. Este, como se viu, é tomado como aspecto nuclear nas teorias sistémicas da inteligência.

Para o paradigma construtivista o processo de formulação da inteligência humana está associado diretamente as dinâmicas de adaptabilidade que o ser humano possui ao meio em que está inserido, essas adaptações se dão no plano intelectual e se estende pelas ações. Jean Piaget é o expoente máximo desse paradigma, mesmo não sendo da área da Psicologia tinham como método um pensamento centrado na lógica e partido desse uma grande formulação epistêmica. Segundo Miranda (2002, p. 23) “no construtivismo psicogenético, o desenvolvimento é uma marcha para o equilíbrio, e cada construção integra e reorganiza, num plano superior, as que a antecedem”.

Dito isto, para o paradigma construtivista as habilidades de inteligências humanas nas formulações de tecnologias se dão a partir de um processo de interação dos sujeitos com os diferentes estímulos que recebem, essa sucessão de desenvolvimento intelectual (instigada) faz parte de uma marcha evolutiva de transformação intelectual/tecnológica humana.

No paradigma informacional há um polo central fincado no entendimento de como se dá o processamento da cognição, aqui os processos (programas) são valorizados como componentes fundamentais para o desenvolvimento da cognição humana e seus desenvolvimentos (MIRANDA, 2002). Nesse sentindo, há uma forte consolidação dos estudos voltados para o raciocino lógico aliados a uma base de aptidões (STERNBERG, 1977).

Ao apresentarmos as visões paradigmáticas e torno da compreensão da inteligência humana queremos fazer emergir as contribuições epistemológicas em torno da construção de um entendimento sobre as múltiplas intersecções da inteligência humana. Podemos entender a inteligência humana como uma série de qualidades, diferentes em cada indivíduo, que é exercida no dia a dia, transpassada pelo processo que leva a cognição de determinadas situações (MIRANDA, 2002) e ao mesmo tempo é a articulação de diferentes aspectos em uma compressão sistêmica, integrada e compreensível (STERNBERG, 1977).

Dito isto, ao traçarmos os paralelos possíveis aos paradigmas mencionados anteriormente podemos ver que a formulação de um pensamento computacional, alicerçado ao desenvolvimento do entendimento da inteligência humana, caminha par a par as transformações destas dimensões da Ciência Computacional. As tecnologias possíveis se dão na mesma proporção em que a investigação da capacidade humana se desenvolve.

3.2 A inteligência cognitiva e os saltos tecnológicos na inteligência artificial

Retomamos neste tópico um ponto importante para seguirmos, a ideia de inteligência cognitiva. A inteligência cognitiva está relacionada com a capacidade de relacionar habilidades e informações para melhorar o desempenho de aprendizado e raciocínio lógico. A ideia de construção dessas habilidades possui uma ligação com o pedagogo e psicólogo Alfred Binet (1857-1911) ao propor testes que pudessem quantificar e qualificar as diferentes dificuldades que as crianças possuíam, não somente a partir dos acertos, mas também dos erros nos testes.

Assim como no paradigma construtivista, Jean Piaget será peça-chave na formulação das ideias de inteligência cognitiva. Os processos (programas) de adaptabilidade darão contornos significativos para elaboração dos entendimentos da cognição das I.A. Nesse sentido, nos é interessante a partir dessa perspectiva epistemológica a construção de Inteligências artificiais que possam corroborar em atividades benéfica aos seres humanos (TIBERIUS, 2016).

Dito isto, ao considerarmos que o estudo da inteligência cognitiva pode nos levar a compreender e desenvolver capacidades que estão além do que possuímos agira, isso pode ser aplicado também as I.A. na medida em que a correspondência do desenvolvimento dessas inteligências é operada pelo ser humano tais como: *machine learning*, as redes neurais, *deep learning* e processamento de linguagem natural (LIMA, 2007).

Outro ponto relevante é compreender, assim como Mueller e Massaron (2018) que a inteligência artificial não algo feito para suplantar a inteligência e processo de cognição humana. O que temos são I.A. que são modeladas a partir de uma simulação da inteligência humana. Conforme Neves (2020) a Inteligência Artificial está baseada em algoritmos que busca atingir um objetivo, o autor ainda afirma que:

> A Inteligência Artificial (IA) foi mal compreendida ao longo dos anos, em parte porque as pessoas realmente não entendem do que se trata a IA, ou mesmo o que ela deve e pode realizar. Uma parte significativa do problema é que filmes, programas de televisão e livros conspiraram para dar falsas esperanças quanto ao que a IA realizará. Além disso, a tendência humana de antropomorfizar (dar características humanas) à tecnologia faz parecer que a IA deve fazer mais do que realmente ela pode executar (NEVES, 2020, p. 187).

Dentro desse campo dos estudos da inteligência artificial outro campo vem evoluindo e ganhando um terreno bastante fértil na produção de novas formas de fazer tecnologia, é a Computação Cognitiva (CC) se destacando por abranger um campo vasto de outras ciências como a Ciência da Computação, Ciência da Informação, Big Data, inteligência e cognição no intuito de compreender o funcionamento do pensamento da inteligência natural e processamento de informações não somente pré-estabelecidas mas a partir de um conjunto de possibilidades (WANG *et al.,* 2010).

O que temos é o desenvolvimento de componentes e *softwares* que conseguem executar tarefas sem a intervenção direta do ser humano, possuem a capacidade de elaborar soluções a partir da combinação de diferentes dimensões complexas e não somente da combinação de dados e de respostas programadas. A problemática do uso da inteligência artificial, além dos levantados pelo cinema entre outros, se dá no campo das ciências sociais e humanas aplicadas (READS, 2017; NEVES, 2020), na relação entre o uso da computação cognitiva e a retirada de postos de trabalhos de seres humanos.

Dito isto, a inteligência cognitiva aplicada a inteligência artificial produz saltos qualitativos no que concerne a aplicabilidade de soluções tecnológicas a determinados espaços de trabalho, seja na área médica até ao cotidiano das pessoas como o desenvolvimento das atendentes virtuais das lojas de departamento, de bancos virtuais e físicos (WANG *et al.,* 2010).

Nesse sentindo é importante que se pense como se dá essa aplicabilidade da inteligência cognitiva correlata ao processo de inteligência artificial. Para isso, o terceiro capítulo se dedicará a compreender como essas correlações são instituídas no processo de desenvolvimento de novas tecnologias aliadas as necessidades humanas e das próprias ciências que se estabelecem no decorrer (CAMARGO, 1999).

4. APLICABILIDADES DA INTELIGÊNCIA COGNITIVA E A EFETIVIDADE DA INTELIGÊNCIA ARTIFICIAL

Sem dúvidas as ciências voltadas para o entendimento do funcionamento da inteligência humana sofreram transformações profundas e marcam avanços na produção de soluções para problemas que relacionam o pensamento e a ação humana. Ao tratar dessas questões pretende-se apontar a aplicabilidade das inteligências cognitivas no cotidiano das pessoas principalmente ao se traçar um paralelo com a efetividade da inteligência artificial (WANG *et al.* 2010).

Neste capítulo se dedicará a demonstrar a relação entre a aplicabilidade da inteligência cognitiva e a efetividade da inteligência artificial. Aponta-se da mesma forma a produção de recursos tecnológicos e a presença da inteligência artificial em vários aspectos da vida cotidiana das pessoas. (CAMARGO, 1999).

4.1 A inteligência cognitiva e as tecnologias cognitivas

Observa-se nos últimos anos um avanço significativo das tecnologias cognitivas em diversos campos da vida humana, desde as a operação na Bolsa de Valores até o campo da medicina. Esses saltos tecnológicos evidenciam a relação íntima entre a produção de uma inteligência e ciência cognitiva como ferramenta eficaz nas relações sociais dos indivíduos. Da mesma forma, evidencia uma ocupação maior de um trabalho não-humano, mas que estabelece relações de trabalho diferenciadas (NISTA-PICCOLO *et al.*, 2002).

As tecnologias cognitivas são bastante utilizadas nas empresas que trabalham com cibersegurança, um ramo que tem crescido bastante nos últimos anos, principalmente com as dimensões da internet onde os usuários e empresas podem se valer de ferramentas digitais e da própria inteligência artificial para diversos fins tais como: propaganda, venda de produtos e ataques cibernéticos (NISTA-PICCOLO *et al.*, 2002).

Segundo Cunningham (2019 *apud* FORCEPOINT, 2019) umas das principais cientistas da Forcepoint destaca as dimensões interdisciplinares que compõe a cibersegurança centrada nos seres humanos. São ao menos seis disciplinas, entre elas: Antropologia, Psicologia, Filosofia, Neurociência, Linguística e inteligência Artificial.

Para Margareth Cunningham (2019 *apud* FORCEPOINT 2019):

> A cibersegurança na neurociência tem impactado profundamente o processamento de informações, design de redes, modelagem computacional e desenvolvimento de sensores — e continua a inspirar inovações na construção

> de ferramentas para melhorar a representação do conhecimento e do raciocínio em tecnologia.

Essas inovações afetam da mesma forma o próprio entendimento do funcionamento dos processos de formulação do pensamento humano. O raciocínio em tecnologia proporciona uma ampliação do desenvolvimento da ciência cognitiva, trazendo eficácia em determinadas tarefas, uma vez que, a memória das inteligências artificias quando relacionando com ciência cognitiva não produzem informações que serão esquecidas (TACCCHELLA *et al.,* 2017).

Margareth Cunningham (2019 *apud* FORCEPOINT 2019):

> O que descobrimos ao considerar as complexas influências biológicas e ambientais na cognição é que o campo da ciência cognitiva deve fundir e equilibrar *insights* de múltiplas disciplinas. Da mesma forma, a cibersegurança eficaz requer várias fontes e tipos de informações para construir uma compreensão dos sistemas de tecnologia e suas vulnerabilidades. Quando desafiada com a tarefa de proteger e compreender um sistema grande e cada vez mais distribuído, um único indicador de uma única disciplina não é adequado. Vamos explorar algumas definições básicas das disciplinas de ciências cognitivas, e como elas impactam tanto a ciência cognitiva quanto a cibersegurança.

O que se observa é uma forma aplicada e eficaz da inteligência cognitiva, em especial da ciência cognitiva, em situações de máxima importância. Vê-se cada vez mais os Estados Nacionais se valerem de tecnologias com inteligência artificial e cognitiva na proteção de informações econômicas e desenvolvimento de tecnologias (SECURITY REPORT, 2019).

Um setor em que a inteligência cognitiva ganha bastante terreno em sua aplicabilidade é no setor administrativo onde cada vez mais são usadas inteligências artificiais que traçam diversos paralelos entre os dados obtidos para poder apontar as melhores decisões considerados diversos cenários e suas instabilidades. O interessante nessa aplicação é o próprio processo de aprendizado que fica registrado pela I.A. o que corrobora com outras tomadas de decisões que surgirão (SECURITY REPORT, 2019).

Um campo que vem ganhando forte influência das tecnologias que usam a I.A. e buscam é o campo da educação. As estratégias usadas através da gameficação[1] vem ganhando terrenos bastes promissores, cada vez mais vem a entrada de aplicativos, plataforma, o uso da robótico e de campos da ciência da cognição que estimulam os estudantes a interagirem e se valerem desses recursos para as aulas e para o cotidiano (SARAIVA, 2011).

Segundo Revel e Scardua (2021, p. 13-14) em seus estudos sobre a adoção da gamefication, "as referências encontradas confirmam a eficácia da gamificação como potencializador de aprendizagem em disciplinas de cursos superiores, em especial quando os conteúdos são por demais teóricos". Chama atenção a diversidade dos campos de conhecimento nos quais a gamificação foi aplicada com sucesso. Chama a atenção também a aparente falta 14 de trabalhos em língua portuguesa aplicando gamificação ao ensino de IA em um curso de engenharia, que é a essência desse projeto de intervenção pedagógica.

Os autores elaboram um projeto de intervenção pedagógica dentro do curso de Ciência da Tecnologia e utilizaram a gameficação para conseguir explicar o funcionamento das I.A. para isso fizeram uma busca e puderam constar que há uma expansão do uso da

1 Gamificação (ZICHERMANN; CUNNINGHAM, 2011 *apud* DEVELY; SCARDUA 2021) consiste em utilizar elementos dos jogos no contexto educacional, com o intuito de motivar o estudante a aprender, envolvendo-o em um ambiente no qual o aprendizado se dá por meio de atividades lúdicas.

gameficação e das I.A. no processo educacional.

4.2 A eficácia da inteligência artificial

Se observou até aqui as diversas aplicabilidades dos estudos a inteligência cognitiva e sua eficácia em atividades tanto do cotidiano quanto de áreas mais restritas como a medicina. Da mesma forma, se apresentou os diferentes usos das I.A. em atividades que vão desde o plano pedagógico nas universidades e escolas, quanto em processo de compra e venda através de App's, sites etc., passando por questões mais complexas como os sistemas de Segurança dos Estados Nacionais (TACCCHELLA *et al,* 2018; NISLA-PICCOLO *et al.*, 2002).

Dentro deste tópico pretende-se salientar a eficácia da inteligência artificial, trazendo exemplos que possam corroborar as afirmações que consolidem o entendimento das I.A. enquanto ferramentas possíveis e baseadas na lógica e necessidade humana e não enquanto máquinas destruidoras como nas histórias fantasiosas do cinema.

Para Cabral e Figueiredo (2020) a I.A. aplicada a organização da administração pública possui efeitos significativos no que concerne e efetividade de do *Machine learning* onde as I.A. fortes conseguem através das experiências anteriores criar um acúmulo de aprendizados capaz de auxiliar na organização das diversas dimensões do qual o Poder Público cuida como saúde, educação, segurança pública, entre outros.

Os autores Cabral e Figueiredo (2020) destacam ainda que o *Machine learning* aplicado as I.A. não proporcionam a substituição direta da mão de obra humana, mas há redução e/ou alteração nas funções desempenhadas pelos humanos, pois com essa inserção há uma transformação real na lógica do trabalho, algo que é bastante pertinente nas críticas das ciências sociais e humanos aplicadas.

Na medicina se observa a utilização tanto na *machine learning* quando do *deep learning*, considerando as limitações que são inerentes ao próprio ser humano, por isso a necessidade de utilização de I.A. que possam elaborar diferentes camadas de possibilidades de resolução cirúrgica ou mesmo de diagnósticos. Segundo Taccchella (*et al.,* 2018) e Nisla-Piccolo (*et al.*, 2002) os avanços obtidos a relação hibrida entre seres humanos e "máquinas" atingem capacidades prognósticos de algoritmos muito mais superiores aos obtidos dentro do nicho fechado aos pares humanos.

Segundo Braga (*et al*., 2022, p. 940):

> a inteligência artificial mostra-se ineficaz ao não conseguir sustentar uma boa relação médico-paciente. O computador fornece o diagnóstico, e ao médico cabe o conhecimento da fisiopatologia dos processos orgânicos e o desenvolvimento das habilidades de ouvir, examinar e orientar um paciente e, consequentemente, propor um diagnóstico e um tratamento de seu problema de saúde, acompanhando sua evolução.

Como havia sido destacado anteriormente as I.A. possuem as limitações que lhes são inerentes, até então, na medida em que necessitam do ser humanos para estruturação enquanto inteligência e funcionamento, sendo assim, há funções em que as I.A. não operam, pois não possuem habilidades para fazer.

5. CONSIDERAÇÕES FINAIS

Chega-se à guisa das considerações finais com elementos pertinentes no que concerne a aplicabilidade da Inteligência artificial no cotidiano dos seres humanos, pode-se traçar ao longo do trabalho um leque de elementos que corroboram com aquilo a que se propôs a refletir, sobre como as múltiplas inteligências podem estar concatenadas as necessidades humanas, da mesma forma que se pode atender aos objetivos específicos em questão.

Compreendeu-se que inteligências são essas e como elas estão coadunas na formulação de um pensamento computacional ligado a criação de novas tecnologias capazes de auxiliar os seres humanos em suas tarefas cotidianas, em atividades essenciais, bem como em questões relacionadas a vida.

Traçou-se as correlações de como se dá o processo de interação entre as inteligências artificial, cognitiva e humana ao pensarmos *constructos* e novas ferramentas tecnológicas, destacou-se a necessidade do entendimento das inteligências humanas em quatro dimensões paradigmáticas. Nesse ínterim pôde-se destacar a relação intricada que as ciências da computação, da cognição possuem com a psicologia e a filosofia, ao se fazer as reflexões que gravitam em torno do que a mente humana e redes neurais podem operar.

Demonstrou-se a aplicabilidade real da inteligência artificial com exemplificações tanto na área da saúde, quanto do processo educacional. A pandemia de Covid-19 é um dos momentos históricos da saúde mundial em que as tecnologias operadas por inteligência artificial tiveram um grande prestígio, principalmente no que tange a dinâmicas do processo educacional, como a própria *gameficação*. Dessa forma, ao tratar da aplicabilidade da I.A. traçou-se um panorama geral dessa contribuição em várias dimensões cotidiano humano.

Dito isto, o campo de pesquisa em torno da Inteligência Artificial e suas aplicabilidades é vasto e se configura de maneira interdisciplinar, trazendo à baila outras ciências que corroboram com a construção de técnicas e tecnologias úteis a necessidade humana. Essa vastidão com campo de pesquisa e aplicabilidade deixa um leque de aberto de possibilidades a serem abordadas, que vão desde dimensões psicológicas a dimensões filosóficas em torno da vida e programação de IA's.

Referências

AFONSO, Maria João. **Paradigmas diferencial e sistémico de investigação da inteligência humana**: perspectivas sobre o lugar e o sentido do construto (Tese de doutoramento. Faculdade de Lisboa, 2007.

BRAGA, Ana Vitória. *Et al*. **Inteligência Artificial na Medicina**. v. 2 (2018): III CIPEEX - Ciência para a redução das desigualdades. Publicado em 2022. Disponível em: http://anais.unievangelica.edu.br/index.php/CIPEEX/issue/view/78. Acesso em: 10 de nov. 2022.

CAMARGO, Kátia Gavranich. **Inteligência Artificial aplicada a Nutrição na prescrição de planos alimentares.** 1999. 252 f. Dissertação (mestrado em engenharia) – Universidade Federal de Santa Catarina – UFSC, Florianópolis, 1999.

CATTELL, R.B**. Intelligence: its structure, growth and action.** Amsterdam: North-Holland, 1987.

FONTE. **Computação cognitiva e a humanização das máquinas**. Prodemge, Minas Gerais, Ed. 17, p. 3, 07 de jul. 2017. Disponível em: https://www.prodemge.gov.br/revista-fonte/Publication/19-Computacao-cognitiva-e-a-humanizacao-das-maquinas. Acesso em: 27 de mar. 2022.

FORCEPOINT**. A relação da ciência cognitiva na cibersegurança.** Disponível em: https://inforchannel.com.br/2019/02/21/forcepoint-a-relacao-da-ciencia-cognitiva-na-ciberseguranca/ Redação Acesso em: 21 fev. 2019.

HARAWAY, Donna J., “A Cyborg manifesto: science, technology, and socialist feminism in the late twentieth century” In: *Simians, cyborgs, and women: the reinvention of nature,* New York, Routledge, 1991. Trad. Bras. Tomaz Tadeu. In:

HARAWAY, Donna; KUNZRU, Hari & TADEU, Tomaz. **Antropologia do ciborgue: As vertigens do pós-humano.** Belo Horizonte, Autêntica, 2009.

HEBB, D.O. **The organization of behavior. A neuropsychological theory**. New York: Wiley, 1949.

LEMOS, Gina; ALMEIDA, Leandro S.; GUISANDE, M. Adelina; PRIMI, Ricardo. Inteligência e rendimento escolar: análise da sua relação ao longo da escolaridade. **Revista Portuguesa de Educação**, vol. 21, núm. 1, 2008, pp. 83-99 Universidade do Minho Braga, Portugal, 2008.

LIMA, G.A.B. Interfaces entre a ciência da Informação e a ciência cognitiva. **Ciência da Informação**. jan/abr. 2003, 32 (1), 77-87. Disponível em: http://www.ibict.br/cienciadainformacao/viewarticle.php?id=166&layout=abstract. Acesso em: 28 maio 2007.

MACCULLOCH, W.; PITTS, W. **A logical Calculus of Ideas Immanent in Nervous Activity**. Bull. Mathematical Biophysics, Vol. 5. 1943.

MIRANDA, Maria José. A inteligência humana: contornos da pesquisa. **Paidéia (Ribeirão Preto)** [online]. 2002, v. 12, n. 23, pp. 19-29. Disponível em: <https://doi.org/10.1590/S0103-863X2002000200003>. Epub 29 Jul 2009. ISSN 1982-4327. https://doi.org/10.1590/S0103-863X2002000200003. Acesso em: 25 out. 2022.

MUELLER, J.P.; MASSARON, L. **Artificial Intelligence.** New Jersey: John Wiley & Sons, 2018.

NEVES, B. C. Inteligência artificial e computação cognitiva em unidades de informação: conceitos e experiências. **Logeion: Filosofia da Informação**, *[S. l.]*, v. 7, n. 1, p. 186–205, 2020. DOI: 10.21728/logeion. 2020, v.7, n.1.p186-205. Disponível em: https://revista.ibict.br/fiinf/article/view/5260. Acesso em: 17 nov. 2022.

NISTA-PICCOLO, Vilma Lení. SILVA, Yara Machado da. MELLO, Flora Loureiro de. **A inteligência humana e o cotidiano escolar**. Série-Estudos, Campo Grande, MS, v. 23, n. 47, p. 27-41, jan./abr. 2018. Disponível em: file:///C:/Users/Erick%20Reis/Downloads/1114-Texto%20do%20artigo-2630-2953-10-20180412.pdf. Acesso em: 10 de nov. 2022.

PACHECO, C. A. R.; PEREIRA, N. S. Deep Learning Conceitos e Utilização nas Diversas Áreas do Conhecimento. Revista **Ada Lovelace, *[S. l.]*, v. 2, p. 34–49, 2018.** Disponível em: http://anais.unievangelica.edu.br/index.php/adalovelace/article/view/4132. Acesso em: 7 out. 2022.

READS, Smart. Inteligência Artificial: Compreender o que consiste a I.A e o que implica a aprendizagem das máquinas**.** *In:* Cap. **5: A tomada de decisões das máquinas da inteligência artificial.** Bebelcube, Inc., 2017.

SAMUEL, Arthur L. **Some Studies in Machine Learning Using the Game of Checkers**. IBM Journal of Research and Development. – 1959.

SARAIVA, C. A. E.; ARGIMON, I. I. DE L. Ciência da computação e ciência cognitiva: um paralelo de semelhanças. **Ciências & Cognição**, v. 12, 2 abr. 2011.

SCARDUA, Leonardo Azevedo. DEVELLY, David. Paolini. **Gamificação no ensino de inteligência artificial aplicada à engenharia de controle e automação.** Instituto Federal do Espírito Santo, Campus Santa Teresa, 2021. Disponível em: http://anais.unievangelica.edu.br/index.php/CIPEEX/article/view/2997/1348. Acesso em: 10 de nov. 2022.

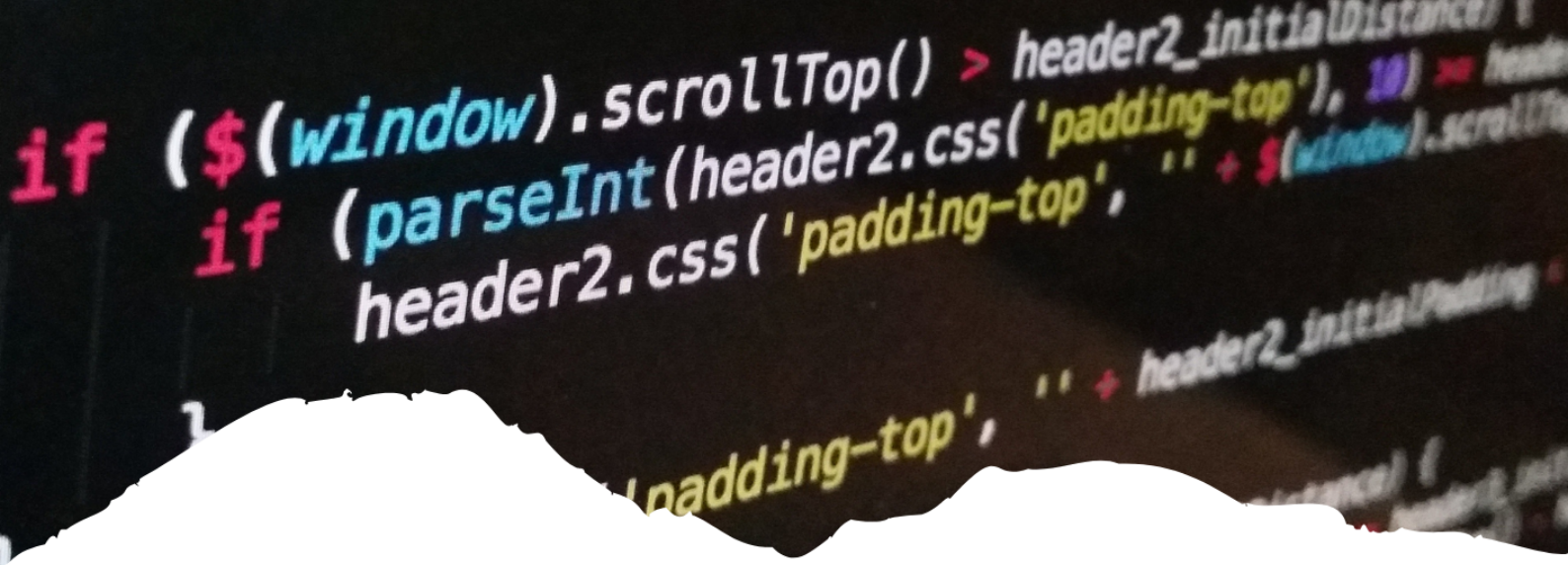
STERNBERG, R.J. **Intelligence, Information Processing and Analogical Reasoning: The componential analysis of Human Abilities.** New York: Wiley, 1977.

TACCHELLA A., et. al. Collaboration between a human group and artificial intelligence can improve prediction of multiple sclerosis course: a proof-of-principle study. F1000Researc, v.6, p. 2172, 2017.

TEIXEIRA, J.F. **Mentes e Máquinas: uma introdução às Ciências Cognitivas**. Porto Alegre: Artes Médicas, 1998.

TIBERIUS, Jose. **O cérebro e os Computadores Modernos: a teoria cognitiva global** – MOLWICK, v. 1, p. 16, 2016.

TURING, A. **Computing machinery and intelligence.** Mind, 59, 1950.



11

FERRAMENTAS E FRAMEWORKS PARA O DESENVOLVIMENTO WEB

TOOLS AND FRAMEWORS FOR WEB DEVELOPMENT

Robson Mateus Santana do Lago

Evinerison Silva Avelar

Iago Emanuel Fernandes Moreira

Rafael Costa Santana

Thamyres Mikaelly dos Santos Conceição

Resumo

O principal objetivo da Indústria 4.0 é proporcionar uma completa descentralização do controle da produção e o aprimoramento da manufatura através da disseminação do uso de novas tecnologias interligadas ao longo de todo o processo produtivo. Diante disso, essa pesquisa buscou entender a importância da criação de uma aplicação web utilizando ferramentas e padrões performáticos. Realizou-se uma revisão bibliográfica. Como resultados, pode-se verificar que a Web é uma rede de informações, pode ser considerada uma teia com várias ramificações, é baseada em hipertexto, que são comunicadas entre servidores que armazenam informações e dados dos usuários. As etapas que compõem o Desenvolvimento Web são: planejamento, desenvolvimento do protótipo do site, planejamento e desenvolvimento do designe do site, desenvolvimento do código, teste do site e lançamento. Observou-se também que um framework é considerado um conjunto de classes que se inter-relacionam, com o intuito de facilitar o desenvolvimento de um domínio de aplicação. Portanto, pode-se com essa pesquisa, compreender os aspectos e as etapas relacionadas ao processo de criação web.

Palavras-chave: Web; Desenvolvimento; Ferramentas.

Abstract

The main objective of Industry 4.0 is to provide a complete decentralization of production control and the improvement of manufacturing through the dissemination of the use of new interconnected technologies throughout the entire production process. Therefore, this research sought to understand the importance of creating a web application using tools and performance standards. A bibliographic review was carried out. As a result, it can be seen that the Web is an information network, it can be considered a web with several branches, it is based on hypertext, which are communicated between servers that store information and user data. The stages that make up the Web Development are: planning, development of the prototype of the site, planning and development of the design of the site, development of the code, test of the site and launch. It was also observed that a framework is considered a set of classes that are interrelated, with the aim of facilitating the development of an application domain. Therefore, with this research, it is possible to understand the aspects and steps related to the web creation process.

Keywords: Web; Development; Tools.

1. INTRODUÇÃO

Entende-se que a tecnologia vem evoluindo e as formas de desenvolvimentos são cada vez como um processo de organização, sendo assim se tornando essencial para qualquer organização ou desenvolvedor priorizar a melhor forma de desenvolvimento. Os sistemas webs na sua maioria são desenvolvidos com um preparo e pesquisa, é feita uma análise prévia dos requisitos e um levantamento para o desenvolvimento, o aumento crescente de pessoas que consomem a internet, necessitou de cuidado com as aplicações.

Desde o surgimento das primeiras interfaces gráficas 30 anos atrás, as aplicações têm o objetivo de ser performática, responsiva, atrativa e elegante, estes conceitos são abordados em experiência do usuário a chamada UX ou experiência do usuário que foi utilizado pela primeira vez em 1990 por Donald Norman, com tantas informações e modos de uma aplicação ser criada, é necessário o interesse de buscar um fluxo de informações para ajudar o planejamento, Assim, com o objetivo de facilitar e aprimorar o desenvolvimento dessas aplicações para uma melhor performance, surgiram os frameworks que melhoraram a produtividade na hora da construção de um novo projeto e desenvolvimento, os principais frameworks para a web são Vue, React, Angular.

Aprender técnicas e metodologias é de grande importância no cenário profissional de qualquer desenvolvedor de software, entender sobre padrões de projetos e tecnologias modernas, técnicas que irão ajudar a desenvolver um software seguro, estável e bonito é essencial, a fim de cada vez mais facilitar a vida do usuário de tal software, além disso a segurança e confiabilidade nesses softwares também são de suma importância.

Em determinado momento a modernização e o avanço das tecnologias no desenvolvimento de software se tornou uma busca por melhorar o desenvolvimento, diversas ferramentas disponíveis no mercado para auxiliar a criação, a fim de melhor a experiência do desenvolvimento de apps e a experiência do usuário, Toda aplicação demanda de uma pesquisa e um planejamento antes de ser criada, é necessário criar padrões e selecionar ferramentas eficientes para auxiliar o projeto ferramentas que não somente auxiliam o desenvolvimento, mas também a produtividade de toda a equipe envolvida no projeto Assim a pesquisa visa entender a necessidade de compreender as principais formas de desenvolver uma aplicação web, como também mostrar as melhores maneiras de relacionar os padrões e metodologias, Qual a importância da criação de uma aplicação web utilizando ferramentas e padrões performáticos?

Temos como objetivo geral: Entender a importância da criação de uma aplicação web utilizando ferramentas e padrões performáticos. Para alcançarmos esse objetivo geral, temos os objetivos específicos: conceituar a web e as ferramentas de desenvolvimento; entender os passos de desenvolvimento web; apresentar as características de conceitos de frameworks.

O tipo de pesquisa que será realizado neste trabalho é a metodológica de revisão bibliográfica, sendo uma pesquisa qualitativa e descritiva. A busca de informações sobre o tema que será abordado, serão utilizados livros, site, artigos científicos e dissertações que foram publicadas nos últimos 30 anos.

2. CONCEITOS DA WEB E SUAS FERRAMENTAS

A globalização e o desenvolvimento tecnológico trouxeram consigo diversas conse-

quências para o setor industrial. Uma delas é o surgimento de processos industriais com melhor desempenho e máquinas mais modernas e eficientes. Nesse contexto, a Indústria 4.0 surge como um novo conceito de indústria que engloba as principais inovações tecnológicas nos campos da Tecnologia da Informação e da Engenharia aplicadas à manufatura (ALVES, 2018).

A Indústria 4.0 tem como principal objetivo proporcionar uma completa descentralização do controle da produção e o aprimoramento da manufatura através da disseminação do uso de novas tecnologias interligadas ao longo de todo o processo produtivo. O termo Indústria 4.0 pode ser utilizado para identificar o uso das principais inovações tecnológicas dos campos de automação, controle e tecnologia da informação, aplicadas aos processos de manufatura. A utilização dos recursos tecnológicos inovadores possibilita, assim, a otimização, a eficiência e o melhor desempenho do processo produtivo (LIMA et al., 2021).

De acordo Alves (2018) o termo Indústria 4.0 tornou-se popular em 2011, quando uma companhia de representantes do governo, organizações e academia promoveu a ideia de uma abordagem com o intuito de aperfeiçoar a competitividade da indústria alemã. Assim, o governo alemão deu suporte à iniciativa e declarou que a Indústria 4.0 seria parte do projeto High-Tech Strategy 2020 for Germany, com o objetivo de levar a Alemanha à liderança na inovação tecnológica.

Conforme destaca Nunes (2021), recursos inovadores como os Sistemas Cyber-Físicos (tradução de Cyber Physical Systems – CPS), Internet das Coisas e Internet dos Serviços possibilitam que os processos industriais e produtivos possuam maior eficiência, autonomia e melhores custos. Assim, a Indústria 4.0 vem representar um novo período no contexto das grandes revoluções industriais, com impactos diretos em diversos setores do mercado e que proporcionam o crescimento de diferentes setores da economia (SILVA; TIOSSO, 2020).

Loundon (2021) ressalta que as empresas deverão introduzir redes globais, que incorporem suas máquinas, sistemas de armazenagem e instalações de produção na forma de Sistemas Físico-Cibernéticos. Os CPS propõem a integração de mundos físicos e virtuais para suportar todas essas exigências e capacidades, de forma a incorporar os elementos computacionais em entidades físicas e conectar essas entidades em uma infraestrutura baseada em nuvem, com a finalidade de proporcionar uma gestão mais eficaz do ambiente físico e seus processos.

Em 1957, dois países Estados Unidos e a União Soviética entraram em combate na chamada guerra fria um embate que diferente da segunda guerra mundial (1945), foi um combate ideológico, econômico, tecnológico, desse conflito surgiu a necessidade de os estados unidos proteger suas comunicações e dessa maneira veio a ser criado o que hoje é conhecida como internet. Com o passar do tempo criou-se a necessidade de criar uma organização que desenvolvesse padrões e regras na web, foi então que em 1994 o engenheiro britânico Timothy John Berners-Lee fundou a World Wide Web Consortium (W3C) (BENTO, 2021).

Uma organização que tem como objetivo estabelecer padrões e diretrizes para a criação de conteúdo para a Web e garantir o crescimento dela, o objetivo dela é atingir o potencial máximo da Web. Além disso, com o avanço da internet, de acordo com Sebesta (2018, p.92) “O uso da Web explodiu em meados dos anos 1990, após a aparição dos primeiros na-vegadores[*sic*] gráficos. A necessidade de computação associada a documentos HTML, os quais por si só eram completamente estáticos, rapidamente se tornou crítica”.

Como o avanço dos anos as aplicações ficam cada vez maiores, “Se você considerar

quão diferente é a Internet de hoje daquela que existia dez anos atrás, ficará claro o grau de complexidade adquirido pelas aplicações web e a rapidez com que as mudanças ocorreram" (LOUDON, 2021, p.17)

A Web é uma rede de informações, pode ser considerada uma teia com várias ramificações, é baseada em hipertexto, que são comunicadas entre servidores que armazenam informações e dados dos usuários.

A internet vem evoluindo a tempos, dessa forma se torna indispensável para a sociedade, todavia a web desde sua criação até os dias atuais vem passando por diversas mudanças e atualizações.

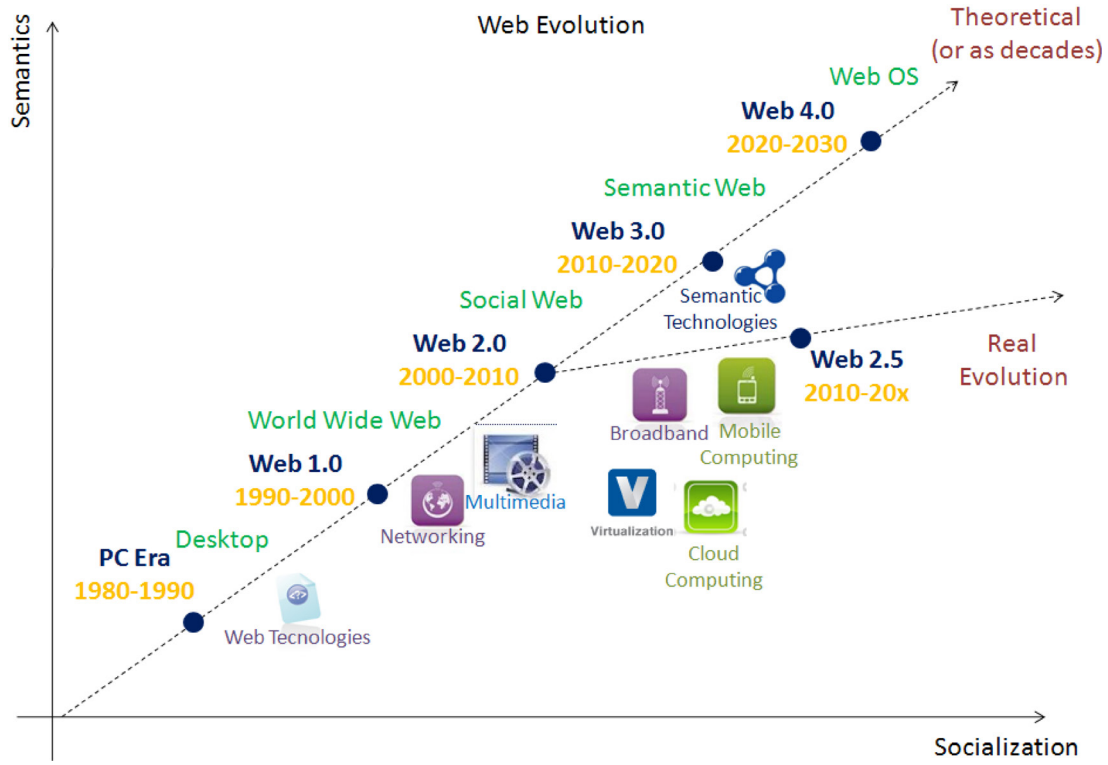


Figura 1 - Evolução da web

Fonte: Madurai (2018).

O site medium mostra a evolução da web desde 1980 até 2040, com surgimento das tecnologias webs até a banda larga. Web 1.0 foi marcado por todas as suas páginas serem estáticas, desse modo o conteúdo da página não poderia ser modificado e a navegação ficava bastante limitada, assim como o surgimento das multimidias.

- Web 2.0 nessa fase a web deixou de ser estática, agora o usuário poderia interagir com a página, também foi nesse período que surgiu as redes sociais, esse modelo é utilizado até os dias atuais, também surgiu a computação em nuvem.
- Web 3.0 chamada de Web semântica, é uma internet que busca a aproximação das máquinas com os seres humanos para que ambos possam entender as informações, basicamente mais próxima da inteligência artificial, o Web 4.0 ainda está nas teorias e implementações.

Segundo Silva (2008) O conceito de hipertexto pode ser facilmente resumido em todo o conteúdo inserido em um documento para web que possibilita a interligação a outros documentos web, de forma simples é o esqueleto de uma página. No presente momento o HTML evoluiu e está na sua versão 5 desde sua criação em 1991.

Cascading Style Sheets (CSS) que traduzindo para o português significa folhas de estilo em cascata. O CSS é utilizado com uma forma de personalizar e aplicar vida ao HTML, dando estilo e personalidade, segundo MILETTO (2014) o CSS possibilita criar estilos personalizados para títulos, listas, imagens etc. Além de definir as cores, fontes, alinhamentos entre outros elementos que podem ser ligados a aparência da página

Flanagan (2004) cita que Javascript é a linguagem de programação da Web, e que a ampla maioria dos sites modernos usam Javascript além de todos os navegadores modernos.

O Javascript foi criado por Brendan Eich, que logo na sua criação foi integrado no navegador da Netscape o navigator 2 em 1995. Com seu sucesso foi introduzido também no Internet-Explorer 2.0.

Javascript que também é chamado de ECMAScript, ECMA (European Computer Manufactures Association) que basicamente representa as versões da linguagem. A versão ECMASript 2021 é a versão mais atual.

O desenvolvimento de web app ou somente site e páginas que estão disponíveis na internet são desenvolvidos por developer que traduzindo diretamente para o português significa desenvolvedor(a) uma das várias áreas disponíveis no mundo da TI.

Ao longo dos anos diversas ferramentas surgiram para auxiliar o desenvolvimento de aplicações entre elas frameworks ou bibliotecas como react, vue, bootstrap, angular entre outras que aumentam a produtividade e a performance de uma aplicação acelerando seu desenvolvimento, de forma geral um framework permite que o desenvolvedor facilite o desenvolvimento de tarefas simples e funcionalidades genéricas, assim mantendo o foco em tarefas que requerem um grau de complexidade maior.

Figura 2 - Gráfico de frameworks

Fonte: Stateofjs (2019)

O site stateofjs mostra uma pesquisa realizada com desenvolvedores webs que usaram e voltariam a usar alguns frameworks para o desenvolvimento de sites e o react é a ferramenta mais utilizada, como mostrado na figura 2.

Além de escolher uma boa ferramenta é necessária a adoção de um padrão ou me-

todologia de desenvolvimento, segundo Loudon (2021) cada ano que passa as aplicações têm um grau de complexidade cada vez maior, seja por elas estarem rodando 24 horas por dia ou a grande quantidade de usuários na base de dados.

Com isso, é possível perceber a clara aceitação de novas ferramentas para o desenvolvimento, nesse contexto também é necessário um bom modelo de desenvolvimento, ou seja, um padrão para que as aplicações não saiam de controle em todos o seu desenvolvimento.

O padrão Model View Controller (MVC) é um padrão de desenvolvimento. Segundo o (SESHADRI, GREEN, 2014) o MVC evoluiu como uma prática de separar as responsabilidades no desenvolvimento de aplicações mais complicadas ou de grande porte.

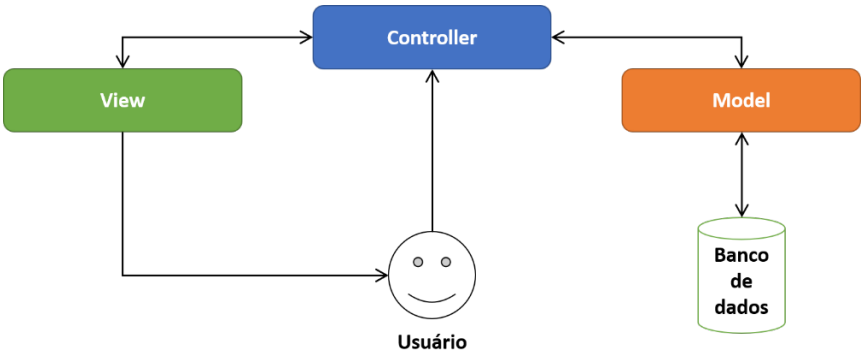


Figura 3 – MVC

Fonte: Guedes (2020).

Como aponta o site trainaweb o MVC segue um fluxo para facilitar o desenvolvimento, separando as tarefas, como mostrado na figura 3.

Basicamente um padrão de desenvolvimento de software que otimiza a velocidade entre o usuário e a requisição, garante segurança, organização eficiência e tempo no desenvolvimento, além de aumentar a produtividade de toda a equipe, por separar as etapas do projeto. Além de deixar o código mais facilitado para futuras manutenções, já que ele traz uma separação e compressão do código.

3. PASSOS DO DESENVOLVIMENTO WEB

Muito se questiona a respeito de como é produzido o que está disponível na internet. Sites, aplicativos ou até mesmo os jogos disponíveis para a população, são desenvolvidos de maneira estratégica e por uma equipe de desenvolvimento de web (ANDRADE et al., 2019).

Segundo Loudon (2021), o número de usuários de internet no Brasil já ultrapassou os 150 milhões, levando em consideração os últimos dados da Agência Brasil. Além disso, ao menos cinco milhões de buscas são feitas diariamente no Google. Esses números evidenciam a importância da presença online das diferentes empresas e organizações, a fim de impulsionar sua marca ou a sua presença. E, para que isso aconteça, a melhor maneira é por meio de um site ou aplicativo.

De acordo com Bento (2021) o desenvolvimento web é o fator responsável por codificar páginas, sites, portais ou aplicativos para a web. Sendo assim, ele é o responsável pela estrutura de um site, tanto no que se refere à área em que o usuário interage, como a parte que ele não vê e não interage, mas que é muito importante e impacta na experiência do usuário.

Sendo assim, de acordo com London (2021), dentro do Desenvolvimento Web, pode-se destacar três funções distintas, sendo elas:

1. Front-end: responsável pela parte do site que o usuário interage;
2. Back-end: responsável pelo o que tem por trás do site;
3. Full-stack: o Full-stack é Front-end e Back-end juntos.

Um website pode ser conceituado como o conjunto de todos os documentos de texto, links, cores, imagens e demais fatores que permitirão que o usuário consiga navegar pelo site. De modo geral, ele vem relacionado à sua URL. Tal domínio é o fator que explica ao Web Browser o local onde estão disponíveis os arquivos, conforme o planejamento do desenvolvedor (VENTEU; PINTO, 2018).

De acordo com Santiago et al. (2021, p.43):

> A um conjunto de páginas web ou hiper textos dá-se o nome de site, e são acessados na Internet pelo protocolo HTTP. O conjunto de todos os sites públicos constituem a World Wide Web. As páginas de um site são organizadas a partir do endereço da página principal. As páginas são organizadas dentro do site numa hierarquia observável no URL, embora as hiper-ligações entre elas controlam o modo como o utilizador percepciona a estrutura global, modo esse que pode ter pouco a ver com a estrutura hierárquica dos arquivos do site.

Os arquivos são gerenciados por meio de softwares de acesso FTP, conforme mostra a imagem seguinte:

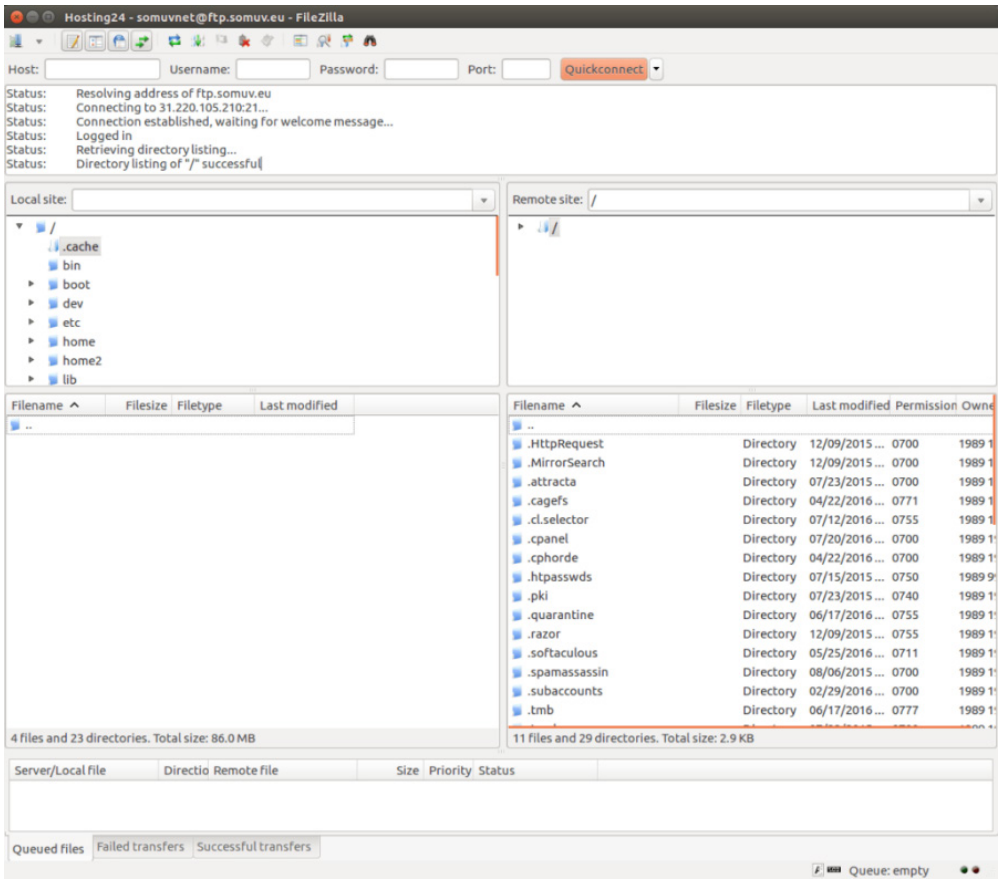


Figura 4 – Software de acesso FTP

Fonte: Pereira (2020).

Pode-se, portanto, afirmar que um Web Browser corresponde a todo aplicativo com capacidade de baixar e exibir esses documentos, assim como as suas informações, de modo sistematizado e organizado ao usuário. Como exemplo, pode-se citar o Mozilla Firefox e o Google Chrome como os mais utilizados (PEREIRA, 2020).

Diante disso, pode-se afirmar que o Desenvolvimento Web diz respeito a ao conjunto de processos envolvidos no desenvolvimento de um projeto ou de um site da Web. Ele é formado diversas fases, como o planejamento, desenvolvimento, teste e lançamento na web. Todo o processo de Desenvolvimento Web exige a participação de técnicos e especialistas responsáveis pela implantação das diversas tarefas e atividades necessárias para a criação de um site (SILVA; NASCIMENTO; TENÓRIO, 2021).

A seguir, serão detalhadas todas as etapas que compõem o Desenvolvimento Web:

a) Planejamento

Durante o Desenvolvimento Web, a primeira etapa é o planejamento. Ele corresponde a uma das etapas mais importantes do processo e exige muita atenção do seu desenvolvedor, tendo em vista que ele guiará todo o processo de desenvolvimento, desde as ações mais básicas até a estruturação de todo o site (BRITO et al., 2022).

Inicialmente, o os objetivos do site devem ser esclarecidos, pois é com base neles que todo o planejamento será desenvolvimento. A partir disso, o perfil do público consumidor, bem como as suas preferências e comportamentos serão conhecidos. Nesta etapa, também será analisado todo o fluxo de informações, storyboards e wireframes, a fim de que sejam estabelecidos os protótipos na etapa seguinte. Além disso, na etapa de planejamento é definida a melhor ferramenta para o gerenciamento do conteúdo que o site abrigará (ROCHA et al., 2018).

Tais ferramentas são denominadas de Content Management System (CMS) e elas possibilitam a edição de conteúdo de modo simples. Como exemplos conhecidos de CMS, pode-se citar o WordPress e Joomla, comumente utilizados na edição de blogs e sites. Caso seja interesse do cliente, também pode-se definir nesta etapa de planejamento o Customer Relationship Management (CRM), que é uma ferramenta que coleta os dados dos visitantes do site e que define as ações que cada um toma, o que influencia diretamente no marketing comercial, como por exemplo: RD Station, Salesforce, Highrise e Insightly. Logo em seguida da definição dessas questões, pode-se estimar os requisitos, o tempo de duração do Desenvolvimento Web e os custos do projeto (SILVA et al., 2021).

b) Desenvolvimento do protótipo do site

A partir do que foi estabelecido no planejamento, será definido um protótipo. Ele corresponderá ao conjunto de todos os storyboards e wireframes do site. Portanto, pode-se dizer que o protótipo é uma forma de documentação mais categórica que demonstrará a arquitetura do site, orientando todo o Desenvolvimento Web (ALVES, 2018).

Para a criação do protótipo, incialmente, devem ser identificadas todas as páginas e a sua organização, de modo que seja possível identificar de que modo elas se comunicarão, assim como selecionar quais serão necessárias para o menu de navegação. Além disso, é importante ressaltar que toda interação entre as páginas deve ocorrer de modo intuitivo ao usuário, e a quantidade de páginas deve ser estabelecida de modo que o usuário alcance seu objetivo de forma rápida (SILVA; TIOSSO, 2020).

O conteúdo das páginas principais é outro ponto importante e que deve ser considerado. As páginas de conteúdo do site deverão trazer informações relevantes para o usuário. Desse modo, deverão ser bem escolhidos os Call to action (CTA), dentro de cada página,

a fim de que as chamadas ocorram de forma natural. Ressalta-se que todo o conteúdo deve ser desenvolvido de modo intuitivo e que auxilie os usuários na navegação pelo site (NUNES, 2021).

É relevante destacar que a homepage do site também merece atenção, pois ela corresponde à porta de entrada aos usuários. Estima-se que os primeiros segundos que o usuário passa no site determinarão se ele continuará ou não ali. A métrica ideal para a velocidade de carregamento é de 2,5 segundos, o que quer dizer que o site deve ser rápido, para conquistar a atenção dos usuários. Além disso, é importante a integração com outras ferramentas, como as ferramentas de CMS, de CMR e o Google Analytics (PEREIRA, 2022).

c) Planejamento e desenvolvimento do design do site

O desenvolvimento do layout do site somente deve ocorrer após a criação do protótipo, tendo em vista que ele orientará o trabalho do designer. Enquanto se cria o protótipo, pode-se fazer o mood board do projeto, que corresponde à um painel de referências virtuais que permitem a visualização da estética do site e a sua interação com o objetivo da marca. Após a criação do layout, a próxima etapa corresponde à escrita do código (PINTO, 2022).

d) Desenvolvimento do código

O desenvolvimento do código do site é considerado, por muito, uma das etapas mais trabalhosas e complexas do Desenvolvimento Web. Nessa fase, ocorre o desenvolvimento e a implementação do planejado para o funcionamento do site. Os programadores são os elementos responsáveis por executar e dar vida ao layout planejado pelos UI/UX designers, assim como gerenciar banco de dados, criar funcionalidades, desenvolver e integrar APis, garantir a otimização do servidor, dentre outras funções (SILVA, 2018).

Geralmente, o código estrutural é escrito no formato HTML/CSS. Já outras funções, incluindo o suporte, é escrito em PHP ou Javascript, quando se trata do front-end. Já o back-end faz uso de outas tecnologias, como por exemplo, o MongoDB, Node JS e Typescript (LIMA et al., 2021).

e) Teste do site e lançamento

Assim que o Desenvolvimento Web é realizado, a etapa seguinte diz respeito à revisão do código. É de grande importância nesta etapa que seja debugado o que foi escrito, a fim de encontrar prováveis erros e falhas. Os erros revelarão se há necessidade de revisão de alguma linha do código de programação. Espera-se que, nessa etapa, as dificuldades identificadas apontem a existência de algum local do layout que não esteja completamente intuitivo e necessite ser refeito. O ideal é que, nessa fase, o protótipo esteja suficientemente desenvolvido e que seja possível identificar e analisar possíveis falhas existentes. Esse levantamento de feedback é de suma importância para a garantia do lançamento de um site como o público consumidor espera (ALVES, 2018).

E por fim, a última etapa do Desenvolvimento Web é o lançamento do site. Após as revisões, pode-se divulgá-lo para o acesso pelas pessoas. O ideal é que sejam criadas campanhas de lançamento, para que o público comece a encontrá-lo (LIMA et al., 2021).

4. FRAMEWORKS

Diversas definições para framework são apresentadas na literatura, porém, de acordo com Loudon (2021, p.21), “um framework é um conjunto de classes que cooperam entre si provendo assim um projeto reutilizável para um domínio específico de classes de sistema”.

Um framework pode abranger programas de suporte, linguagens script, bibliotecas de código e demais softwares que podem auxiliar no desenvolvimento e na junção de diversos componentes de um projeto de software.

De acordo com Bento (2021), os frameworks são projetados com o objetivo de tornar mais fácil o desenvolvimento de um software, de modo a habilitar programadores e projetistas a destinarem mais o seu tempo detalhando as exigências de negócio do software, do que com detalhes considerados de baixo nível do sistema.

Segundo as palavras de Santiago et al. (2021, p.43), tem-se como definição para framework:

> Framework é um esqueleto de implementação de uma aplicação ou um subsistema de aplicação, em um domínio de problema particular. É composto de classes abstratas e concretas e provê um modelo de interação ou colaboração entre as instâncias de classes definidas pelo framework. Ele é utilizado através de configuração ou conexão de classes concretas e derivação de novas classes concretas a partir das classes abstratas do framework. Ou seja, é um conjunto de classes cooperantes que constroem um projeto reutilizável para uma classe específica de software.

Um framework é considerado um conjunto de classes que se inter-relacionam, com o intuito de facilitar o desenvolvimento de um domínio de aplicação. Ele é formado por classes concretas e abstratas, que possuem implantações incompletas que devem ser estendidas, a fim de formar as classes completas da aplicação final (PEREIRA, 2020).

De acordo com Loudon (2021), o que motiva o desenvolvimento de frameworks é a possibilidade de reutilizar o código e o projeto, com o objetivo de elevar a produtividade no desenvolvimento de softwares, ditando a arquitetura da aplicação. Sendo assim, ele passa a definir a estrutura geral, a sua classificação e, consequentemente, as responsabilidades das classes dos objetos. Isso ocorre de modo a possibilitar que o projetista se concentre nos aspectos inerentes à sua aplicação.

Sendo assim, alguns critérios devem ser levados em consideração para que projetos de softwares sejam realmente considerados um framework, sendo eles, basicamente:

- É necessário que seja reutilizável;
- É preciso que seja um facilitador do desenvolvimento de sistemas;
- Apresentar uma boa documentação;
- É necessário que seja completo para o que se propõe a fazer;
- Deve ser eficiente (SILVA; NASCIMENTO; TENÓRIO, 2021).

Ao utilizar frameworks, é importante ressaltar que uma das principais vantagens é a redução de custos, levando em consideração que já existe uma estrutura pré-definida, bem como o desenvolvimento pode se concentrar na implementação das normas do negócio em que o sistema atuará. Além disso, um framework também possibilita maior capacidade de reutilização de códigos, bem como a fatoração de problemas comuns a diversas aplicações, possibilitando assim a obtenção de sistemas em códigos mais seguros, menos frágeis e com menos falhas.

Um framework é responsável por capturar as decisões estratégicas do projeto que são pertencentes ao seu domínio de aplicação. Dessa forma, ele dá ênfase ao reuso dos códigos, ainda que, de modo geral, inclua algumas subclasses concretas que o desenvolvedor

pode utilizar de modo imediato. Para que haja o aumento da produtividade, é importante levar em consideração a granularidade do artefato do software, pois um framework apresenta maior grau de granularidade, se comparado à reutilização de rotinas (SILVA; NASCIMENTO; TENÓRIO, 2021).

Quando ocorre a reutilização de uma classe, todos os seus métodos e atributos também são reutilizados. Ou seja, reutilizar uma classe pode ser mais eficaz do que uma rotina de maneira isolada. A reutilização de classes de abordagem de framework se encontra em um nível de granularidade maior que a reutilização de classes de uma biblioteca, pois nessa situação, são usados artefatos de software isolados, devendo o desenvolvedor garantir a sua interligação. Quando se trata do framework, procede-se com a reutilização de um conjunto de classes, inter-relacionadas pelo projeto do framework. Considerando a possibilidade de reutilização de códigos e projetos, os frameworks possibilitam o aumento da produtividade no desenvolvimento e criação de um novo software (BRITO et al., 2022).

A figura abaixo demonstra a aplicação desenvolvida reutilizando um framework:

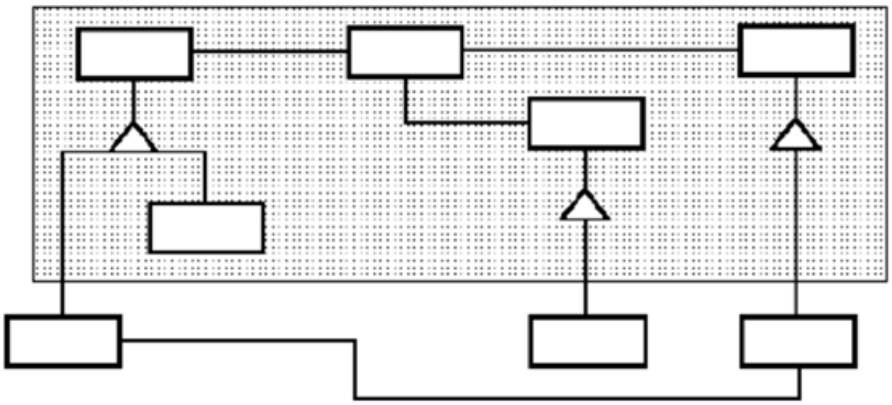


Figura 5 - Aplicação desenvolvida reutilizando um framework

Fonte: Pereira (2020).

A reutilização neste nível acaba levando a uma alteração de controle entre o software sobre a qual ela se baseia e a aplicação. Dessa forma, quando utiliza-se da biblioteca de funções, acaba sendo escrita a estrutura primordial da aplicação e se chama também o código que será reutilizado. Quando um framework é utilizado, o corpo principal é reutilizado e escrito o código que ele chama. Portanto, o desenvolvedor deverá escrever as operações nomeadas e as convenções de chamadas, já com suas especificações. Dessa forma, como resultado de tudo isso, o desenvolvedor poderá não apenas construir aplicações de forma mais rápida, mas também aplicações com estruturas parecidas. No entanto, em contramão, o desenvolvedor acaba perdendo a sua liberdade de criação, tendo em vista que já tomou diversas decisões em relação ao projeto (SILVA et al., 2021).

Segundo Alves (2018), os frameworks são classificados, conforme a sua forma de utilização, em três tipos, sendo eles: caixa-branca, caixa-cinza e caixa-preta. As características de cada um são apresentadas a seguir:

a) Frameworks Caixa Branca (White-Box)

Esse tipo de framework se baseia nos mecanismos de herança e ligação dinâmica existentes em orientação a objetos. Os recursos presentes nesse tipo de framework podem ser reutilizados e usados por extensão a partir da herança da sobrecarga e das classes do framework. A expressão caixa-branca faz referência à visibilidade, pois, os detalhes internos das classes precedentes podem ser visualizados pelas subclasses.

Segundo Nunes (2021, p.20)

> Os frameworks de Caixa Branca são baseados na especialização por herança e sobrescrita de métodos, com a disponibilidade de classes abstratas, que não podem ser instanciadas diretamente, podem ser herdadas e utilizar os recursos destas.

Esse método de implementação é descrito pelo Template Method. Neste tipo de padrão, redefine-se um método em uma subclasse, que modificará o comportamento do método que se herdou. Portanto, frameworks caixa-branca apresentam mais facilidade de implementação, no entanto, mais dificuldade quanto ao seu uso, tendo em vista que a geração de subclasses a partir das classes do framework requer maior conhecimento e domínio sobre a sua estrutura e dos métodos que serão implementados, a fim de que as subclasses desenvolvidas funcionem de modo correto (SILVA; TIOSSO, 2020).

b) Frameworks Caixa Preta (Black-Box)

Baseiam-se nos elementos que compõem o software. A extensão da arquitetura é realizada com base nas interfaces estabelecidas para os componentes. Os recursos que existem são estendidos e utilizados através do conceito de um fator componente adequado para uma interface específica, bem como de sua integração.

São os frameworks focados na composição devendo utilizar as funcionalidades já presentes no framework, ou seja, neste tipo de framework as funcionalidades internas não podem ser vistas nem modificadas e devem utilizar as interfaces fornecidas pelo framework. Neste tipo as instanciações e composições feitas são o que determinam as particularidades da aplicação (PEREIRA, 2022).

Assim como a expressão caixa-branca, o termo caixa-preta também está associado à visibilidade, pois os detalhes internos dos componentes não podem ser vistos, logo, não são visíveis. O padrão de projeto Strategy é o que descreve essa forma de implementação. Esse padrão conceitua uma família de algoritmos, as encapsula e com isso, as torna intercambiáveis. Esse tipo de framework geralmente é fácil de ser utilizado, pois não existe uma herança envolvida, somente objetos, que por sua vez, são mais fáceis de serem entendidos e mais concretos. Entretanto, se comparados à caixa branca, eles são menos flexíveis, pois o aplicativo é formado com base em um conjunto de componentes interligados, ao invés da derivação de classes (PINTO, 2022).

c) Frameworks Caixa-Cinza

A caixa-cinza, por sua vez, é a combinação da caixa-preta e a caixa-branca, com o objetivo de aproveitar os pontos fortes de cada uma. Sendo assim, utiliza a flexibilidade da caixa-branda e a facilidade de uso e compreensão da caixa-preta. De modo geral, na prática, a maior parte dos frameworks desenvolvidos classificam-se nessa categoria (SILVA, 2018).

Portanto, para que um framework garanta um bom suporte ao domínio de aplicações a que se coloca a fazer, é necessário que se busque algumas características e aspectos que contribuirão para o aumento da sua qualidade. Dentre essas características, pode-se citar a extensibilidade, alterabilidade e generalidade. Para tanto, é necessário que o projeto seja bem desenvolvido, visando sempre identificar qual parte deve ser mantida com sua flexibilidade (LIMA et al., 2021).

5. CONCLUSÃO

Essa pesquisa buscou entender a importância da criação de uma aplicação web utilizando ferramentas e padrões performáticos. Diante da análise dos materiais coletados, pode-se concluir que a Web é considerada uma rede de informações, com várias ramificações, baseando-se em hipertextos, que se comunicam entre servidores que armazenam informações e dados dos usuários. Além disso, observou-se que a internet vem evoluindo a tempos, dessa forma se torna indispensável para a sociedade. No entanto, a web desde sua criação até os dias atuais vem passando por diversas mudanças e atualizações.

Ainda, pode-se observar também com a pesquisa que o Desenvolvimento Web se refere ao conjunto de processos envolvidos no desenvolvimento de um projeto ou de um site da Web. Ele é formado diversas fases, como o planejamento, desenvolvimento, teste e lançamento na web. É importante ressaltar que todo o processo de Desenvolvimento Web exige a participação de técnicos e especialistas responsáveis pela implantação das diversas tarefas e atividades necessárias para a criação de um site.

Por fim, essa pesquisa demonstrou que um framework tem o papel de captar as decisões estratégicas do projeto que são pertencentes ao seu domínio de aplicação. Desse modo, algumas subclasses concretas que o desenvolvedor pode utilizar de modo imediato. Portanto, a fim de que haja o aumento da produtividade, ressalta-se a importância de considerar a granularidade do artefato do software, tendo em vista que o framework apresenta maior grau de granularidade, quando comparado à reutilização de rotinas.

Referências

ALVES, William Pereira. **Java para Web–Desenvolvimento de Aplicações**. Saraiva Educação SA, 2018.

ANDRADE, Icaro et al. Relato de experiência das limitações na proposta de ensino de desenvolvimento web para discentes do nível fundamental da Rede Pública Municipal. In: **Anais da XIX Escola Regional de Computação Bahia, Alagoas e Sergipe**. SBC, 2019. p. 625-633.

BENTO, Evaldo Junior. **Desenvolvimento web com PHP e MySQL**. Editora Casa do Código, 2021.

BRITO, Ana Sara Rodrigues Chrisostomo de et al. Desenvolvimento da plataforma digital Hair Chance. 2022.

FLANAGAN, David. **JavaScript: o guia definitivo**. Bookman Editora, 2004.

GUEDES, Marylene. O que é MVC? 2020. Disponível em: https://www.treinaweb.com.br/blog/o-que-e-mvc. Acesso em: 15 set. 2022.

LIMA, Mahara Iasmine Sampaio Cardoso et al. Plataforma Web para inspeção da segurança em canteiros de obra apoiado por VANT e dispositivos móveis. **SIMPÓSIO BRASILEIRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA CONSTRUÇÃO**, v. 3, p. 1-11, 2021.

LOUDON, Kyle. Desenvolvimento de grandes aplicações Web. **Revista Telfract**, v. 1, n. 1, 2021.

MADURAI, Vivek. **Evolução da Web de 1.0 a 3.0**. 2018. Disponível em: https://medium.com/@vivekmadurai/web-evolution-from-1-0-to-3-0-e84f2c06739. Acesso em: 22 set. 2022.

MILETTO, Evandro Manara; DE CASTRO BERTAGNOLLI, Silvia. **Desenvolvimento de Software II: Introdução ao Desenvolvimento Web com HTML, CSS, JavaScript e PHP-Eixo: Informação e Comunicação-Série Tekne**. Bookman Editora, 2014.

NUNES, Vinicius George Carlos. Avaliação de abordagens e definição de diretrizes para o desenvolvimento de aplicativos mobile: um relato de experiência utilizando aabordagem não nativa de desenvolvimento. 2021.

PEREIRA, Pryscilla. Simplificando o desenvolvimento web acessível na prática. **Revista Diálogos Acadêmicos**, v. 9, 2020.

PEREIRA, Ricardo. Desenvolvimento do Multifactor: Aplicação mobile que implemente serviços de verificação de duas etapas para autenticação multifator. 2022.

PINTO, Ricardo Nuno Rafael Monteiro da Silva. **Uso do estado da arte no desenvolvimento de aplicações web para a criação e teste de uma aplicação responsiva**. 2022. Dissertação de Mestrado.

ROCHA, Paulo Santana et al. Modelando trajetórias de aprendizagem utilizando princípios de design baseado em blocos: um estudo de caso aplicado à aprendizagem em desenvolvimento web. **RENOTE**, v. 16, n. 2, p. 351-361, 2018.

SANTIAGO, Cynthia Pinheiro et al. Desenvolvimento de sistemas Web orientado a reuso com Python, Django e Bootstrap. **Sociedade Brasileira de Computação**, 2020.

SEBESTA, Robert W. **Conceitos de Linguagens de Programação-11**. Bookman Editora, 2018.

SESHADRI, Shyam; GREEN, Brad. **Desenvolvendo com AngularJS: aumento de produtividade com aplicações web estruturadas**. Novatec Editora, 2014

SILVA, Danilo Moura; NASCIMENTO, Matheus Maciel; TENORIO, Daniel Barboza. DESENVOLVIMENTO DE UM SISTEMA WEB COMO FACILITADOR DE MARCAÇÃO DE CONSULTAS NO SISTEMA PÚBLICO DE SAÚDE DE GUARULHOS PARA REDUÇÃO DE FILAS PRESENCIAIS. **Revista Computação Aplicada-UNG-Ser**, v. 9, n. 1, p. 10-14, 2021.

SILVA, Igor Henrique Ferraz Alves et al. APLICAÇÃO DE GAMIFICAÇÃO EM UMA PLATAFORMA WEB COM PRINCÍPIOS DO DESENVOLVIMENTO SUSTENTÁVEL. **Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia**, v. 5, n. 1, p. 20-20, 2021.

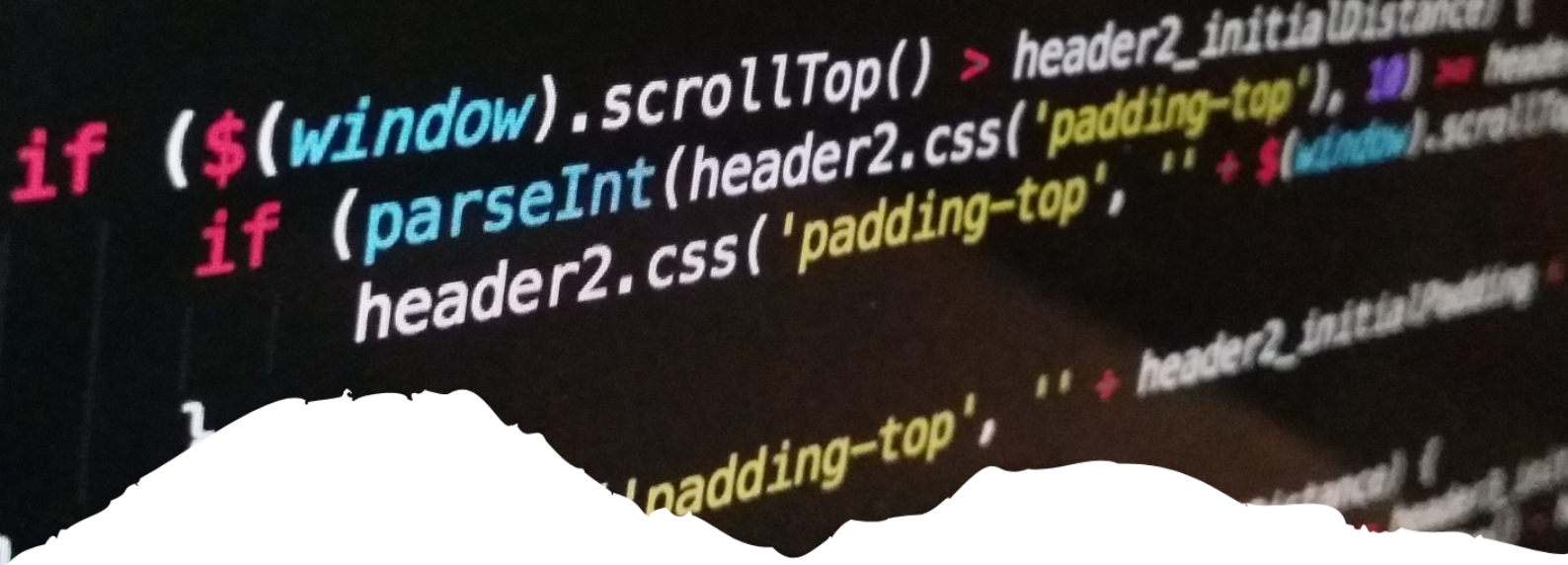
SILVA, Jonathas Kranmer; TIOSSO, Fernando. Revisao bibliográfica sobre conceito de progressive web applications (pwa). **Revista Interface Tecnológica**, v. 17, n. 1, p. 53-64, 2020.

SILVA, Maurício Samy. **Criando sites com HTML: sites de alta qualidade com HTML e CSS**. Novatec Editora, 2008.

SILVA, Maurício Samy. **Web Design Responsivo: aprenda a criar sites que se adaptam automaticamente a qualquer dispositivo, desde desktops até telefones celulares**. Novatec Editora, 2018.

STATEOFJS. Frameworks Front End. 2019. Disponível em: https://2019.stateofjs.com/pt/front-end-frameworks/. Acesso em: 25 abr. 2022.

VENTEU, Kelly Cristina; PINTO, Giuliano Scombatti. Desenvolvimento móvel híbrido. **Revista Interface Tecnológica**, v. 15, n. 1, p. 86-96, 2018.



12

INTERNET DAS COISAS: APLICAÇÃO E SEGURANÇA

INTERNET OF THINGS: APPLICATION AND SECURITY

Breno Leonan Cardoso Barros

Resumo

Este artigo foi escrito com o objetivo de alertar sobre as vulnerabilidades inerentes de um sistema formulado em Internet das Coisas, buscando Conceituar a Internet das Coisas; compreender a importância da segurança da Informação e identificar as vulnerabilidades de um sistema modelado em Internet das Coisas. Trata-se de uma pesquisa baseada em aspectos descritivos e qualitativos pertencente às vertentes de metodologias de revisão bibliográfica, iniciando-se ao buscar compreensão sobre os primórdios da internet das coisas (IoT), desde sua teoria, relacionando com a máquina de Turing até sua aplicação na indústria 4.0.A Indústria 4.0 está navegando rumo à automação completa. Com seus dispositivos se comunicando através da rede com outros dispositivos. Cita-se como exemplo, a linha de produção de carros totalmente automatizados por inteligência artificial, tal como carros integrados com a própria inteligência artificial, a exemplo, carros que não precisam mais de motoristas.

Palavras-chave: Internet das Coisas, Indústria 4.0, Segurança da Informação

Abstract

This article was written with the objective of warning about the inherent vulnerabilities of a system formulated in the Internet of Things, seeking to Conceptualize the Internet of Things; understand the importance of Information security and identify the vulnerabilities of a system modeled in the Internet of Things. This is a research based on descriptive and qualitative aspects belonging to the strands of literature review methodologies, starting by seeking understanding about the beginnings of the Internet of Things (IoT), from its theory, relating it to the Turing machine to its application in Industry 4.0.Industry 4.0 is navigating towards complete automation. With its devices communicating over the network with other devices. One example is the production line of cars fully automated by artificial intelligence, such as cars integrated with artificial intelligence itself, for example cars that no longer need drivers.

Keywords: Internet of Things, Industry 4.0, Information Security

1. INTRODUÇÃO

Discute-se, na atualidade, a implementação de sistemas baseados em Internet das Coisas nos processos produtivos do mercado de trabalho. Tal discussão iniciou-se após a terceira revolução industrial, visando o advento da "quarta revolução industrial". O foco do debate é a chamada indústria 4.0, cuja características são a maior autonomia durante a tomada de decisões, tal como um maior entendimento da relação Homem-Máquina.

No mundo globalizado, precisa-se de internet para quase tudo que faz-se necessário no dia-a-dia, desde uma mensagem através de aplicativo até assistir canais de televisão favoritos. Portanto, a desvinculação da internet em vários graus com mundo em que se vive, torna-se impossível. Transparecendo a total dependência do ser humano para com a Internet das Coisas. Porém, é primordial que pessoas sejam totalmente capacitadas para adentrar neste mundo tecnológico.

Internet das Coisas aplica-se em várias áreas da tecnologia atual, tangenciando computadores, *smartphones*, *tablets, smartwatches*, câmeras, lâmpadas e até casas. Embora pouca parcela da população brasileira se beneficie da internet das coisas, este termo vem se expandindo nos últimos anos e se ampliou ainda mais durante a Pandemia, onde difundiu-se o conceito de *Home Office* ou teletrabalho como uma forma de trabalho *mainstream*. Com todo esse acesso por parte de diferentes usuários e empresas, surge uma indagação: Quais as vulnerabilidades inerentes de um sistema formulado em internet das coisas?

Possuímos como objetivo geral: Alertar sobre vulnerabilidades inerentes de um sistema formulado em Internet das Coisas. Para alcançarmos esse objetivo geral, temos objetivos específicos a serem alcançados também: Conceituar a Internet das Coisas; compreender a importância da Segurança da Informação; identificar as vulnerabilidades de um sistema modelado em Internet das Coisas.

O método utilizado neste trabalho foi uma pesquisa de cunho descritiva e qualitativa sobre o tema de Internet das Coisas. Tal pesquisa é pertencente à vertentes de metodologias de revisão bibliográfica. A pesquisa realizada a partir do Google Acadêmico obterá informações presentes tanto em artigos científicos, quanto em livros publicados durante o novo milênio. Período em que o tema entrou em pauta com força em seminários sobre tecnologia, tal como entre grandes indústrias visando um impacto de seus produtos no mercado mundial.

2. CONCEITUANDO A INTERNET DAS COISAS

Buscando incrementar as utilidades da Internet moderna ao criar um ecossistema tecnológico, a Internet das Coisas está interconectando os mais variados objetos. Tal feito poderá ajudar a sociedade futura, de um futuro não tão distante, em seu cotidiano. Porém, não restringindo-se à coisas rotineiras.

Para compreender a importância prevista da IoT, faz-se necessário a análise da origem de sistemas de processamento. Segundo Santaella *et al*. (2013, p. 22) "na década de 1930, deu-se o aparecimento teórico da máquina de Turing na sua busca por mecanizar o potencial do pensamento humano para o cálculo. Porém o processo de maturação dessa tecnologia foi longo, emergindo primeiro em máquinas pré-programadas, como calculadoras para tomar forma mais definida em um suporte midiático programável, graças ao

trabalho de Von Neumann na década de 1950".

Turing estava a procura de um algoritmo que fosse capaz de aprender ao receber dados, algo que seria mais explorado futuramente por grandes corporações que, visam atingir um público cada vez maior através de dados obtidos em todo o globo à toda velocidade. Tal ambição de Turing poderia ajudar a população a resolver alguns de seus problemas que mais causavam repercussão na época.

Com essas metas, a IoT surge para ser uma inovação facilitadora, tal como a máquina de Turing foi em seu tempo. Previsões sobre como a vida seria com a tecnologia integrada foram feitas ao longo dos anos. Principalmente na área da ficção. O filme "Eu, Robô", lançado em 2004, baseado no livro de mesmo nome, aborda uma sociedade com robôs já estabelecidos.

Os robôs auxiliam as pessoas em diversas tarefas. Do mais básico, como carregar sacolas de compras, até tarefas mais complexas como a tentativa de salvamento de vidas baseado em probabilidades da chance de sobrevivência de uma determinada pessoa. Compreendendo o que já foi dito, chega a vez, enfim, de falar sobre a própria Internet das Coisas.

Segundo Magrani (2018, p. 20) "de maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em contexto de hiperconectividade".

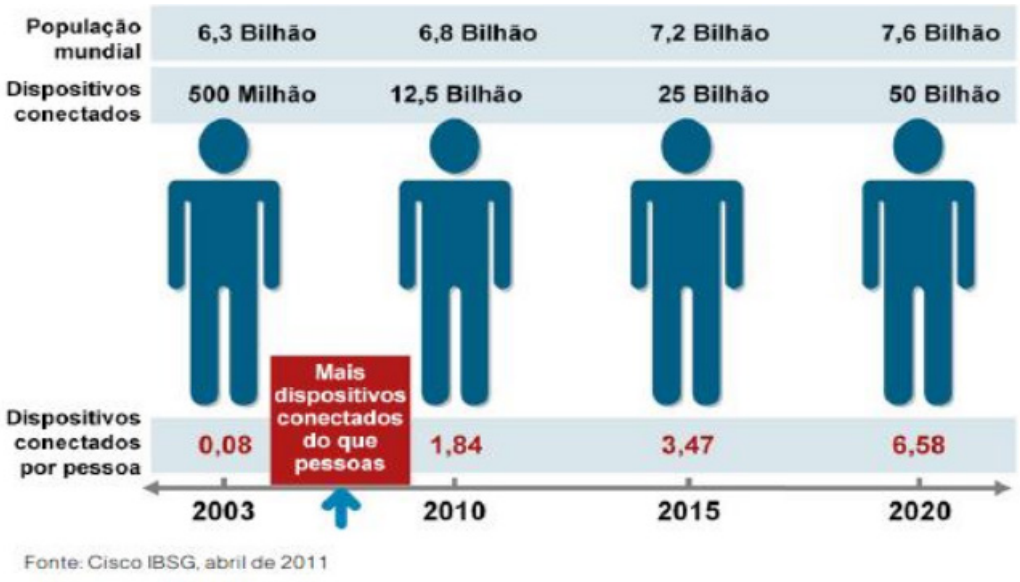


Figura 1 – População x Dispositivos Conectados

Fonte: Cisco IBSG, abril de 2011

A IoT, facilmente aceita na sociedade, já é uma realidade, extrapolando o mundo filosófico e fictício. A IoT é uma tecnologia de inovação que exige recursos financeiros e infraestrutura de ponta para o seu funcionamento pleno. Cada informação obtida contribui para o *Big Data*. Sempre se incrementando de forma recursiva. Atualmente é integrada em vários setores, como as aplicações na indústria, um dos setores mais beneficiados pela IoT.

Segundo Evans (2011), a conectividade à internet está presente mais pelo lado dos "objetos/coisas" do que pelas pessoas em si, tornando a IoT um paradigma, em sua visão. Gradativamente, durante os anos, as pessoas foram adquirindo dispositivos com a capacidade de conectividade com outros aparelhos, e a Figura 1 compara o número destes dispositivos, possuindo uma projeção até o ano de 2020.

Segundo Diniz (2006), toda a ideia que rodeia a internet das coisas é fruto de uma facilitação provida pela internet pois além de permitir a transmissão e comunicação de dados em qualquer lugar, também é considerada a comunicação de qualquer coisa. Juntamente com as abreviações G2C e C2C, também são incorporados ao 'internetês' novas abreviações, sendo elas H2T e T2T.

Vale ressaltar que Internet das Coisas não é restrita apenas a usos triviais, há um vasto universo de possibilidades a serem exploradas, com um breve exercício de criatividade já é possível encontrar alguns exemplos. De Oliveira (2017, p. 17) comenta que a Internet das Coisas está transformando o mundo e como o ser humano se relaciona com os objetos que lhe rodeiam.

Neste processo, segurança, energia, meio ambiente, trânsito, mobilidade e logística também são transformados. Este é o momento ideal para a ocorrência dessa integração de IoT com a sociedade, visto que houve o barateamento dos dispositivos necessários para tal.

Segundo Lacerda e Lima (2015) "A IdC afeta a humanidade em diferentes escalas. Envolve desde *nanochips* implantados em seres vivos a objetos de uso comum interconectados, equipados com sensores e identificados por RFID - capazes de trocar informações entre si, com as pessoas ou com o ambiente - até cidades inteiras sendo projetadas de maneira totalmente conectada e automatizada (as chamadas smart cities ou cidades inteligentes). As formas de manifestação da IdC são heterogêneas, incluindo dispositivos de múltiplos propósitos (celulares, *tablets*, relógios e óculos inteligentes) e dispositivos especializados (sensores de temperatura, dispositivos ativos e passivos etc.), suportados por uma variedade de plataformas de *software* **e** *hardware*. O desafio de projetar espaços na IdC é contemplar os diferentes níveis de granularidade de forma transparente, garantindo a interoperabilidade".

Como já dito anteriormente, Internet das Coisas está presente em várias áreas, visto como a sua versatilidade é o grande fator para a escolha de utilização deste modelo. Alguns exemplos de áreas que se beneficiam da IoT são: Planejamento urbano, comércio, educação, indústria, turismo e muito mais, o futuro está se moldando à Internet das Coisas para extrair o máximo do ser humano.

O setor industrial, citado como um dos mais beneficiados pela IoT, está em sua mais nova fase. A Primeira Revolução Industrial, ocorrida no final século XVIII, foi um marco para a humanidade. Um período de introdução da energia a vapor e a consolidação da produção mecanizada. Sendo um dos fatores cruciais para o surgimento do capitalismo.

A Segunda Revolução Industrial, ocorrida no século XIX, trouxe a descoberta de uma nova fonte de energia, a energia elétrica, além da produção de linha de montagem, por Henry Ford. Essa foi a Indústria que definiu como as outras duas seguintes seriam.

A Terceira Revolução Industrial, também chamada como Indústria 3.0, iniciou-se durante os anos 70, no século XX. Utilizava-se de uma semi automação, ou automação parcial. Utilizando-se de controladores e computadores programáveis por memória. Claramente mais tecnológica que a indústria anterior, 2.0, alterando todo um contexto político/econômico/social.

Por fim, a Quarta Revolução Industrial, o foco para a discussão deste trabalho, chamada de Indústria 4.0. É afirmado por Kagermann *et al.* (2013) que a termologia Indústria 4.0 originou-se em uma feira, especificamente, de Hannover na Alemanha.

Vindo de uma necessidade de uma indústria manufatureira alemã mais competitiva visando maior lucro para a economia do país na época, a Indústria 4.0 aplica tecnologias de informação juntamente da sua comunicação com a própria indústria.

Baseada nos avanços ocorridos na Terceira Revolução Industrial, a Indústria 4.0 está navegando rumo à automação completa. Com seus dispositivos se comunicando através da rede com outros dispositivos. Melhorando uns aos outros com essa troca constante de informação, otimizando o resultado de empresas; aumentando a produtividade de times por completo; transformando o mundo ao seu redor. IoT na Indústria 4.0 deixou a sua marca e mostrou que veio para ficar.

Voltando ao cenário casual do uso de IoT, vulgo uso cotidiano, cidades poderão possuir uma arquitetura totalmente diferente da que conhecemos, tanto no quesito físico/tátil, quanto no quesito legislativo. A máquina terá ações diferentes do ser humano, levando a uma complexa e talvez demorada reestruturação, prometida como algo positivo para todos que estiverem participando deste novo ecossistema, porém, nem só de qualidades vive a IoT.

Com a constante integração de Homem-Máquina, alguns autores de ficção científica tiveram uma visão não tão positiva do futuro para com as pessoas. *Cyberpunk* é um subgênero da ficção científica que nos mostra um futuro distópico onde a tecnologia evoluiu com uma velocidade extrema, porém, não melhorou a qualidade de vida dos seres humano, revelando uma má integração da Internet das Coisas na sociedade.

Criado em 1983 por Bruce Bethke, um escritor norte-americano, o subgênero ganhou muita popularidade devido à essa visão pessimista da tecnologia, mas sem chegar no extremo de dominação por parte das máquinas, algo que 'Matrix' (1999) e 'O Exterminador do Futuro' (1984) fizeram. A ficção científica é uma área que explora bastante tais temas e seus impactos no mundo.

Segundo Amaral (2003, p. 4) "A visão cyberpunk reconhece o enfraquecimento do espaço público e o aumento da privatização da vida social, na qual os laços sociais fortes não existem mais. Para os autores, nesse espaço público as pessoas são tecnologizadas e reprimidas ao mesmo tempo, sendo que a tecnologia média nossas vidas sociais. É ainda mais fácil de perceber tais características nas imagens mostradas nos produtos culturais como videoclipes, filmes, livros, comerciais, todos enfatizando a interação e interface homem-máquina, seja via internet, realidade virtual, RPGs etc."

A 'cibernetização' do ser humano pode ser considerada o ápice da Internet das Coisas, esse é o momento, na ficção, em que a sociedade começa a ruir, visto que não há como suprir as necessidades de uma sociedade tão avançada e custosa. Em decorrência disso, muitas pessoas não terão acesso às novas tecnologias, tornando-se assim alheias à sociedade, sendo marginalizadas e esquecidas.

Por causa disso, crimes irão aumentar, dados valiosos serão perdidos ou vendidos clandestinamente, e no meio dessa bagunça toda, estarão grandes empresas; responsáveis por fornecer tal tecnologia ao mercado; travando guerras entre si para ver quem tem mais posse de informações pessoais de pessoas pertencentes a esse ecossistema *Cyberpunk*.

Mesmo parecendo um futuro distante e pessimista, alguns cuidados devem ser tomados para evitar que uma possível catástrofe tecnológica ocorra, por conta disso, todo

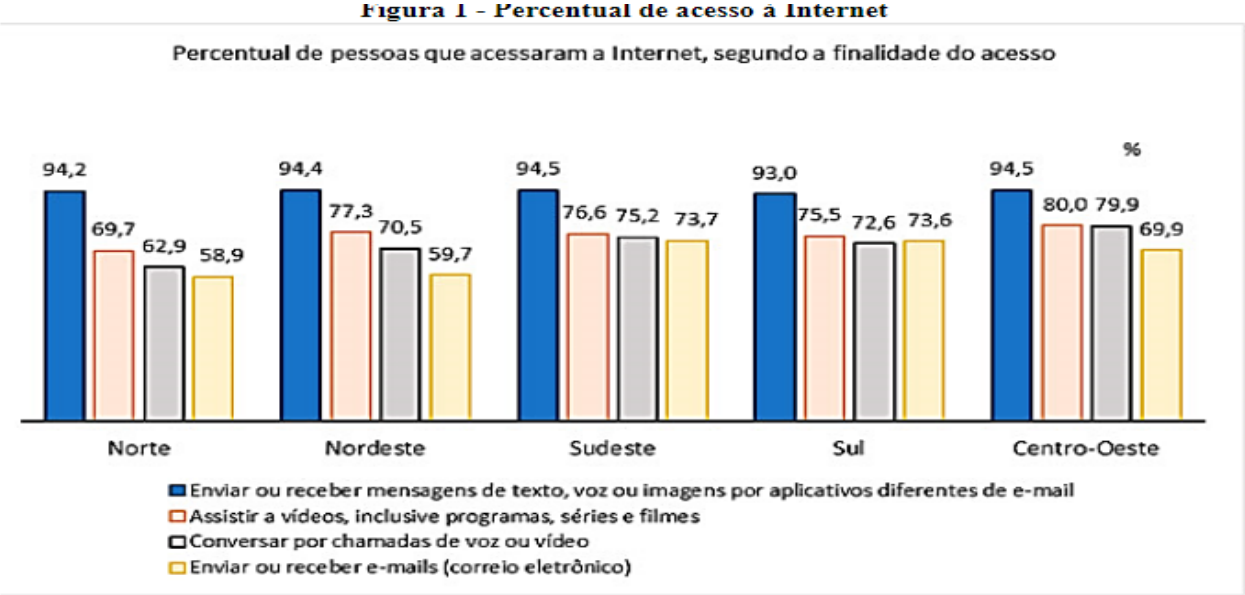
investimento em segurança é necessário. O próximo capítulo abordará com mais detalhes sobre a importância da Segurança da Informação em sistemas baseados em Internet das Coisas.

Quando se faz parte de um ambiente conectado com a rede, é comum pensar na proteção de informações, principalmente de informações pertencentes a grandes empresas, informações essas que valem muito dinheiro, e neste mundo em que se vive, existem muitos *hackers* esperando o momento certo para lucrar com ações ilícitas, neste contexto, a Segurança da Informação é muito necessária e eficiente para proteção de ativos virtuais.

3. COMPREENDENDO A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Em pleno século XXI, o ser humano nunca esteve mais conectado. Crianças, adolescentes, adultos, todos estão acessando a rede, trocando informações pela internet. O Instituto Brasileiro de Geografia e Estatística (IBGE) revelou a partir do PNAD Contínua TIC 2016 a porcentagem de pessoas que utilizaram a Internet para a troca de mensagens, tanto de texto, imagens ou mensagens de voz através de diversos aplicativos. Assistir vídeos, entre outras finalidades. A Figura 2 mostra a tal porcentagem em um gráfico separado por regiões brasileiras.

Figura 1 - Percentual de acesso à Internet



Ao analisar-se a Figura 2, percebe-se o alto número de pessoas que utilizam-se da Internet. Com tal fato em vista, faz-se importante a presença da Segurança da Informação, abreviada de SI, para manter os dados de cada usuário da Internet sob sigilo, visto que possuem certo valor.

Segundo Silva Netto (2007) “podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos”.

Para Araujo (2009, p. 36) “A segurança da informação é uma preocupação antiga, mas é um tema pouco explorado como objeto de pesquisa sob a ótica da Ciência da Informação. No mundo conectado em rede, onde a informação flui, as organizações, sejam empresas privadas ou do setor governamental, necessitam de processos e controles de segurança para garantir e preservar suas informações de uma gama de novas ameaças”.

Ao participar de um contexto no qual os objetos do dia a dia estão conectados, juntamente das pessoas, é de suma importância que dados sejam criptografados eficientemente, visto que tais informações são valiosas para o processo do auxílio na tomada de decisões, especificamente em quesitos sociais.

Os critérios descritos na Segurança da Informação são confidencialidade, integridade, disponibilidade, autenticidade. ACID em abreviatura. Confidencialidade trata do limite do acesso à determinada informação para sua entidade provedora.

Integridade trata da garantia de uma informação em sua forma original, livre de qualquer alteração que poderia sofrer nas mãos de alguma outra entidade que não fosse a entidade provedora.

Disponibilidade trata de a capacidade da informação ser acessível, independente da situação em que o armazenamento de uma determinada informação esteja. É importante, principalmente, para garantir a segurança contra perda de alguma informação.

Por fim, a autenticidade consiste na certeza de que a fonte de informação é uma fonte verídica, sendo capaz de realizar a verificação da identidade do provedor desta informação. A partir dos conceitos apresentados, infere-se que um sistema baseado em IoT precisa necessariamente de um bom sistema de Segurança da Informação para garantir que suas funcionalidades estejam em pleno uso, seja para transmitir dados através da rede, ou também para interagir com o mundo físico em que se vive.

Como dito por Silva (2018, p. 7) “as pessoas são o alicerce de qualquer empresa, e a implantação de uma nova ferramenta de software deve ter um foco maior para esses colaboradores que alimentarão esse software”. Isso indica que as empresas deverão implantar tecnologias que estejam de acordo com o perfil dos seus funcionários para haver melhor aproveitamento destes com o meio em que se trabalham.

Portanto, devido à massiva utilização dos recursos tecnológicos em diversos setores socioeconômicos, é necessária a garantia de eficiência e longevidade de tais recursos, visto a sua importância. A política da Segurança da Informação é um fator a ser considerando quando se pensa acerca do tema.

Segundo Fontes (2012, p. 20) “a política define o escopo para o qual serão considerados os controles de segurança a informação que serão desenvolvidos e implantados. A Gestão de Risco, considerando o contexto definido pela política de segurança, identificará os ativos, selecionará os controles apropriados e definirá as prioridades de implantação destes controles. A não implantação da política impede o desenvolvimento adequado da segurança da informação na organização, uma vez que faltarão referências para implantação dos controles. Sem a política não haverá a definição do escopo que delimita o campo de ação dos controles, e esta falta de limites fará com que o processo de segurança da informação seja infinito e nunca possa ser avaliado adequadamente”.

Então é necessário que a probabilidade da inexistência da política seja minimizado ao máximo. Citado esse risco, Fontes (2012, p. 21) afirma que para “a redução ou eliminação deste risco, faz-se necessária a implantação de um aglomerado de regulamentos, dando início pela política principal, ou diretriz, definidora do escopo e dos limites da gestão de risco”.

Tais regulamentos também serão aplicados aos funcionários pertencentes à empresa. Para Hintzbergen *et al*. (2018, p. 1) “os funcionários precisam saber por que devem cumprir diariamente as regras de segurança. Os gerentes imediatos precisam ter esse entendimento, uma vez que são responsáveis pela segurança da informação no seu departamento”. Ou seja, os regulamentos de segurança da informação são responsáveis pelo uso

estruturado da informação presente na organização, de tal forma que o empreendimento/negócio não seja prejudicado por um mal uso da mesma, lembrando que tal mal uso pode ser efetuado acidentalmente, o que deve ser levado em conta sempre.

A gestão da Segurança da Informação é uma questão a ser tratada com bastante cautela pois a política de segurança descreve todos os processos e regras a serem seguidas para o uso do recurso informacional, tendo em mente qualquer ambiente a qual ele esteja inserido, explicitando para todos os usuários que acessarem a informação qual a filosofia da empresa acerca deste recurso, com o objetivo de assegurar a proteção das informações da organização, tal como de seus clientes.

Segundo Fontes (2008) "a política e demais regulamentos definem estratégias, regras, padrões e procedimentos que direcionarão todas as ações para atingirmos os objetivos de segurança da informação. Essas ações podem ser atividades técnicas ou atividades de usuários. Sem uma política ficamos sem saber para onde queremos ir, sem saber qual é a filosofia da organização sobre o assunto segurança e qual o nível de proteção desejado para a organização".

Porém, a política não pode e nem deve surgir ao acaso pois deve estar alinhada aos objetivos da organização/empresa. Objetivos de segurança da informação serão criados baseados nos objetivos de negócios, estes que são dependentes do uso dos recursos informacionais.

Como missão, cabe a todos da organização proteger a informação, independente do cargo que estejam ocupando, por isso todo esse processo de Segurança da Informação se trata de um trabalho coletivo. Esse último é importante para prevenir casos de engenharia social.

Sobre a política, para se adequar estruturalmente, é necessário que exista o fio condutor, a política principal. A política principal deverá estar contida em um documento de simples compreensão para os funcionários da empresa, visto que eles devem saber o modo como a empresa desejará que seja realizado o tratamento da informação, tais como as responsabilidades pertencentes a cada funcionário.

Acerca da Política de Segurança da Informação, a Norma NBR ISO/IEC 27001 é de suma importância durante o processo de gestão de riscos. Segundo Fontes (2012, p. 34) "A NBR ISO/IEC 27001 descreve uma orientação para a existência de um Sistema de Gestão da Segurança da Informação (SGSI), considerando o Modelo PDCA (*Plan, Do, Check, Act*). O relacionamento desta norma com esta pesquisa se deve ao fato de que a política de segurança da informação está contemplada na etapa de Planejamento (*Plan*) de Modelo PDCA do SGSI".

Ou seja, a norma NBR se trata de uma política buscando padronizar o modo ao qual um SGSI deve ser efetuado. É uma forma efetiva de medir o nível de segurança de um sistema baseado em Internet das Coisas, ao relacionar o escopo do SGSI com a política de segurança da informação.

Segundo Wagner (2009, p. 38) "a NBR ISO/IEC 17799 define a informação como 'um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegido".

Visando o funcionamento apropriado do SGSI, faz-se necessária a transparência da gestão de riscos e a política de segurança da informação para com todos os envolvidos, os conceitos pertencentes à segurança também devem ser apresentados e discutidos.

Segundo Hintzbergen *et al.* (2018, p. 18) "Para entender como a segurança pode ser

gerenciada, diversos conceitos importantes devem ser explicados primeiro. “Vulnerabilidade”, “ameaça”, “risco” e “exposição” são termos frequentemente usados para representar a mesma coisa, mesmo que tenham diferentes significados e relações entre si. É importante entender a definição de cada palavra, mas mais importante ainda é entender as suas relações com outros conceitos”.

Após apresentados os conceitos, os gerentes e funcionários devem entender quais dados serão protegidos e a sua importância para a empresa ao qual participam. Outro conceito a ser apresentado é a análise de risco, que trata-se da obtenção de conhecimento acerca das possibilidades, benefícios e riscos envolvidos, realizando sempre esse paralelo entre benefício e risco.

Para efetuar tal análise de riscos, deve-se fazer um levantamento de requisitos de segurança. Segundo Hintzbergen *et al.* (2017, p. 18) “requisitos de segurança são identificados através de uma avaliação metódica de riscos de segurança. As despesas com controles devem ser equilibradas de acordo com os danos, resultantes de falhas de segurança mais prováveis de ocorrer no negócio. Os resultados da avaliação do risco ajudarão a guiar e a determinar a ação apropriada de gestão e as prioridades para gerenciar os riscos de segurança da informação e para implementar os controles escolhidos para proteção contra risos e ameaças”.

Com todos os dados obtidos, a avaliação de risco será realizada, além do mais, a avaliação do risco deve ser repetida frequentemente, visto que toda e qualquer mudança, mínima que for, pode influenciar nos resultados parciais e finais da análise de risco.

No entendimento de Araujo (2009, p. 43) “o receio de perder informações sigilosas e sistemas, de sofrer com os ataques virtuais, desenvolvidos pelos cibercriminosos gerou uma paranóia nas organizações, que têm realizado investimentos consideráveis para proteger seus ativos informacionais. Para evitar desastres irremediáveis, os indivíduos da organização devem estar cientes e atentos à segurança da informação implementada na organização. Com o entendimento da importância desse tema e seguindo recomendações de organismos internacionais, o Governo Federal brasileiro instituiu pelo Decreto nº 3.505, de 13 de junho de 2000, uma política de segurança da informação nos órgãos e entidades da administração pública federal”.

Tal política de segurança da informação tem como finalidade: proteger assuntos merecedores de tratamento especial, assegurar os direitos individuais e coletivos do povo, a confidencialidade de sua privacidade e correspondência será inviolável, de acordo com as disposições da constituição, capacitação dos segmentos das tecnologias sensíveis, uso predominante de mecanismos de segurança da informação, com o controle de tecnologias sensíveis e duplicativas, desenvolvimento e maturação de mentalidade de segurança da informação, treinamento voltado para a área científica e tecnológica nacional para utilizar-se da criptografia com o objetivo de defesa do estado e por fim, conscientizar as entidades superiores federais sobre a importância das informações pertencentes ao estado e também sobre o risco que a vulnerabilidade dessas informações apresenta.

4. CONCEITUANDO A GESTÃO DE RISCOS

Após as análises sobre Segurança da Informação e Avaliação do Risco, a gestão de riscos, como o nome sugere, se trata de como os envolvidos em um projeto irão lidar com as probabilidades de falhas ocorrerem, tal como os riscos que as falhas representam para a empresa, o projeto e a todos envolvidos.

Para Best (1998, p. 2) “o risco só tem um sentido verdadeiro à medida em que resulta em perdas financeiras, quer direta, quer indiretamente. As instituições financeiras enfrentam muitos riscos, que podem, se não for controlada, dar origem a riscos financeiros”.

Em outras palavras, gestão de risco trata-se do controle e gerenciamento de riscos por parte de empresas, tendo em mente a questão de orçamento estipulado para ser investido em determinado serviço. Requer uma alta habilidade para prever questões relacionadas ao mercado e ao público que a empresa visa atingir, tal como deve-se ter em mente quais informações serão importantes e devem ser mantidas seguras ao longo prazo, por isso vulnerabilidades devem ser evitadas o máximo que puderem.

Segundo De Almeida (2014, p.26) “a análise de vulnerabilidades pode ser uma resposta a dificuldades na estimação do risco, permitindo atenuar os inconvenientes associados a incertezas significativas, em particular na estimação de probabilidades, e ser mais eficaz operacionalmente:

- Pode ser independente de probabilidades de ocorrência;
- Tem um enfoque em mitigação de danos e na capacidade de recuperação (resiliência) face a ameaças futuras possíveis;
- Pode incluir a perceção social dos riscos e o controlo da Exposição;
- Inclui cenários holísticos e cadeias de causalidade física simplificadas (Vulnerabilidade Social). Dificuldades potenciais da análise de vulnerabilidades:
- Possibilidade de análises de custo/benefício no presente, sem a moderação dos valores expectáveis ou das probabilidades de cada cenário;
- Pode empolar consequências possíveis mais pouco prováveis;
- Pode tornar mais difícil de hierarquizar as ações na qualidade de variável de decisão!”.

Todo o processo de gestão de riscos é uma parte importante quando se planeja construir um sistema baseado em Internet das Coisas, visto que se deve sempre aprender com os erros, mesmo os erros mais elementares, para melhorar o sistema toda vez que um erro novo surgir, nada deve ser ignorado.

Segundo Araujo (2009, p.47) “o risco pode ser de diferente natureza: financeiro, de projeto, relacionado a pessoas etc. Por essa razão, gerir ou administrar risco é uma atividade que permeia vários setores de uma organização. Portanto é foco de estudo em diferentes áreas: Economia, Contabilidade, Administração, Engenharia, Tecnologia da Informação, Ciência da Computação etc.”

A gestão de riscos está presente em diversas áreas, uma delas é a área computacional, como já citado. Nesta área, muitas vezes os programadores costumam ficar em um impasse, ou seja, deve-se ser inovador e correr mais riscos, que podem arruinar todo o projeto, ou deve-se ser conservador e realizar procedimentos já consagrados, porém caindo na mesma fórmula, como dito anteriormente, consagrada funcional.

Segundo Assi (2021) “O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações e pode envolver perdas, bem como oportunidades. Em finanças, a relação risco-retorno indica que, quanto maior o nível do risco aceito, maior o retorno esperado dos investimentos. O risco tanto é uma propriedade objetiva de um evento ou atividade, relativa à probabilidade de ocorrência de um evento adverso bem definido, como também é uma construção social e cultural”.

Na visão de Tittel *et al.* (2003, p. 178), a possibilidade de que algo aconteça e os dados

sejam danificados, destruídos ou expostos é chamado de risco. O gerenciamento de riscos, do inglês *Risk Management*, também conhecido como gerência de riscos, foi desenvolvido para solucionar esse problema.

Para Assi (2021) “o risco está associado às leis de probabilidade, fatos novos ou inesperados podem ocorrer sempre, o risco tem de ser algo possível”. Ou seja, o risco deve ser sempre algo palatável ao ecossistema em que o produto/projeto está inserido, podendo ou não ser algo surreal.

Em resumo, a gestão de risco trata-se de todo um processo, coletivo, que visa a identificação de fatores, ou circunstâncias, que possam prejudicar e expor o dado a ser protegido, em conjunto com a avaliação do risco, O principal objetivo do gerenciamento de riscos é reduzir os riscos a um nível aceitável. O que é esse nível depende da organização, do valor de seus recursos e do tamanho de seu orçamento.

Na visão de Assi (2021) “a gestão de riscos precisa considerar o desconhecido e devemos nos concentrar não somente naquilo que podemos compreender, mas encontrar oportunidades que podem ser aproveitadas, desde que entendamos melhor o que se passa à nossa volta. Simplificar os fatos e acontecimentos é importante, mas avaliar como trata-los se torna mais relevante”.

Também, segundo Assi (2021) “a ameaça é um risco na segurança corporativa, pois é um evento capaz de produzir perdas reais e em certos casos mensuráveis por um padrão comum (é definido pela organização – pode afetar seu balanço e suas finanças até o desgaste de sua imagem interna ou externa, que serão mensurados pelo impacto da reputação em seus serviços ou produtos)”.

Segundo Tittel *et al*. (2003, p. 179), a análise de risco é efetuada visando “fornecer à administração as informações necessárias para decidir quais riscos devem ser tratados, transferidos ou aceitos”. Como resultado, uma comparação de custo-benefício entre o custo esperado de perda de ativos e o custo de implantação de proteção contra ameaças e vulnerabilidades será mostrado e avaliado.

A análise do risco, citada anteriormente, identifica e avalia os riscos pautados na realidade e a gravidade do impacto que possíveis ameaças podem causar à questão do orçamento relacionado à segurança do produto final, sendo de extrema importância durante o processo de tomada de decisão, um aliado dos lucros obtidos pela empresa.

Segundo Krutz e Vines (2001, p.19) “comumente utilizada para atribuir um valor a alguma função que possa ser perdida/corrompida/exposta de um negócio, os resultados principais da análise de risco, que são a identificação dos riscos e a justificativa financeira para o investimento em contramedidas são vitais para a construção estratégia para redução de risco, além do mais, a gestão de risco é composta por atributos, fazem parte desses atributos a execução de análise de risco, a análise de custo/benefício do processo de segurança, implementação desse sistema, revisão e manutenção dos protocolos de segurança implementados”.

Em suma, os processos efetuados para a implementação da gestão de riscos em uma empresa podem ser divididos em 4 partes: mapear, classificar, monitorar e tratar. Durante a fase de mapa, é realizado o mapeamento geral de riscos no projeto, é importante ter conhecimento da maioria das possibilidades de algo dar errado; ou todas, se possível.

Durante a fase de classificação, os riscos serão “postos à mesa” para então serem classificados em seu grau de prejuízo. Tal classificação pode ser realizada de uma maneira qualitativa ou quantitativa, dependendo dos objetivos da empresa, tal como da renda gerada pela organização.

Segundo Krutz e Vines (2001, p. 21) “a diferença entre análise de risco quantitativa e qualitativa é simples: a quantitativa realiza tentativas de atribuição de valor numérico ou monetário objetivo a componentes de avaliação de risco e avaliação de perda potencial, enquanto qualitativa se concentra mais em dados e outros valores intangíveis ativos, não apenas valor puro. Quando todos os elementos (valor recursos, impacto, frequência de ameaças, eficácia de proteção, custo de proteção, incerteza e probabilidade) são valores medidos, divididos e atribuídos, o processo é considerado totalmente quantitativo. No entanto, a análise de risco com quantificação completa é impossível porque, de alguma forma, medidas qualitativas devem ser aplicadas”.

A fase de monitoramento é marcada por estratégias propostas para ações em caso de risco real. Tal risco pode ser algo que não chegou a ocorrer, mas já foi previsto ou algo que ocorreu anteriormente. Essas estratégias são nada mais que planos de contingência visando a perda mínima de lucros e recursos empresariais, facilitando todo o processo de monitoramento e como os envolvidos no projeto irão lidar com tal situação.

Por fim, a fase de tratamento é justamente o último estágio desse processo todo, no qual os funcionários irão aplicar correções e tentarão tratar os riscos, seja investindo mais em sistemas de segurança, investindo em treinamentos especializados para os funcionários, uma reformulação na equipe de trabalho, entre outras configurações.

Todos esses processos são tentativas de eliminar a causa raiz do que pode se tornar um enorme problema para a organização. Porém, nem sempre é possível efetuar 100% o tratamento da questão, por isso faz-se necessário ter vários planos de contingência para tentar contornar tais situações adversas, lembrando que nenhuma solução é absoluta pois as tecnologias estão constantemente sendo atualizadas, causando mais e mais furos de segurança.

Sobre o processo de gestão de risco, segundo Araujo (2009, p. 50) “para permitir esse processo, algumas propriedades dos vários elementos necessitarão ser determinadas, como; por exemplo, o valor dos recursos, ameaças, vulnerabilidades e a probabilidade dos eventos. Uma parte preliminar do processo de gestão de risco está em atribuir valores às ameaças e estimar sua frequência, ou a probabilidade dessa ameaça ocorrer”.

Visando estimar o valor de perdas perante uma ameaça, toda informação/propriedade intelectual deve ser avaliada conforme a sua importância, após isso, a propriedade intelectual possuirá um valor financeiro correspondente. Vale lembrar que não se trata de um *Token* não fungível.

Uma breve descrição sobre *Token* não fungível é a seguinte: basicamente trata-se de um certificado digital de propriedade criptográfico utilizado para confirmar a autenticidade de algum ativo, bastante utilizado no mercado de criptomoedas e estendendo-se também a outros mercados, como o mercado de *cardgames*, por exemplo.

Segundo Araujo (2009, p. 55) “existem diferentes razões para determinar o valor de um ativo, como: necessidade de realização de uma análise de custo/benefício; necessidade de implementação de seguros; provisão de informações para decisões na seleção das proteções; e também pode ser necessário satisfazer o cuidado devido, prevenir negligências e atender responsabilidades legais”.

Ao especificar, por exemplo, um ambiente corporativo de trabalho, é possível obter-se mais detalhes sobre os processos do gerenciamento de risos. Nas palavras de Haynee e Free (2014), o Gerenciamento Corporativo de Riscos é interpretado como uma ferramenta necessária para que o valor do negócio empresarial seja preservado. Na visão de Souza (2011), esse processo começa ao identificar, medir e controlar os riscos de negócio, como

citado anteriormente.

Segundo Araujo (2009, p. 56) “gerenciar o risco é uma atividade permanente nas organizações, pois sempre estão surgindo novas ameaças que se constituem em novos riscos, e não existe forma de eliminar todos os riscos já conhecidos. Embora os efeitos de um risco possam ser minimizados, com a implementação da análise de risco e com a valoração de ativos, que pode identificar quais ativos devem ser protegidos. Este fator é agravado quando se trata de ativos intangíveis, que afetam diretamente as organizações da sociedade do conhecimento. Neste sentido, o estudo de aspectos relacionados à gestão do conhecimento torna-se importantes no contexto das organizações”.]

Como citado acima, todo o processo de gerenciamento e análise de riscos é algo a ser sempre pensado por organizações. Às vezes não compensa tomar certas decisões se os riscos forem muitos, por esse motivo que grandes empresas precisam ter uma boa equipe de gestão pois um pequeno erro pode custar muito caro. Embora muitas vezes não possam ser eliminados por completo, os riscos podem ser minimizados e a situação pode ser otimizada para permitir operações que atuem sob o efeito de um risco para uma grande empresa.

5. CONSIDERAÇÕES FINAIS

A IoT foi a maior inovação tecnológica deste século, trazendo comodidade à humanidade, porém tornando-a dependente de sua própria criação. Essa dependência torna-se evidente ao observar o valor que as informações contidas na rede possuem. Empresas realizam investimentos, usuários armazenam dados, majoritariamente importantes, ambos acrescentando ao Big Data, que é a coletânea de informações presentes na internet.

Estes dados podem ser utilizados para fins comerciais, por parte de empresas; ou fins criminosos, por parte de ciber-criminosos. Onde ocorre o roubo de informações em troca de dinheiro por parte da vítima ou por parte de outras empresas; ocorrendo, assim, um loop, onde mais dados são roubados e comercializados, gerando uma maior necessidade de melhoria em setores de segurança da informação.

Observa-se, também, todo o processo de desenvolvimento da indústria no último século, em que tal desenvolvimento ainda ocorre até os dias atuais. Esta evolução relaciona-se principalmente com a Internet das Coisas e a sua versatilidade para com diferentes áreas de atuação em diferentes indústrias de produção.

A partir do estudo realizado, observa-se como o número de pessoas conectadas em função ao número de dispositivos existentes têm crescido de forma não proporcional, porém, proporcionalmente a este aumento, a necessidade de uma segurança melhor tal como o número de pessoas mal intencionadas também aumentou, portanto faz-se necessário uma intervenção dos profissionais da área de segurança da informação para a redução e até a extinção de problemas relacionados à brecha em sistemas de segurança online, tendo em vista todo o processo quase simbiótico que rodeia as pessoas e a tecnologia existente.

Referências

AMARAL, Adriana. Cyberpunk e Pós-modernismo. **Biblioteca On-Line de Ciências de**, 2003.

ARAUJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento**. 2009.

ASSI, Marcos. **Gestão de riscos com controles internos**. Saint Paul Editora, 2021.

BEST, P. **Implementing Value-at-Risk**. New York: John Wiley & Sons, 1998.

DE ALMEIDA, A. Betâmio. Gestão do risco e da incerteza. Conceitos e filosofia subjacente. **Realidades e desafios na gestão dos riscos: diálogo entre ciência e utilizadores Publicado por**, 2014.

DE OLIVEIRA, Sérgio. **Internet das coisas com ESP8266, Arduino e Raspberry PI**. Novatec Editora, 2017.

DINIZ, Eduardo Henrique. **Internet das coisas.** 2006.

Evans, D. (Abril de 2011). **The Internet of Things** Fonte: Cisco: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Brasport, 2012.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008.

HAYNEE, C.; FREE, C. **Hybrid professional groups and institutional work: COSO and the rise of enterprise risk management. Accounting, Organizations and Society**, v.39, p.309- 330, 2014

HINTZBERGEN, Jule *et al*. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Brasport, 2018.

IBGE/2017 Fonte:<https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar--mensagens> Acesso em: Jan.2019

KAGERMANN, H *et al.* **Recommendations for implementing the strategic iniative Industrie**. 2013.

KRUTZ, Ronald L.; VINES, Russell Dean. **The CISSP Prep Guide:** mastering the ten domains of computer security. USA: Wiley Computer Publishing, 2001.

LACERDA, Flavia; LIMA-MARQUES, Mamede. Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas. **Perspectivas em Ciência da Informação**, v. 20, p. 158-171, 2015.

MAGRANI, Eduardo. **A internet das coisas**. Editora FGV, 2018.

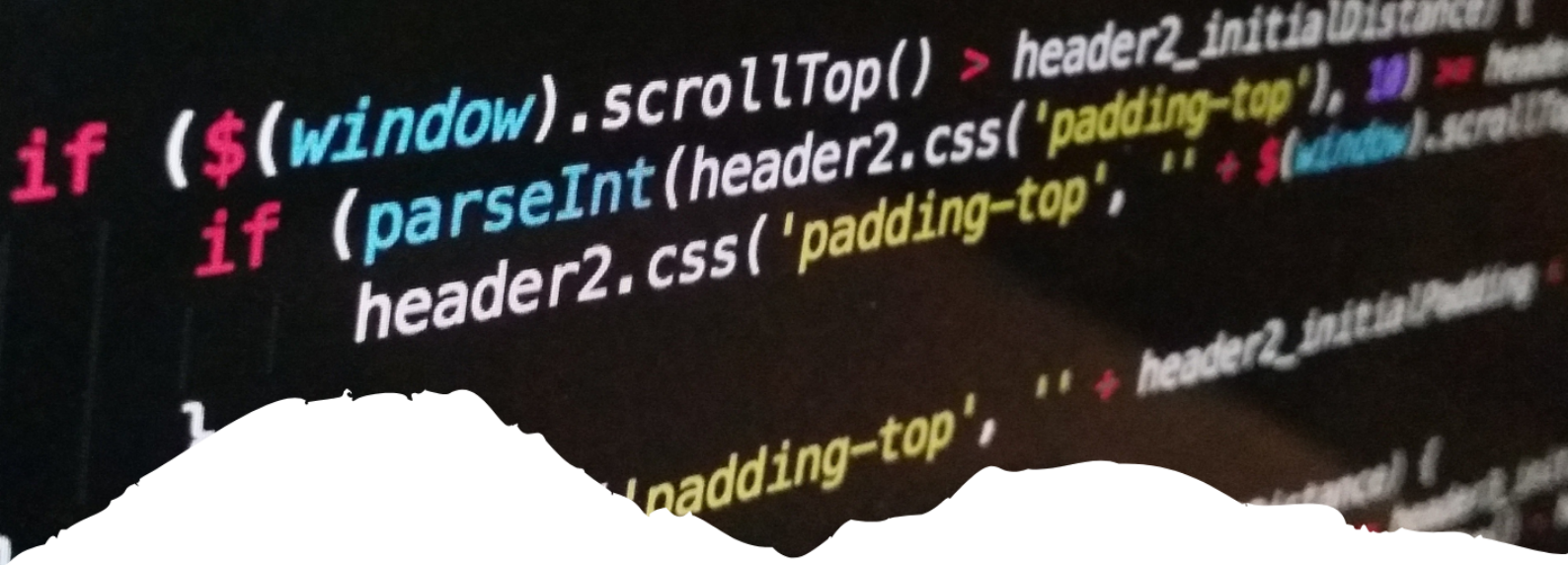
SANTAELLA, Lucia *et al*. Desvelando a Internet das coisas. **Revista GEMInIS**, v. 4, n. 2, p. 19-32, 2013.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, p. 375-397, 2007.

SILVA, Marina Santos; DE AZEVEDO, Viviane Ramalho. ESTUDO SOBRE A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO PARA EVITAR ATAQUES DE ENGENHARIA SOCIAL. **Gestão e Tecnologia: Reflexões e Práticas**, p. 72.

SOUZA, J. S. **Modelo para Identificação e Gerenciamento do Grau de Risco de Empresas – MIGGRI. Tese (Doutorado em Engenharia).** Universidade Federal do Rio Grande do Sul - UFRGS, Porto Alegre, 2011.

TITTEL, Ed; CHAPPLE, Mike; STEWART, James Michael. **Certified information systems, security professional:** study guide. San Francisco: SYBEX, 2003.



13

GERENCIAMENTO DE REDES EM INSTITUIÇÕES DE ENSINO FUNDAMENTAL

NETWORK MANAGEMENT IN ELEMENTARY EDUCATION INSTITUTIONS

Paulo Riler Oliveira Faustino

Resumo

O objetivo deste trabalho foi investigar a gestão de redes em instituições de ensino fundamental. A pesquisa se concentrou em identificar as principais dificuldades enfrentadas pelos gestores de redes e as soluções adotadas para melhorar a eficiência da gestão. A metodologia utilizada envolveu a realização de entrevistas com gestores de redes de diferentes escolas, bem como a análise de documentos e relatórios relacionados ao tema. A partir dos resultados obtidos, concluiu-se que as principais dificuldades enfrentadas pelos gestores de redes em instituições de ensino fundamental incluem a falta de recursos financeiros, a falta de capacitação técnica dos profissionais envolvidos e a falta de planejamento estratégico. No entanto, algumas soluções foram adotadas pelos gestores para enfrentar esses desafios, como a terceirização de serviços, a realização de treinamentos e a elaboração de planos de ação. Em geral a pesquisa demonstrou a importância de uma gestão eficiente de redes em instituições de ensino fundamental para garantir um ambiente educacional seguro e com acesso à tecnologia de qualidade.

Palavras-chave: Sistemas de Informação, Ambiente Escolar, Segurança da Informação, Vulnerabilidades, Proteção de Dados.

Abstract

The objective of this work was to investigate network management in elementary education institutions. The research focused on identifying the main difficulties faced by network managers and the solutions adopted to improve management efficiency. The methodology used involved conducting interviews with network managers from different schools, as well as analyzing documents and reports related to the topic. From the results obtained, it was concluded that the main difficulties faced by network managers in elementary education institutions include the lack of financial resources, the lack of technical training of the professionals involved and the lack of strategic planning. However, some solutions were adopted by managers to face these challenges, such as outsourcing services, conducting training and drawing up action plans. In general, the research demonstrated the importance of efficient network management in elementary education institutions to ensure a safe educational environment with access to quality technology.

Keywords: Information Systems, School Environment, Information Security, Vulnerabilities, Data Protection.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes.

As redes de internet são essenciais em instituições de ensino fundamental, já que o acesso à informação e o uso de tecnologia são fundamentais para o aprendizado das crianças. Entretanto, a segurança dessas redes pode ser comprometida, expondo alunos e professores a riscos de ataques cibernéticos, roubo de informações pessoais, e até mesmo exposição a conteúdos inadequados. Nesse contexto, este trabalho tem como objetivo analisar a segurança de redes de internet em instituições de ensino fundamental.

As Instituições de Ensino têm encontrado muitas dificuldades em proteger dados importantes devido a vulnerabilidades descobertas pelas empresas de segurança cibernética, e esse é um grande motivo de preocupação, pois essas Instituições possuem uma grande necessidade de proteção das informações, mas a quantidade de brechas de segurança é imensa, muitas nem foram descobertas pelas empresas de segurança ainda, podendo ser usadas para roubo de informações, o que pode causar sérios problemas, e inclusive processos jurídicos à Instituição.

A segurança das informações contribuirá para o desenvolvimento das Instituições, mantendo principalmente qualidade e confiabilidade nos serviços prestados para com os alunos e pais e evitará grandes prejuízos, pois, uma Instituição de Ensino que não investe em segurança corre o risco de perder muito dinheiro e encontra dificuldades para desenvolver e expandir novos negócios.

Ao investir em segurança física e lógica da informação, as Instituições de Ensino se destacam em um mercado cada vez mais competitivo. Isso é importante porque protege todas as categorias de dados contra roubo e danos. Isso inclui informações confidenciais, informações pessoais, informações de saúde, direitos de propriedade intelectual, dados e sistemas de informação, tanto dados corporativos quanto governamentais.

Analisando as informações, vemos como esta pesquisa pode contribuir para a área acadêmica com um tema importante a ser desenvolvido tendo em destaque a segurança das informações de Instituições de Ensino Fundamental que será utilizado para auxiliar nas tomadas de decisões através da tecnologia.

O problema de pesquisa deste trabalho é verificar se as redes de internet em instituições de ensino fundamental estão adequadamente protegidas contra os ataques cibernéticos e exposição a conteúdos inapropriados. Analistas do setor de segurança cibernética afirmam que a educação é a categoria mais vulnerável a ataques cibernéticos, visto que 81,65% dos incidentes relacionados a malware analisados pelos pesquisadores em um período de 30 dias vieram desse setor.

Não basta um bom firewall ou equipamentos de última geração para proteção da rede, é preciso manter os serviços bem implementados, configurados e atualizados para melhorar a segurança das informações internas e sensíveis da instituição, o que exige estratégia, conscientização administrativa e treinamentos na área de T.I. e segurança da informação para todos os colaboradores. Portanto, a segurança lógica e física das informa-

ções institucionais é importante.

O objetivo geral deste trabalho é identificar as principais ameaças cibernéticas enfrentadas pelas instituições de ensino fundamental e propor medidas de segurança para preveni-las. Para alcançar esse objetivo, serão propostos os seguintes objetivos específicos:

- Identificar as principais ameaças cibernéticas enfrentadas pelas instituições de ensino fundamental;
- Analisar as medidas de segurança atualmente adotadas por instituições de ensino fundamental;
- Propor medidas de segurança adicionais para prevenir ameaças cibernéticas em instituições de ensino fundamental.

2. DESENVOLVIMENTO

2.1 Importância do sistema de informação para o ambiente escolar

Os Sistemas de Informação atuam como um facilitador para o gestor escolar, trazendo mais eficiência, agilidade e segurança para o ambiente de tecnologia da escola. Eles permitem conectar todas as soluções de modo automatizado, possibilitando a interação entre elas de forma integrada.

No dia a dia das escolas, principalmente aquelas que passaram ou estão passando por um processo de transformação digital, é comum encontrar vários sistemas compondo o ambiente tecnológico da instituição.

A integração de sistemas, além de centralizar todo seu ambiente de tecnologia em um só lugar, mantem um controle atualizado de todos os dados, usando somente um login e senha, bem como disponibiliza as informações para áreas diferentes.

O desenvolvimento da sociedade da informação, em que se multiplicam as possibilidades de acesso a dados e a fatos, a educação deve permitir que todos possam recolher, selecionar, ordenar, gerir e utilizar as mesmas informações. Nestas condições, a educação deve, pois, adaptar-se constantemente a estas transformações da sociedade, sem deixar de transmitir as aquisições, os saberes básicos frutos da experiência humana. (DELORS, 1996, p. 20).

Os processos de desenvolvimento através dos sistemas de informação atingem toda a sociedade, sendo assim, todos inclusive as instituições de ensino tendem a se encaixar no modelo proposto para que se mantenham em um ambiente competitivo e seguro do mercado educacional.

2.2 Vulnerabilidades físicas e lógicas nos sistemas de informação das instituições de ensino fundamentais

Não existe ambiente totalmente seguro. Independentemente de todo o aparato tecnológico, sempre haverá o elemento humano. As melhores ferramentas até então conhecidas podem ter sido aplicadas, mas nem todas as vulnerabilidades são conhecidas em um momento específico no tempo. As vulnerabilidades são pontos em que o sistema é susceptível a ataques. Consideramos aqui também, além das fragilidades do sistema, erros que nele existam. A identificação das vulnerabilidades técnicas nem sempre é trivial, requerendo, em geral, profundo conhecimento de Tecnologia da Informação e de Comu-

nicação.

Os tipos de ameaças e vulnerabilidades irão variar conforme o ambiente interno e externo da organização. A infraestrutura de dados e de comunicação utilizada, a organização dos processos, a cultura de segurança dos usuários, o apoio da direção à política de segurança da informação, a competitividade do mercado, a visibilidade da organização, tudo isso são fatores a serem considerados. Identificar os riscos importa em identificar as ameaças e as vulnerabilidades que podem ser aproveitadas por estas aos sistemas de informação envolvidos e o impacto que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

Sabemos que as informações dentro de um sistema de redes interno de uma instituição de ensino são sensíveis e estão vulneráveis a ataques hacker, por isso as medidas de segurança são tão importantes, visando a proteção de dados por meios de segurança físicos e lógicos, evitando assim prejuízos.

A informática sempre foi vista como ferramenta de melhoria. Porém, quando se fala em Segurança da Informação, alguns aspectos são vistos de forma negativa no processo, tais como aumento de custos, perda de liberdade, aumento de complexidade, perda de desempenho etc. É primordial que haja medição e controle da eficiência e da eficácia dos serviços de tecnologia da informação. Também não se pode deixar de lado a otimização dos custos na obtenção do resultado final. Contudo não se pode negar que de fato a proteção dos ativos informacionais custa dinheiro e que a segurança naturalmente traz restrições (FREITAS, 2009, p.17 e 18).

Segundo Spanceski (2004), planejar uma segurança eficaz em um sistema de rede, não é uma tarefa fácil, pois envolve um conjunto de conhecimentos de segurança, ambiente de rede, organização, cultura, pessoas e tecnologia, sendo uma tarefa muito trabalhosa, onde envolve muitas pessoas de diferentes funções, que vai de um chefe executivo até uma recepcionista, no entanto, a maior dificuldade será em fazer cumprir essa política criada, todos os funcionários devem entender a política, as regras e procedimentos que são estabelecidos para que todos os funcionários a cumpram de fato.

O planejamento da política deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. A política de segurança pode ser dividida em vários níveis, podendo ser de um nível mais genérico, como o objetivo que os executivos possam entender o que está sendo definido, nível dos usuários de maneira que eles tenham consciência de seus papéis para a manutenção da segurança na organização, e podendo ser de nível técnico que se refere aos procedimentos específicos como, por exemplo, a implementação das regras de filtragem do firewall (SPANCESKI, 2004, p. 34 e 35).

A segurança física é feita internamente na instituição de ensino e leva em consideração a prevenção de danos a equipamentos e invasão à ativos da infraestrutura de redes e que devem ser protegidos e monitorados. Por isso é tão importante estar sempre atento aos problemas de acesso, infraestrutura predial, elétrica e monitoramento de maquinário, principalmente em data centers, onde as informações mais trafegam, e onde estão localizados os servidores de arquivos, informações sensíveis e backups da instituição de ensino.

A segurança lógica tem como objetivo a forma como um sistema é protegido por regras ou softwares para controle de acesso. Normalmente é utilizada para proteção de ataques e vulnerabilidades também servindo para proteger sistemas de erros não intencionais e a remoção acidental de dados. Para isso são implementados processos tecnológicos como firewalls, antivírus, políticas de segurança e controle de usuários, entre outros necessários para proteção dos dados.

2.3 Melhorias em sistemas físicos e lógicos nas instituições de ensino

As instituições de ensino, são ambientes com muita demanda de rede e precisam ser protegidas, pois contam com centenas de alunos e professores que precisam acessar de forma segura a rede de onde quer que estejam.

Fazer uma boa integração de sistemas é um grande passo para aumentar a eficiência operacional e a performance da instituição de ensino. Com ela você economiza tempo, reduz gastos, integra os setores e protege seus dados, diminuindo a chance de erros ou infrações às leis, além de melhorar o desempenho de todos os setores e o fluxo de informações entre eles.

Felizmente, há diversas ações e ferramentas que podem ajudar a mitigar os riscos online para instituições de ensino:

- Concentrar esforços no treinamento da equipe nos princípios básicos de segurança cibernética e garantir que todos entendam a necessidade de manter determinados protocolos para a proteção de dados;
- Nomear um gerente de segurança cibernética com o objetivo de garantir a manutenção de boas práticas, com auditorias regulares e um processo de notificação para sinalizar problemas ou violações em potencial;
- Instalar uma solução de segurança unificada que proteja ambientes, usuários e dispositivos, seja fácil de implementar e usar, bem como evite ataques em potencial em todos os estágios;
- Criptografar e fazer o backup dos sistemas para garantir a recuperação de dados caso haja uma violação cibernética;
- Configurar redes Wi-Fi seguras com VPN para todas as conexões com a Internet.

A digitalização da educação traz diversas vantagens, mas elas podem ser ameaçadas por uma segurança cibernética precária. O treinamento nessa área é importante, assim como a implementação por gerentes de TI de novas soluções que protejam os usuários e permitam que eles aproveitem todas as oportunidades oferecidas pela tecnologia.

Os resultados são significativos para a administração da escola em geral, porém vão muito além disso, sendo percebidos também por alunos e responsáveis, trazendo benefícios para a reputação da sua instituição, que se torna destaque no mercado educacional.

3. METODOLOGIA

Para realizar este trabalho, foi utilizada a metodologia de revisão bibliográfica sistemática. Foram utilizadas as bases de dados eletrônicas Scopus, Web of Science e IEEE Xplore para a busca dos estudos relevantes para o tema proposto. Os descritores utilizados na busca foram “segurança de rede”, “instituições de ensino fundamental”, “malware”, “phishing” e “DoS”.

Os critérios de inclusão para os estudos foram: abordagem da segurança de redes de internet em instituições de ensino fundamental, discussão sobre as principais ameaças cibernéticas e medidas de segurança adotadas. Os critérios de exclusão foram: estudos com metodologia inadequada ou pouco confiável, estudos com enfoque em outras áreas além da segurança de redes em instituições de ensino fundamental. Foram selecionados 15 estudos para a revisão sistemática. A análise dos estudos foi realizada por meio de leitura dos resumos e do texto completo. Utilizaremos alguns autores como DELORS, FREI-

TAS, SPANCESKI, entre outros. As palavras-chave utilizadas serão: segurança cibernética, LGPD, gestão de redes etc.

4. RESULTADOS E DISCUSSÃO

O gerenciamento de redes em instituições de ensino fundamental é um tema crucial para garantir a efetividade e a segurança das atividades educacionais. A gestão eficiente da infraestrutura de rede é fundamental para garantir o acesso à internet e a outros recursos digitais, o que é essencial para o aprendizado e desenvolvimento dos alunos.

Segundo diversos estudos, o gerenciamento de redes em instituições de ensino pode ser desafiador devido à grande quantidade de usuários e dispositivos conectados, especialmente por conta do avanço das tecnologias e a adoção de dispositivos móveis e internet das coisas. Além disso, a necessidade de garantir a segurança da rede e a privacidade dos dados dos alunos pode aumentar ainda mais a complexidade desse gerenciamento, a Instituição de Ensino deve estar sempre atenta às mudanças no cenário tecnológico e se adaptar rapidamente a elas.

Uma rede mal gerenciada pode resultar em uma série de problemas, como baixa performance, interrupções de serviços, falhas de segurança, dentre outros. Por outro lado, um gerenciamento eficiente pode garantir uma rede mais segura, eficiente e confiável, o que impacta diretamente na produtividade e na qualidade dos serviços prestados pela Instituição de Ensino.

Pileggi et al. (2018) avaliou o uso da internet em escolas de ensino fundamental e médio no Brasil. Os resultados mostraram que a maioria das escolas possuía acesso à internet, mas que a velocidade de conexão era baixa. Além disso, a maioria das escolas não possuía políticas de segurança da informação bem definidas, o que pode aumentar o risco de ataques cibernéticos e vazamento de informações.

Yu et al. (2020) analisou o uso da tecnologia na educação em escolas de ensino fundamental na China. Os resultados mostraram que a infraestrutura de TI das escolas era adequada, mas que havia uma necessidade de melhorar a gestão de TI e a formação dos professores para melhorar o uso da tecnologia em sala de aula.

Os resultados da revisão sistemática indicam que as instituições de ensino fundamental estão expostas a várias ameaças cibernéticas, como malware, phishing e ataques DoS. Essas ameaças podem comprometer a integridade dos dados confidenciais, bem como interromper as atividades acadêmicas da instituição.

Os estudos selecionados apontam que as instituições de ensino fundamental adotam medidas de segurança, como firewalls, sistemas de detecção de intrusão e antivírus atualizados, para prevenir essas ameaças. No entanto, tais medidas não são suficientes, pois a segurança cibernética depende também de políticas de segurança e treinamento dos usuários. Os usuários devem ser treinados para entender as políticas de segurança da Instituição de Ensino e como usá-las. O treinamento pode ser realizado por meio de workshops, manuais ou apresentações, esses processos ajudam a garantir que as informações sobre a segurança da rede sejam repassadas de maneira clara e objetiva, aumentando a conscientização e a segurança da rede.

Os estudos também indicam que uma medida adicional que pode ser adotada é a autenticação multifator, que exige mais de um método de confirmação de identidade, como uma senha e um código enviado por mensagem de texto. A autenticação multifator aumenta a segurança do acesso à rede, pois dificulta o acesso por pessoas não autorizadas.

Um estudo realizado por Pinto et al. (2019) mostrou que o gerenciamento de redes em instituições de ensino fundamental é crítico para garantir a qualidade do ensino e aprendizagem. O estudo destacou a importância do monitoramento e gerenciamento contínuos da rede, para garantir a disponibilidade dos recursos de TI e a prevenção de problemas técnicos. Além disso, o estudo ressaltou a importância da implementação de políticas de segurança da informação para proteger os dados pessoais dos estudantes e funcionários da instituição.

Além disso, um estudo realizado por Reis et al. (2021) destacou a importância do treinamento e capacitação dos profissionais de TI responsáveis pelo gerenciamento de redes nas instituições de ensino fundamental. O estudo mostrou que a capacitação dos profissionais é fundamental para o sucesso do gerenciamento de redes, pois permite o desenvolvimento de habilidades técnicas e gerenciais necessárias para garantir a disponibilidade e segurança dos recursos de TI.

É essencial que a equipe de TI responsável pelo gerenciamento da rede esteja sempre atualizada em relação às tecnologias e tendências de segurança da informação, para garantir a proteção dos dados dos alunos e a continuidade das atividades educacionais.

Outro estudo realizado por Silva et al. (2020) destacou a importância do uso de ferramentas de gerenciamento de redes, como softwares de monitoramento de tráfego e de gestão de ativos, para facilitar o trabalho dos administradores de redes nas instituições de ensino fundamental. O estudo mostrou que essas ferramentas permitem o acompanhamento em tempo real do tráfego de dados na rede, a identificação de possíveis problemas e a gestão eficiente dos ativos de TI.

Para gerenciar efetivamente a rede em instituições de ensino fundamental, é importante implementar políticas de segurança da informação, como firewalls, antivírus e filtros de conteúdo, além de garantir que todos os dispositivos conectados à rede estejam atualizados e seguros. Também é importante garantir que a infraestrutura de rede esteja em boas condições e que haja um sistema eficiente de gerenciamento de incidentes para lidar com problemas na rede de forma rápida e eficaz.

Uma das principais questões envolvendo o gerenciamento de redes é a necessidade de manter um equilíbrio entre a segurança e a disponibilidade da rede. De um lado, é necessário garantir que a rede seja protegida contra ameaças e ataques cibernéticos. De outro, é importante que a rede esteja sempre disponível para os usuários, evitando interrupções e perda de dados.

Para encontrar problemas na rede de forma rápida e resolvê-los é importante documentar toda a infraestrutura de rede, incluindo informações sobre os dispositivos, servidores, cabos, switches, roteadores, entre outros. Essa documentação deve ser atualizada periodicamente para garantir que todas as informações estejam corretas e atualizadas. Uma vez que todas as informações estejam atualizadas encontrar o problema será mais fácil, pois o caminho estará completo pela documentação, bastando apenas segui-lo, funcionando também para planejar futuras expansões e atualizações na rede. É fundamental também implementar um sistema de múltiplos backups de dados para garantir a recuperação dos dados em caso de perda ou corrupção. Os backups devem ser realizados periodicamente e armazenados em locais seguros.

A segurança de redes de internet em instituições de ensino fundamental é um tema que merece atenção especial pois é um tema crítico para o sucesso do aprendizado e desenvolvimento dos alunos e que também depende de uma infraestrutura de TI para suas atividades. É necessário implementar medidas de segurança eficazes para proteger as redes contra as ameaças cibernéticas mais comuns, além de promover a conscientização

dos usuários sobre a importância da segurança cibernética e a adoção de boas práticas de segurança, garantindo também que a equipe de TI esteja sempre atualizada em relação às tecnologias e tendências de segurança da informação.

5. CONCLUSÃO

Ao longo deste trabalho, foi possível constatar que o gerenciamento de redes é fundamental para garantir a qualidade do ensino e aprendizagem. O uso adequado de ferramentas de gerenciamento de redes permite que a instituição monitore continuamente a disponibilidade e desempenho dos recursos de TI, bem como identifique e resolva problemas rapidamente.

Ignorar os riscos não os faz deixar de existir. A informação é um ativo da organização cuja segurança deve fazer parte de sua gestão. Cada vez mais as instituições de ensino se tornam dependentes das informações contidas em Sistemas de Informação, mas acabam se esquecendo que equipamentos também estão sujeitos a falhas e deve haver um planejamento para a continuidade do negócio. O valor da informação, a competitividade da empresa, o alinhamento estratégico, irão atuar de forma integrada na justificativa ou não do investimento em segurança da informação.

A gestão de riscos em Sistemas de Informação tem a missão de fazer com que os riscos não venham superar aquele que a alta direção está disposta a correr. Os riscos dependem do contexto e envolvem pessoas, processos e tecnologia. As melhores práticas devem ser aplicadas a toda a organização e a manutenção das políticas de segurança devem contar com o apoio da alta direção.

Em conclusão, o gerenciamento de redes em instituições de ensino fundamental é uma tarefa crítica que exige monitoramento contínuo, implementação de políticas de segurança da informação, uso de ferramentas de gerenciamento de redes e capacitação dos profissionais de TI. A implementação dessas práticas pode garantir a disponibilidade e segurança dos recursos de TI nas instituições de ensino, contribuindo para a qualidade do ensino e aprendizagem.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ARAÚJO, Márcio Tadeu de; FERREIRA, Fernando Nicolau Freitas. Política de Segurança da Informação: Guia Prático para Elaboração e Implementação. Rio de Janeiro: Ciência Moderna, 2008.

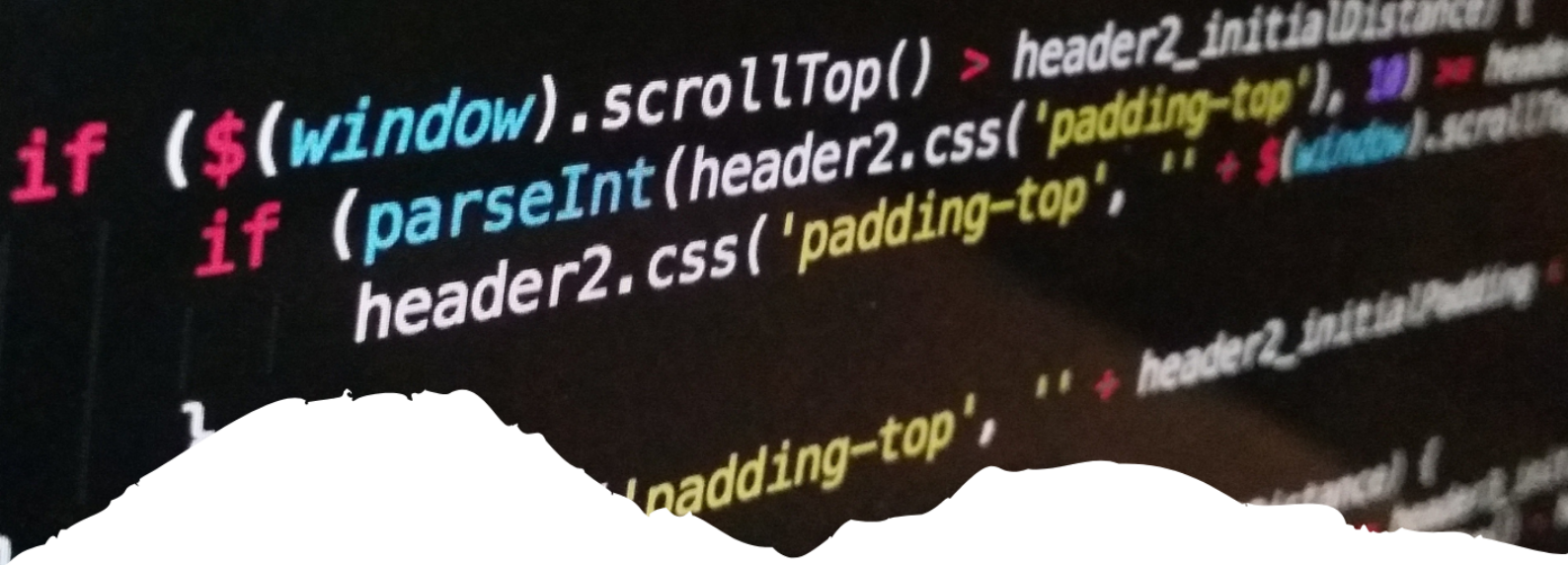
ABNT. Tecnologia da informação – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799). Rio de Janeiro, RJ: 2001

FONTES, Edison Luiz Gonçalves. Praticando a Segurança da Informação. Rio de Janeiro: Brasport, 2008.

Janssen, K., & Moen, J. (2016). **School information security: A qualitative case study. International Journal of Information Management,** 36(6), 1033-1043.

Kim, K., & Bae, S. (2019). **A security framework for K-12 school information systems. International Journal of Information Security,** 18(1), 1-16.

Saran, D., & Mathur, A. P. (2018). **Information security management in educational institutions. International Journal of Information Security,** 17(6), 669-684.



14

UM ESTUDO SOBRE AS EVOLUÇÕES TECNOLÓGICAS DE INTELIGÊNCIA ARTIFICIAL NO SETOR EMPRESARIAL

A STUDY ON THE TECHNOLOGICAL EVOLUTION OF ARTIFICIAL INTELLIGENCE IN THE BUSINESS SECTOR

Iago Emanuel Fernandes Moreira

Resumo

A interação entre humanos e máquinas nas empresas possibilita o trabalho humano a humano por meio do uso de técnicas cognitivas de aprendizado de máquina, denominada Inteligência Artificial. Diante disso, essa pesquisa buscou investigar a importância do uso de inteligência artificial no setor empresarial. Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Para tanto, buscou-se auxílio em livros, revistas e artigos das bases de dados Google Acadêmico e Sciello, que pudessem oferecer referenciais teóricos condizentes com o tema apresentado. Constatou-se que a Inteligência Artificial é considerada um avanço tecnológico que possibilita a sistemas a simulação de uma inteligência similar à humana, ultrapassando a programação de ordens específicas para a tomada autônoma de decisões, fundamentadas em padrões de grandes bancos de dados. Observou-se que a Indústria 4.0 tem como principal objetivo proporcionar uma completa descentralização do controle da produção e o aprimoramento da manufatura através da disseminação do uso de novas tecnologias interligadas ao longo de todo o processo produtivo. Além disso, verificou-se que existem muitos exemplos de aplicações de IA, como veículos autônomos, diagnóstico médico, desenvolvimento de arte, teoremas matemáticos, jogos, mecanismos de busca, assistentes online, reconhecimento de imagem, filtragem de spam, julgamentos e marketing online. Dessa forma, pode-se perceber que a IA possui inúmeras aplicações na sociedade.

Palavras-chave: Inteligência Artificial. Empresas. Aplicação.

Abstract

The interaction between humans and machines in companies enables human-to-human work through the use of cognitive machine learning techniques, called Artificial Intelligence. Therefore, this research sought to investigate the importance of using artificial intelligence in the business sector. To carry out this work, the methodology used was a Bibliographic Review Survey. To this end, help was sought in books, magazines and articles from the Google Scholar and Sciello databases, which could offer theoretical references consistent with the theme presented. It was found that Artificial Intelligence is considered a technological advance that enables systems to simulate an intelligence similar to that of humans, surpassing the programming of specific orders for autonomous decision-making, based on patterns of large databases. It was observed that Industry 4.0 has as its main objective to provide a complete decentralization of production control and the improvement of manufacturing through the dissemination of the use of new interconnected technologies throughout the entire production process. In addition, it was found that there are many examples of AI applications, such as autonomous vehicles, medical diagnosis, art development, mathematical theorems, games, search engines, online assistants, image recognition, spam filtering, judgments and online marketing.Thus, it can be seen that AI has numerous applications in society.

Keywords: Artificial Intelligence. Companies. Application.

1. INTRODUÇÃO

As origens da inteligência artificial são atribuídas ao matemático britânico Alan Turing, o fornecedor da criação de máquinas capazes de decodificar informações. Dessa forma, a inteligência artificial é entendida como o termo representado por um conjunto de software, lógica e computação capaz de criar sistemas capazes de realizar atividades próximas à inteligência humana.

Ao longo dos anos, as empresas têm crescido cada vez mais forte no mercado de trabalho. Nesse caso, a tecnologia passa a fazer parte da unidade de negócios, empregando sistemas automatizados. A partir dessa evolução, as empresas mudaram suas estratégias de negócios, buscando investir mais no uso da tecnologia aplicando a inteligência artificial.

O conceito de Inteligência Artificial vem crescendo gradativamente com o avanço da tecnologia e suas atribuições são importantes em diversas áreas. Nesse contexto, essa pesquisa se tornará relevante, pois ela irá investigar e identificar quais as tecnologias de Inteligência Artificial são utilizadas no crescimento e desenvolvimento das empresas. Com isso, essa investigação trará uma grande contribuição para o âmbito acadêmico e social, sendo mais específico para o setor empresarial o qual mostrará as mudanças e evoluções que as empresas tiveram que fazer para se desenvolverem e se adaptarem, enquanto na esfera acadêmica, será utilizado por alunos e professores, servindo como fonte de estudos.

A interação entre humanos e máquinas nas empresas possibilita o trabalho humano a humano por meio do uso de técnicas cognitivas de aprendizado de máquina. Da mesma forma, modelos de aprendizado de máquina de última geração são aplicados a robôs inteligentes capazes de aprender como humanos e desenvolver habilidades complementares em diferentes ambientes operacionais. Diante disso, questiona-se: qual a importância do uso de inteligência artificial no setor empresarial?

O principal objetivo dessa pesquisa foi investigar a importância do uso de inteligência artificial no setor empresarial. Especificamente, buscou-se: entender os conceitos de Inteligência Artificial; conhecer o conceito de Indústria 4.0 e Internet das Coisas; identificar as tecnologias de Inteligência Artificial utilizadas para aprimorar ou ajudar no crescimento e desenvolvimento das empresas;

Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Para tanto, buscou-se auxílio em livros, revistas e artigos das bases de dados Google Acadêmico e Sciello, que pudessem oferecer referenciais teóricos condizentes com o tema apresentando, dando subsídio para a construção do trabalho. Foram utilizados os materiais acadêmicos publicados nos últimos cinco anos (2017 a 2022). As palavras-chaves na utilizadas na pesquisa foram: Inteligência Artificial; Computação; Empresas.

2. INTELIGÊNCIA ARTIFICIAL

“O artificial é o que não é natural, feito para imitar a natureza produzido de forma artística ou industrial”. O conceito de Inteligência Artificial teve origem após a Segunda Guerra Mundial, período em que ocorreu uma demanda da criação de máquinas que fizessem e pensassem como seres humanos e, atualmente, abrange uma enorme variedade de subcampos, desde áreas de uso geral, como aquisição de conhecimentos, até tarefas bem específicas, como a resolução de cálculos matemáticos complexos (MAKSYM, 2021).

Segundo Doneda et al. (2018), em termos históricos, aborda que a Inteligência Artificial tem seguido quatro linhas de pensamento distintas:

> I. Sistemas que pensam como humanos: “O novo e interessante esforço para fazer os sistemas pensarem como mentes, no sentido total e literal”;
>
> II. Sistemas que funcionam como humanos: “A arte de criar sistemas que executam funções que exigem inteligência quando executadas por pessoas”;
>
> III. O sistema de pensamento racional: “O estudo das faculdades mentais pelo seu uso de modelos computacionais”;
>
> IV. E sistemas que agem racionalmente: “A inteligência computacional é o estudo do projeto de agentes inteligentes”;

As linhas I e III referem-se a processos de pensamento e raciocínio, enquanto as linhas II e IV referem-se ao comportamento. Vale ressaltar que os pensamentos I e II medem os componentes do sucesso em termos de desempenho humano, enquanto os pensamentos III e IV medem o sucesso em termos de racionalidade.

De acordo com algumas correntes de pensamento, a Inteligência Artificial possui diversas definições, pois, para muitos pensadores, o que a define são os modos de funções específicas adquiras e desenvolvidas por ela quando a inteligência está diretamente relacionada à área na qual trabalha-se. Segundo Kaufman (2019), ainda que os artigos e pesquisas científicas sobre Inteligência Artificial sejam abundantes na sociedade e no ambiente da imprensa, é difícil encontrar uma definição sobre o que ela é.

Peixoto e Silva (2019, p.21) definem a Inteligência Artificial como “o esforço para automatizar tarefas normalmente performadas por humanos”. Desse modo, por meio da criação de algoritmos, uma unidade computacional torna-se capaz de desempenhar funções para a qual foi programada.

A Inteligência Artificial é considerada um avanço tecnológico que possibilita a sistemas a simulação de uma inteligência similar à humana, ultrapassando a programação de ordens específicas para a tomada autônoma de decisões, fundamentadas em padrões de grandes bancos de dados (TRENTO, 2021). Corroborando com essa afirmação, Fava (2018) destaca que a Inteligência Artificial é, grosso modo, a capacidade das máquinas de pensarem como seres humanos (capacidade de aprendizado, percepção e decisão) de modo racional. Até então, os computadores necessitavam de três fatores básicos para a evolução do modelo simples para o atual da computação, sendo eles:

- Bons modelos de dados para a classificação, processamento e análise;
- Acesso a um grande volume de dados não processados;
- Computação de boa potência e custo acessível, que fosse capaz de processar dados de forma eficiente e rápida.

Com a evolução desses três elementos, a IA tornou-se viável e possível, por meio do trinômio: big data, computação em nuvem e bons modelos de dados. Essencialmente, ela permite que os sistemas tomem decisões de modo independente, eficaz e baseada em dados digitais. Isso acaba multiplicando a capacidade racional do ser humano de resolver problemas práticos, simular contextos e situações, bem como pensar e elaborar respostas, ampliando a sua capacidade de ser inteligente (GARCIA, 2020).

Acerca desse conceito, Oliveira (2019) ressalta que:

> A IA tem se destacado na busca por compreender a inteligência por englobar diversos campos do conhecimento com o objetivo prático de simular a inteligência. Ela tem se mostrado um campo de estudo multidisciplinar e interdisciplinar, que se apoia no conhecimento e evolução de outras áreas do conhecimento. Mas a inteligência artificial se desenvolveu principalmente graças a aparição da informática, por isso ela é mais confundida com seu aspecto informático. A IA fornece métodos e técnicas para o desenvolvimento de programas que simulam nas máquinas comportamentos inteligentes, isto torna os computadores capazes de pensar e tomar decisões. Por isso, as técnicas de IA necessitam de uma grande quantidade de conhecimentos e de mecanismos de manipulação de símbolos. Esses conhecimentos devem ter a possibilidade de representação, modificação e ampliação (OLIVEIRA, 2019, p.21).

Entretanto, conforme expõe Ludermir (2021), a abordagem algorítmica decompõe a inteligência artificial (IA) em dois grupos distintos: a IA tradicional e o aprendizado de máquina. Sendo assim, a grande diferença entre essas duas classificações consiste em sua lógica. Na Inteligência Artificial normal as regras e os dados de entrada são disponibilizados para uma unidade computacional, que retorna para uma saída. Já na Inteligência Artificial baseada em aprendizado de máquina, são fornecidos tanto os dados de entrada como os de saída, o que faz com que a unidade computacional, por meio de algoritmos, gere o conjunto de regras que estabelece relações entre a saída e a entrada. Nesse caso, após alcançar as regras, o algoritmo prevê as saídas associadas aos novos dados que são inseridos.

A Figura 1 apresenta a diferença de paradigma entre as subclassificações da inteligência artificial, que recebe os dados rotulados, e o algoritmo de aprendizado de máquina, que identifica as regras responsáveis por mapear a conexão entre esses dados.

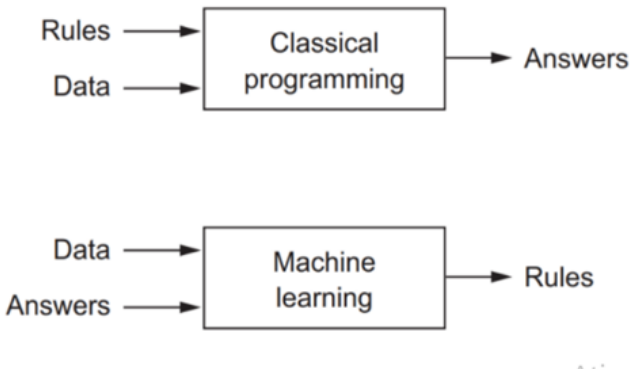


Figura 1 - Subclassificações da Inteligência Artificial

Fonte: Ludermir (2021).

Inserido no conjunto de aprendizado de máquina está o subcampo “aprendizagem profunda”. De acordo com Kaufman e Santaella (2020), o aprofundamento dentro do grupo de inteligência artificial traz consigo conjuntos que resolvem problemas complexos, como é o caso deste. O autor destaca ainda que o algoritmo de aprendizado da máquina é considerado um dos melhores, enquanto a aprendizagem profunda apresenta a especialidade de trabalhar com dados não-perceptuais, desempenhando tarefas costumeiras para o homem. A Figura 2 apresenta um diagrama demonstrando os subgrupos da inteligência artificial, até chegar em aprendizagem profundo (deep learning).

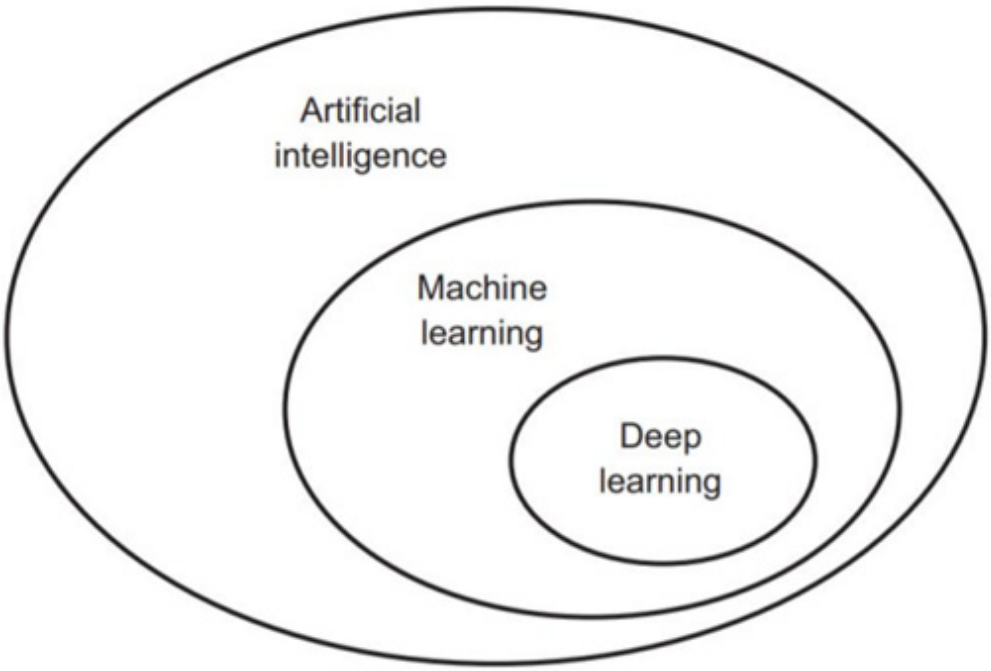


Figura 2 - Subgrupos da IA

Fonte: Ludermir (2021).

Existem dois fatores que justificam o fato de a aprendizagem profunda ser mais robusta do que o conjunto que se encontra, o que faz com que esse tipo de algoritmo seja capaz de desempenhar tarefas mais complexas, no campo computacional, sendo eles: a representação e a profundidade. A respeito disso, Oliveira (2019, p.22) ressalta que:

Representação: o algoritmo é capaz de criar suas próprias representações dos dados, encontrando padrões entre eles sem a ajuda de um especialista. No aprendizado de máquina, a maior parte do tempo de um engenheiro de modelo consiste em estruturar os dados para o treino do modelo; a qualidade dos dados é tão importante quanto o modelo em si. Já em deep learning, o próprio algoritmo encontra representações do modelo, que muitas vezes está fora da compreensão do especialista por trás do modelo, fazendo com que o desenvolvedor passe mais tempo otimizando o modelo, e não os dados os quais serão inseridos.

Profundidade: o outro fator para a robustez do modelo é o número de camadas que o modelo pode ter, fazendo com que o modelo tenha uma quantidade enorme de parâmetros, que se ajustam de forma mais precisa aos dados. A sequência de camadas também possui uma lógica: as camadas do início do modelo extraem dos dados atributos mais simples, e à medida que avança na corrente de camadas, os atributos extraídos pelo modelo possuem mais complexidade.

de paradigmas dentro da inteligência artificial leva os profissionais envolvidos no desenvolvimento de modelos a dedicarem mais tempo para a criação e melhoria do modelo em si, em vez de passar seu tempo trabalhando com os dados, por meio de suas próprias habilidades, com o intuito de inserir no modelo dados de alta qualidade. Além disso, os dados podem oferecer ao modelo representações que não pertencem à ciência atualmente, podendo assim, superar o desempenho do homem (AIRES; ALMEIDA; SILVEIRA, 2019).

A Figura 3 apresenta a diferença dos conjuntos dentro do conceito de Inteligência Artificial, no que se refere às relações extraídas pelo modelo. O modelo básico de regras desenvolvidas pelo homem recebe os dados, perpassa pelo modelo e retorna uma saída.

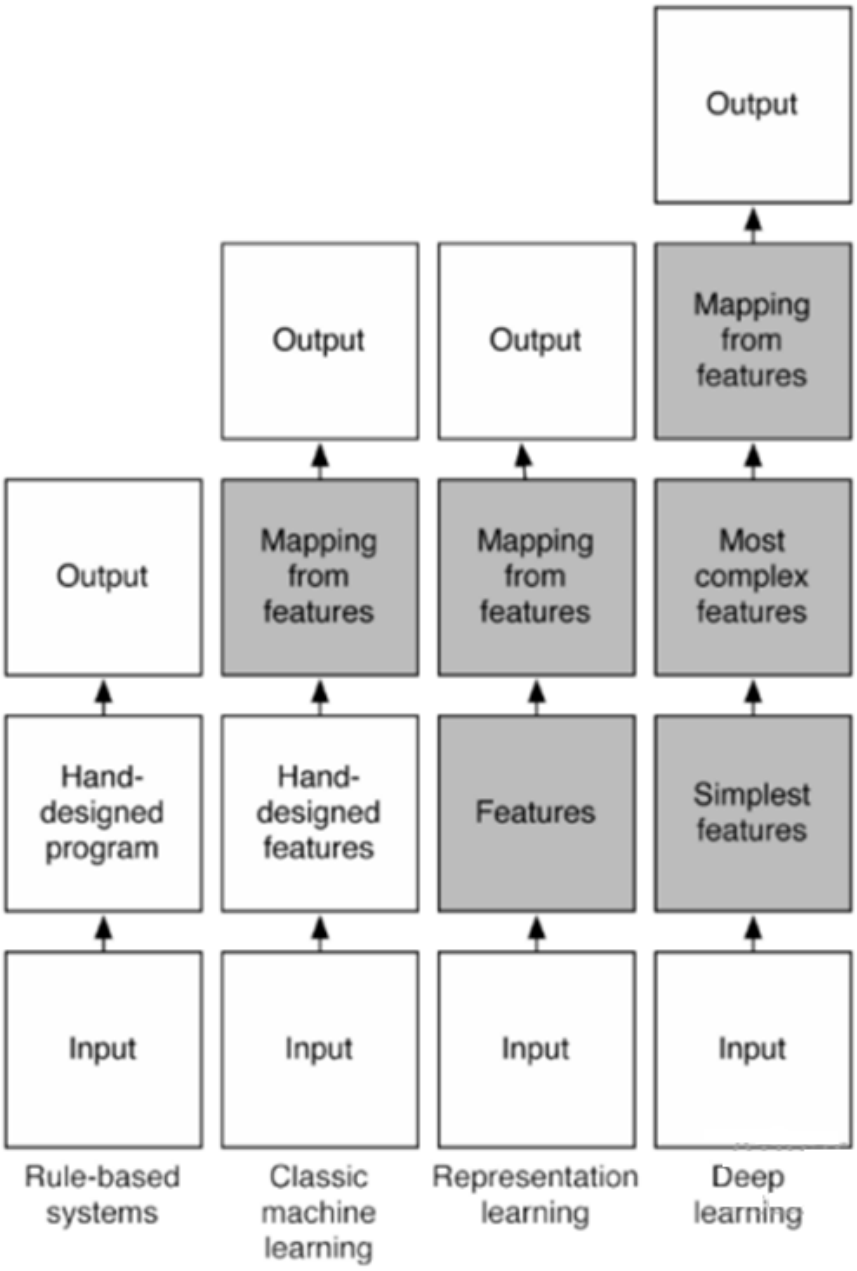


Figura 3- Diferença dos conjuntos na IA

Fonte: Ludemir (2021).

Somente com a evolução das placas gráficas, baseada nos avanços da indústria de jogos eletrônicos, é que ocorreram os principais avanços dentro da Inteligência Artificial. Ressalta-se que essas placas possuem a capacidade de executar paralelamente cálculos, ao contrário das unidades de processadores, que não possuem essa habilidade, exigindo que um cálculo seja finalizado para que se realize outro. Esse aspecto permite a criação de modelos complexos, robustos e com diversas camadas de desenvolvimento superior aos modelos de aprendizado (AGRAWAL; GANS; GOLDFARB, 2020).

3. A INDÚSTRIA 4.0 E A INTERNET DAS COISAS

A globalização e o desenvolvimento tecnológico trouxeram consigo diversas consequências para o setor industrial. Uma delas é o surgimento de processos industriais com

melhor desempenho e máquinas mais modernas e eficientes. Nesse contexto, a Indústria 4.0 surge como um novo conceito de indústria que engloba as principais inovações tecnológicas nos campos da Tecnologia da Informação e da Engenharia aplicadas à manufatura (YUNGAY, 2017).

A Indústria 4.0 tem como principal objetivo proporcionar uma completa descentralização do controle da produção e o aprimoramento da manufatura através da disseminação do uso de novas tecnologias interligadas ao longo de todo o processo produtivo. O termo Indústria 4.0 pode ser utilizado para identificar o uso das principais inovações tecnológicas dos campos de automação, controle e tecnologia da informação, aplicadas aos processos de manufatura. A utilização dos recursos tecnológicos inovadores possibilita, assim, a otimização, a eficiência e o melhor desempenho do processo produtivo (SANTOS et al., 2017).

De acordo com Marcuzzo, Santos e Siluk (2017, p. 2017), o termo Indústria 4.0 tornou-se popular em 2011, quando uma companhia de representantes do governo, organizações e academia promoveu a ideia de uma abordagem com o intuito de aperfeiçoar a competitividade da indústria alemã. Assim, o governo alemão deu suporte à iniciativa e declarou que a Indústria 4.0 seria parte do projeto High-Tech Strategy 2020 for Germany, com o objetivo de levar a Alemanha à liderança na inovação tecnológica.

Conforme destaca Tigre (2018, p. 9), recursos inovadores como os Sistemas Cyber-Físicos (tradução de Cyber Physical Systems – CPS), Internet das Coisas e Internet dos Serviços possibilitam que os processos industriais e produtivos possuam maior eficiência, autonomia e melhores custos. Assim, a Indústria 4.0 vem representar um novo período no contexto das grandes revoluções industriais, com impactos diretos em diversos setores do mercado e que proporcionam o crescimento de diferentes setores da economia.

Nobre (2017) ressalta que as empresas deverão introduzir redes globais, que incorporem suas máquinas, sistemas de armazenagem e instalações de produção na forma de Sistemas Físico-Cibernéticos. Os CPS propõem a integração de mundos físicos e virtuais para suportar todas essas exigências e capacidades, de forma a incorporar os elementos computacionais em entidades físicas e conectar essas entidades em uma infraestrutura baseada em nuvem, com a finalidade de proporcionar uma gestão mais eficaz do ambiente físico e seus processos.

O autor Amorim (2017) destaca que as melhorias na gestão das organizações serão observadas, visto que cada sistema será capaz de compreender suas especificações e se comunicar com outros sistemas. Isso possibilitará rápidas tomadas de decisão e respostas autônomas dos sistemas de produção, além de uma cooperação mais estreita entre parceiros de negócios (por exemplo, fornecedores e clientes) e entre funcionários, a fim de promover novas oportunidades para benefício mútuo.

A implementação da visão da Indústria 4.0 permitirá aos funcionários monitorar, orientar e configurar redes de recursos de produção inteligente e estágios de fabricação com base em situações e contextos alvos. Os funcionários serão liberados de ter que realizar atividades rotineiras, o que lhes permite que foquem em tarefas criativas e de valor agregado. Dessa forma eles manterão uma função essencial, especialmente em termos de garantia de qualidade. Simultaneamente, condições de trabalho flexíveis possibilitarão uma maior compatibilidade entre seus trabalhos e suas necessidades pessoais (RUFONI; SUZIGAN, 2020).

Segundo Christensen (2019, p.14) a abordagem sociotécnica da Indústria 4.0 disponibilizará novos potenciais para o desenvolvimento de inovações urgentemente necessárias, baseada em uma maior conscientização a respeito da importância do trabalho humano

no processo de inovação. O autor menciona ainda que, destacam-se como os pilares da Indústria 4.0: interoperabilidade, virtualização, descentralização, capacidade em tempo real e orientação a serviço.

A interoperabilidade possibilita que os transportadores de peças, estação de montagem e produtos – CPS comuniquem-se com os indivíduos e as fábricas inteligentes por meio da Internet das Coisas e da Internet. Através da virtualização, os CPS podem monitorar a execução dos processos físicos. Por meio da descentralização, o controle dos sistemas ocorre de forma facilitada e em tempo real e de forma instantânea (capacidade em tempo real). Com a orientação a serviços, os serviços de empresas, CPS e humanos tornam-se disponíveis na internet e podem ser utilizados por outras pessoas (BERNI; 2019).

A nova onda tecnológica está atingindo todos os âmbitos, principalmente o mercado econômico, onde as indústrias estão na disputa incessante por inovações e avanços tecnológicos para a melhoria da infraestrutura de redes e comunicações. A Internet das Coisas (Internet of Things – IoT) com uma denominação simples, mas com uma estrutura muito ampla, surgiu para facilitar e tornar a infraestrutura tecnológica dinâmica.

Segundo a CERP (Cluster of European Research Projects on the Internet of Things) a IoT é uma infraestrutura de rede global dinâmica, baseada em protocolos de comunicação em que "coisas" físicas e virtuais têm identidades, atributos físicos e personalidades virtuais, utilizando interfaces inteligentes e integradas às redes telemáticas. As coisas/objetos tornam-se capazes de interagir e de comunicar entre si e com o meio ambiente por meio do intercâmbio de dados. As coisas reagem de forma autônoma aos eventos do "mundo real / físico" e podem influenciá-los por processos sem intervenção humana direta. O novo campo da IoT reúne questões técnicas e sociais (RUSSO, 2020).

As transformações tecnológicas estão crescendo gradativamente, a internet excedeu o número de coisas ligadas, estima-se que haja mais de seis objetos conectados por pessoas no mundo. Esse fato mostra que a internet é uma das redes mais utilizadas e considerada um recurso indispensável, seja no ambiente de trabalho ou na vida social (SILVA, 2022).

A internet no seu começo era um pouco diferente de como se conhece atualmente, porém segue ao mesmo conceito, sendo o de uma rede interconectada de computadores para a troca de informações. A partir deste ponto foram formados grupos de estudo e seminários para o desenvolvimento e pesquisa de redes e protocolos, e rapidamente esta tecnologia foi ganhando espaço. Surgiram aplicações para envio de e-mails, o que representou um grande marco na forma de comunicação, entre outras. Desta forma a rede que inicialmente só conectava dois computadores em diferentes estados agora acomodava uma rede global com diversos usuários, marcando desta maneira a internet das máquinas, pois para o uso da internet era estritamente necessário estar conectado a um computador desktop com acesso à internet (PRADO, 2022).

Segundo Bernardo et al. (2022), o termo Internet das Coisas, ou Internet of Things (IoT) em inglês, foi apresentado primeiramente por Kevin Ashton da MIT Auto Centre, em uma apresentação sobre RFID e a cadeia de suprimentos de uma grande companhia, em 1999. Há uma série de situações, ou aplicações, nas quais se pensa em internet das coisas, por exemplo, ambiente inteligente, computação ubíqua, web das coisas, internet do futuro ou cidades inteligentes. Por conta de toda essa variedade, também há uma série de definições para a Internet das Coisas.

A Internet das Coisas possibilita mais comodidades para as pessoas, e esse maior conforto e agilidade podem ser percebidos em diversos setores, principalmente no transporte marítimo. O transporte marítimo é o modal mais utilizado para movimentar cargas em todo o mundo, alguns fatores justificam essa movimentação, como por exemplo, os pre-

ços convidativos e a possibilidade de consolidação de mercadorias.

A história da internet das coisas (IoT), foi marcada por vários fatos importantes que iniciaram nos meados dos anos 90, esse sistema se fez presente em vários estudos, conferências e pesquisas que buscavam por avanços tecnológicos, através dessa interversão a IoT começou a ser entendida, explorada e implantada para melhoria e crescimento das técnicas, organizações e ações humanas (SILVA, 2022).

Atualmente a Internet das Coisas recebe atenção e suporte da Comissão Europeia (CE) por meio do Programa Horizon, o maior programa de Pesquisa e Inovação da União Europeia (EU), com cerca de 80 milhões de euros de financiamento disponíveis ao longo de 7 anos – período de 2014-2020 (PRADO, 2022).

Para Singer (2012) a simples definição de Internet das Coisas enquanto rede mundial de objetos conectados, que trocam informação entre si é muito ampla. Segundo pesquisa da autora, o termo IoT parece bem aceito na Europa, enquanto nos Estados Unidos as pesquisas estão mais concentradas em torno de termos como objetos inteligentes ou computação em nuvem (BIONI; LUCIANO, 2019).

Romero (2019) define Internet das Coisas como a conectividade entre objetos e humanos, outro ponto relevante nesta definição foi a possibilidade de haver Internet das Coisas sem a interação de seres humanos com os objetos. Vale acrescentar que o futuro de Internet das Coisas está ligado ao conceito da tecnologia evoluir a ponto de não precisar haver interações humanas diretas, ou seja deixando os objetos mais inteligentes para interagir com o ambiente em que estão inseridos.

Seguindo este princípio, já para Russo (2020, p.297) a IoT:

> É uma infraestrutura de rede dinâmica e global com capacidades de autoconfiguração, baseada em protocolos de comunicações padronizados e interoperáveis, onde “coisas” físicas e virtuais tem identidades, atributos físicos e personalidades virtuais. Usam interfaces inteligentes bem como são naturalmente integradas à Internet.

A partir disso, é possível entender um pouco melhor a Internet das Coisas. Este tipo de tecnologia pode fazer a diferença, no contexto em que é inserido:

> A Internet das Coisas é um paradigma que tem como objetivo criar uma ponte entre acontecimentos do mundo real e as suas representações no mundo digital. O objetivo é integrar o estado das Coisas que constituem o nosso mundo em aplicações de software, beneficiando do contexto em que estão instaladas (SILVA, 2020, p. 15).

O intuito da IoT é beneficiar o ambiente em que está inserido, pois sua aplicação é bastante vasta e pode ter aplicações em diversas áreas. A Internet das Coisas permite a conexão de um objeto a um ser humano ou um ambiente, o sistema é constituído pelo uso de uma rede com protocolos e sensores, sendo que a rede permite a comunicação do objeto do mundo real com um ser humano ou até mesmo um sistema. É importante ressaltar que o avanço desta tecnologia está atrelado à padronização do desenvolvimento e à evolução na camada de segurança, assim como na padronização a fim de facilitar o desenvolvimento desta tecnologia na comunidade de desenvolvedores e segurança (PINTO, 2020).

A aproximação do sistema IoT apresenta várias vantagens em diversos ramos, seja na área logística, na indústria, transporte e em empresas de pequeno porte, esta tecnologia

é poderosa aliada no crescimento no mercado industrial, pois permite que as decisões sejam tomadas de uma forma imediata e eficiente, identificando falhas, manutenções, prevenções e riscos ao longo do curso (RUSSO, 2020).

4. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL

É importante destacar que devido à crescente expansão dos estudos relacionados à Inteligência Artificial, aumentou-se também sua utilização em diversas áreas, realizando o surgimento de novos negócios e aprimorando os já existentes. Sendo assim, se faz necessário entender as principais utilidades desta tecnologia.

O fato de a inteligência artificial poder ser utilizada em diversas áreas facilita a produção e otimiza o tempo gasto nas tarefas. Além disso, o uso da inteligência artificial traz a solução para um dos maiores problemas da sociedade, a falta de tempo. O uso dessa tecnologia também traz desvantagens para seus criadores, pois por ser ainda recente e em pesquisa, as máquinas que utilizam IA são programadas com conceitos humanos e não evoluem com o tempo quando uma pessoa reprograma a mesma máquina com novas informações. E se a máquina não for adaptada à realidade da população, essa tecnologia pode causar conflitos na sociedade (SANTELLA, 2021).

Embora ainda existam tarefas que exijam automação, sejam distribuídas na natureza, exijam interação entre as partes e sejam diferenciadamente especializadas, o uso de agentes inteligentes é uma boa solução para essas funções. Delegar tais tarefas pode ter efeitos surpreendentes na sociedade, alterando até mesmo a tomada de decisão humana, a negociação e a pesquisa, que as empresas podem usar para aumentar seu poder de barganha com os fornecedores. Existem muitos exemplos de aplicações de IA, como veículos autônomos, diagnóstico médico, desenvolvimento de arte, teoremas matemáticos, jogos, mecanismos de busca, assistentes online, reconhecimento de imagem, filtragem de spam, julgamentos e marketing online (GARCIA, 2021).

A inteligência artificial é um ramo da ciência da computação, mas também é aplicada na psicologia, linguística, biologia, lógica matemática, tecnologia, filosofia, entre outras. As máquinas começaram a processar grandes volumes de dados e relacioná-los com outros dados, de modo que a aplicação da inteligência artificial pode ser dividida em três áreas: aprendizado de máquina, aprendizado profundo e processamento de linguagem natural (COZMAN, 2018).

Segundo Pinto (2020), o aprendizado de máquina possibilita desenvolver sistemas que tenham a capacidade de aprender por si mesmos e aprimorar seus conhecimentos sem programação, o Processamento de Linguagem Natural permite que os computadores processem e infiram informações com base na fala, enquanto o aprendizado profundo é considerado mais difícil.

O domínio porque envolve a percepção e adoção de padrões e padrões comportamentais. Um exemplo de aprendizado de máquina é a detecção de spam. Inicialmente, os e-mails marcados como spam são oferecidos e, a partir daí, o software anti-spam detecta padrões nos e-mails subsequentes e os marca como spam ou não (ROMERO, 2019).

O processamento de linguagem natural pode ser usado para recuperar informações sem digitar comandos ou palavras-chave. Por fim, um exemplo de deep learning é o reconhecimento de imagens do Google Fotos, que possui uma ferramenta que seleciona as melhores fotos e também consegue identificar pessoas, animais e objetos com características comuns (SILVA, 2020).

Pesquisas atuais mostram que inteligência artificial, aprendizado de máquina e aprendizado profundo andam juntos e podem ser classificados em esferas. O aprendizado profundo está no meio. Essa camada inclui aprendizado de máquina e ambos os campos são inteligência artificial. Vale a pena notar que a IA comete erros, mas são mínimos em comparação com a quantidade de dados a interpretar que faz a máquina funcionar de forma eficaz (BIONI; LUCIANO, 2019).

Assim, com base nas opiniões dos autores, é possível entender como a aplicação de inteligência artificial é permitida em diferentes setores, de forma que para cada setor, uma determinada característica de cada campo é utilizada para otimizar a atividade desejada.

Por isso é importante que haja pessoas qualificadas para desenvolver e utilizar essa tecnologia da melhor forma para que possamos continuar nos desenvolvendo como sociedade. Indo em direção à era do espelho negro influenciada pela literatura e pelo cinema, o hype da IA deixou sua marca no gosto popular e cada vez mais entrou também no ambiente de negócios. Nesse cenário, os chamados gigantes da tecnologia – Amazon, Apple, Facebook, Google, IBM, Microsoft, Tesla, Uber, entre outros – enfrentam uma verdadeira competição pelo domínio do mercado, imprevisível pela velocidade dos acontecimentos. Progresso (SILVA, 2020).

Como exemplo, listamos algumas das tecnologias de IA que se destacam atualmente. Nesse sentido, vale ressaltar que um dos primeiros avanços significativos no processamento de linguagem natural (dados não estruturados) ocorreu no desenvolvimento da inteligência artificial IBM Watson, participando do programa Jeopardy. A IBM opera atualmente em vários campos, como publicidade, perfil do consumidor, educação, serviços financeiros, saúde etc. e fornece vários serviços, como software de assistência pessoal, análise de dados não estruturados, dispositivos de reconhecimento visual, uso de idiomas por meio da plataforma IBM Cloud (GARCIA, 2020).

Outra importante plataforma de computação em nuvem é o Azure da Microsoft, que fornece a infraestrutura necessária para o desenvolvimento de negócios junto com ferramentas de produtividade. Dentre os serviços oferecidos destacam-se máquinas virtuais (sistemas operacionais completos com recursos de armazenamento e computação em nuvem) e serviços cognitivos digitais (algoritmos de processamento de imagem, processamento de linguagem natural, reconhecimento de voz, etc.) (LUDERMIR, 2021).

Um exemplo da importância da inteligência artificial voltada para a área da saúde é a inteligência artificial desenvolvida pela Microsoft e implementada no hospital 9 de Julho. Ao usar redes neurais profundas para entender certas cenas, a análise de imagens de pacientes idosos no hospital permitiu que o hospital reduzisse drasticamente as quedas de leitos (GARCIA, 2020).

Em conclusão, podemos dizer que houve um progresso considerável no campo dos transportes com o desenvolvimento de veículos autônomos e energeticamente eficientes. Em 2016, a Tesla Motors, liderada pelo excêntrico Elon Musk, anunciou que todos os carros produzidos a partir desse momento serão equipados com um sistema que pode controlar veículos sem intervenção humana (TENTO, 2021).

No entanto, a tecnologia dos carros autônomos ainda não pode ser totalmente adotada, pois está diretamente relacionada a riscos à saúde e à integridade física das pessoas – que atualmente circulam em um ambiente de trânsito caótico – que devem ser amplamente mitigados antes de sua implantação, pois qualquer erro nessa área pode ser fatal. Resumidamente, alguns exemplos:

a) Vendas e Marketing - A IA analisa todos os dados de navegação dos clientes para

encontrar os melhores produtos para eles. Os sites de compras também fazem isso quando fornecem recomendações e recomendações de produtos (TENTO, 2021).

b) Medicina - a criação de diagnósticos já requer a existência de inteligência artificial e aprendizado de máquina. Ao coletar muitas informações e resultados de varreduras anteriores, a IA pode fazer diagnósticos precisos por conta própria (RUFONI; SUZIGAN, 2020).

c) Assistentes virtuais - Alexa, Siri e Cortana são os clássicos. A IA estar em outros aplicativos como o Google Maps, não apenas para responder às suas perguntas e realizar ações. É o exemplo máximo de inteligência artificial que facilita o dia a dia porque combina diferentes dados para analisar a melhor rota de acordo com as opções de transporte e tempo.

d) Segurança - reconhecimento facial, reconhecimento de voz ou vigilância por câmeras de vigilância. O que antes era feito por inúmeras pessoas por incontáveis horas e sem muita precisão, hoje contamos com a ajuda da inteligência artificial para nos manter seguros (AMORIM, 2017).

e) Cibersegurança - Com o aumento do número de ataques virtuais devido ao crescimento do home office e de um mundo cada vez mais online, surgiu a necessidade do uso de inteligência artificial para proteger nossa segurança no mundo online. A automatização dos processos de segurança da informação, que antes eram responsabilidade das pessoas, passou a ser uma das tarefas da inteligência artificial, que possibilita uma reação imediata, com menor índice de erros, e também libera a equipe de TI da empresa para atividades mais estratégicas (RUFONI; SUZIGAN, 2020).

f) Tráfego - Os sistemas de gestão de tráfego e logística de muitas empresas contam com inteligência artificial para aumentar a eficiência e a segurança. O uso de inteligência artificial permite cálculos complexos para determinar rotas, rotas alternativas e prazos. Isso simplifica, por exemplo, a logística necessária para a entrega e transporte de mercadorias. É ideal para empresas que lidam com produtos perecíveis, como alimentos (ROMERO, 2019).

g) Atendimento - Os chatbots continuam sendo uma das tendências mais importantes no atendimento e relacionamento com o cliente recentemente. Cada vez mais humanos, eles contam com processos de machine learning e deep learning para soar mais naturais e amigáveis, o que facilita o atendimento e o dia a dia dos clientes. Devido ao alto nível de confiança, os chatbots ou bots de voz contêm programação refinada diariamente para entender as complexas emoções humanas do usuário e agir de acordo (TENTO, 2021).

5. CONSIDERAÇÕES FINAIS

A presente pesquisa buscou investigar a importância do uso de inteligência artificial no setor empresarial. Concluiu-se com essa pesquisa que a Inteligência Artificial é considerada um importante avanço tecnológico para a humanidade, possibilitando a possibilita a sistemas a simulação de uma inteligência similar à humana, de modo a ultrapassar a programação de ordens específicas para a tomada autônoma de decisões, baseadas em padrões de grandes bancos de dados.

Também concluiu-se com a pesquisa que a globalização e o desenvolvimento tecnológico trouxeram consigo diversas consequências para o setor industrial e empresarial,

destacando-se o surgimento de processos industriais com melhor desempenho e máquinas mais modernas e eficientes. Sendo assim, a Indústria 4.0 surgiu na humanidade como um novo formato da indústria, passando a englobar as principais inovações tecnológicas nos campos da Tecnologia da Informação e da Engenharia aplicadas à manufatura.

Além disso, verificou-se que existem muitos exemplos de aplicações de IA, como veículos autônomos, diagnóstico médico, desenvolvimento de arte, teoremas matemáticos, jogos, mecanismos de busca, assistentes online, reconhecimento de imagem, filtragem de spam, julgamentos e marketing online. Dessa forma, pode-se perceber que a IA possui inúmeras aplicações na sociedade. Portanto, pode-se dizer que os objetivos propostos nessa pesquisa foram alcançados.

Referências

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. **Máquinas Preditivas: a simples economia da inteligência artificial**. Alta Books, 2020.

AIRES, Clayton Silva França; ALMEIDA, G. J.; SILVEIRA, Sidioney Onézio. Inteligência artificial na gestão de estoque. **Fateclog**, v. 1, p. 1-7, 2019.

AMORIM, Bianca Costa *et al*. Sistema de controle orçamentário e inovação: Um estudo em empresas de base tecnológica incubadas. **Espacios**, v. 37, n. 15, p. 16, 2017.

BERNARDO, Jaciely Barboza et al. INTELIGÊNCIA ARTIFICIAL E A LEI DE PROTEÇÃO DE DADOS. **Facit Business and Technology Journal**, v. 1, n. 33, 2022.

BERNI, Jean Carlo Albiero *et al*. Interação universidade-empresa para a inovação e a transferência de tecnologia. **Revista Gestão Universitária na América Latina-GUAL**, v. 8, n. 2, p. 258-277, 2019.

BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada. **Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil**, 2019.

CHRISTENSEN, Clayton M. **O dilema da informação: Quando as novas tecnologias levam empresas ao fracasso**. M. Books Editora, 2019.

COZMAN, Fabio Gagliardi. Inteligência Artificial: uma utopia, uma distopia. **TECCOGS: Revista Digital de Tecnologias Cognitivas**, n. 17, 2018.

DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar-Revista de Ciências Jurídicas**, v. 23, n. 4, p. 1-17, 2018.

FAVA, Rui. **Trabalho, educação e inteligência artificial: a era do indivíduo versátil**. Penso Editora, 2018.

GARCIA, Ana Cristina. Ética e inteligencia artificial. **Computação Brasil**, n. 43, p. 14-22, 2020.

GARCIA, Miguel Alexandre da Cruz. **Impacto da inteligência artificial no setor financeiro**. 2021. Tese de Doutorado.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?**. ESTAÇÃO DAS LETRAS E CORES EDI, 2019.

KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. **Revista Famecos**, v. 27, p. e34074-e34074, 2020.

LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Estudos Avançados**, v. 35, p. 85-94, 2021.

MAKSYM, Cristina Borges Ribas. Inteligência artificial aplicada nos serviços públicos rumo ao desenvolvimento sustentável: Artificial intelligence applied in public services towards the sustainable development. **International Journal of Digital Law**, v. 2, n. 1, p. 19-20, 2021.

MARCUZZO, Rafael; DOS SANTOS, Jordana Rech Graciano; SILUK, Julio Cezar Mairesse. Delineamento para identificação e gerenciamento de ativos intangíveis em empresas de base tecnológica. **Revista Científica on-line-Tecnologia, Gestão e Humanismo**, v. 7, n. 1, 2017.

NOBRE, E. A. *et al*. Capacidade de inovação nas empresas incubadas. **HOLOS**, v. 3, p. 198-217, 2017.

OLIVEIRA, Arlindo. **Inteligência artificial**. Fundação Francisco Manuel dos Santos, 2019.

PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. **Revista Brasileira de Inteligência Artificial e Direito-RBIAD**, v. 1, n. 1, p. 1-22, 2020.

PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins da. Inteligência artificial e Direito. **Curitiba: Alteridade**, v. 1, 2019.

PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária accountability. **Revista de Informação Legislativa**, v. 57, n. 225, p. 43-60, 2020.

PRADO, Magaly. **Fake News e Inteligência Artificial: O poder dos algoritmos na guerra da desinformação**. Digitaliza Conteudo, 2022.

ROMERO, Ray Cesar. Análisis del uso de la Inteligencia Artificial en la atención presencial de los clientes de Empresa de Telecomunicaciones Región Sur en el 2018. 2019.

RUFFONI, Janaína; SUZIGAN, Wilson. Inovação tecnológica de firmas em Sistemas Locais de Produção: a realidade dos produtores de máquinas para calçados do Rio Grande do Sul. **Ensaios FEE**, v. 36, n. 4, p. 1005-1036, 2020.

RUSSO, Inês Filipa Duarte. **O Impacte Da inteligência Artificial Na Sustentabilidade Ambiental: Uma Agricultura sustentável**. 2020. Tese de Doutorado. Universidade de Lisboa (Portugal).

SANTAELLA, Lucia (Ed.). **Inteligência artificial & redes sociais**. EDUC–Editora da PUC-SP, 2021.

SANTOS, C. F. *et al*. **Mapping the Conceptual Relationship among Data Analysis, Knowledge Generation and Decision-making in Industrial Processes.** Procedia Manufacturing, v. 11, June, p. 1751–1758, 2017.

SILVA, Bárbara Jennifer Paz de Abreu da et al. **Inteligência artificial e suas implicações ético-jurídicas**. 2020. Tese de Doutorado.

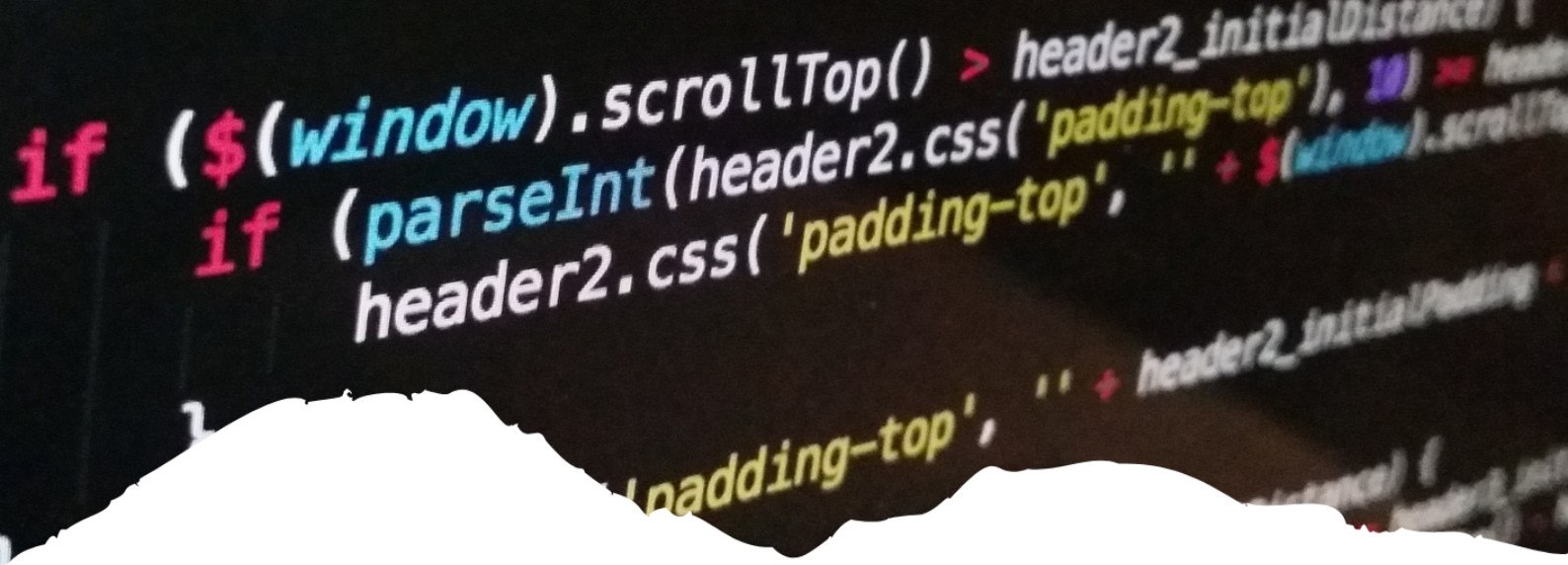
SILVA, Jassen Rodrigues da. A inteligência artificial como suporte à servitização digital. 2022.

TAMANAHA, Rodolfo Tsunetaka. **Tributação e economia digital: análise do tratamento tributário dos rendimentos da computação em nuvem**. 2020. Tese de Doutorado. Universidade de São Paulo.

TIGRE, Paulo Bastos *et al*. Janelas de oportunidades e inovação tecnológica na indústria brasileira de medicamentos. 2018.

TRENTO, Melissa. A inteligência artificial aplicada nos serviços públicos e os principais desafios impostos pela LGPD: The artificial intelligence applied in public services and the main challenges imposed by LGPD. **International Journal of Digital Law**, v. 2, n. 1, p. 17-18, 2021.

YUANGYAI, C. **Decentralized Network Building Change in Large Manufacturing Companies towards Industry 4.0.**Procedia Computer Science, v. 110, p. 46–53, 2017.



15

SEGURANÇA E PRIVACIDADE NA COMPUTAÇÃO EM NUVEM

CURITY AND PRIVACY IN CLOUD COMPUTING

Augusto Matheus Rodrigues Bussinguer

Resumo

Com o desenvolvimento tecnológico que tem se apresentado na computação, a Computação em Nuvem surgiu e tem sido cada vez mais utilizada por empresas e organizações de diferentes setores, com o objetivo de assegurar a proteção e a segurança dos dados, de modo a garantir a integridade e a privacidade das informações armazenadas. O principal objetivo desta pesquisa é identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem. Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Para tanto, buscou-se auxílio em livros, revistas e artigos das bases de dados Google Acadêmico e Sciello. Como resultado, verificou-se que a computação em nuvem, do inglês Cloud Computing, é uma expressão utilizada para definir um modelo de computação em que os recursos e serviços são disponibilizados em uma rede de servidores e utilizados de forma compartilhada através da internet. Observou-se que a solução para a segurança propõe que os provedores de computação em nuvem levem em consideração as práticas de segurança padrão, a fim de garantir a confiabilidade e prevenir contra o ataque de hackers. Além disso, pode-se verificar que a Computação em Nuvem proporciona diversos benefícios, como a escalabilidade, otimização, controle de acesso, disponibilidade e segurança. Como desvantagens, pode-se mencionar o tempo de inatividade, a falta de atenção dos usuários e o fato de que dados criptografados na nuvem podem sofrer ataques cibernéticos. Portanto, é importante preservar estes requisitos de segurança.

Palavras-chave: Segurança. Nuvem. Internet.

Abstract

With the technological development that has been presented in computing, Cloud Computing has emerged and has been increasingly used by companies and organizations from different sectors, in order to ensure the protection and security of data, in order to guarantee the integrity and the privacy of the information stored. The main objective of this research is to identify information security issues for the protection and privacy of data in services that use cloud computing. To carry out this work, the methodology used was a Bibliographic Review Research. For that, help was sought in books, magazines and articles from Google Scholar and Sciello databases. As a result, it was found that cloud computing is an expression used to define a computing model in which resources and services are made available on a network of servers and used in a shared way over the internet. It was noted that the security solution proposes that cloud computing providers take into account standard security practices in order to ensure reliability and prevent against hacker attack. In addition, it can be seen that Cloud Computing provides several benefits, such as scalability, optimization, access control, availability and security. As disadvantages, one can mention the downtime, the lack of attention of the users and the fact that data encrypted in the cloud can suffer from cyber attacks. Therefore, it is important to preserve these security requirements.

Keywords: Security. A cloud. Internet.

1. INTRODUÇÃO

Com a tecnologia no geral se desenvolvendo cada vez mais rápido e o mundo como um todo tornando-se mais conectado a cada dia, várias soluções são criadas para facilitar e baratear custos, tanto para os fornecedores de serviço quanto para os consumidores.

A Computação em Nuvem surgiu como uma tecnologia que possibilita o armazenamento e processamento de forma remota, não havendo a necessidade de máquinas fortes o suficiente para essas funções na empresa que utiliza esses serviços, com isso qualquer máquina conectada na nuvem poderia acessar as ferramentas oferecidas visto que as mesmas estariam sendo disponibilizadas remotamente, e sendo processadas em uma outra máquina.

A tecnologia começou a ser amplamente utilizada sendo mais barata para a empresa do que a forma tradicional que seria possuir todas as máquinas necessárias de forma física, com isso dados e mais dados são armazenados na nuvem, dados esses com informações sigilosas, tanto informações pessoais quanto empresarias. Com isso ataques são feitos a todo momento com o intuito de roubar informações, surge então a grande necessidade de proteger esses dados, utilizando métodos e boas práticas de proteção tanto para enviar golpes e fraldes quanto para manter a credibilidade e confiança com a empresa.

Com a tecnologia da Computação em Nuvem (*Cloud Computing)* tornando-se cada vez mais utilizada por bancos, lojas e Grandes Empresas é necessário assegurar a proteção e segurança dos dados, garantindo assim a integridade e privacidade das informações armazenadas. Sem essa segurança as empresas sofreriam ainda mais com ataques, os dados poderiam ser vazados ou roubados criando assim uma brecha para fraudes, golpes bancários, falsidade ideológica dentre outros crimes e também uma queda na credibilidade e confiança com a instituição atacada, justificando essa pesquisa.

A segurança e proteção de redes se faz cada vez mais importante visto que com os avanços tecnológicos e o mundo cada vez mais conectado surgem também novos casos de invasões e violações em redes por conta de hackers, vírus, malwares e outros fatores de risco. Diante disso, questiona-se: Qual a importância da proteção de redes para serviços que utilizam Computação em Nuvem?

O principal objetivo desta pesquisa é identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam Computação em Nuvem. Especificamente, pretende-se: Analisar os conceitos e características da Computação em Nuvem; apontar os principais aspectos relacionados à segurança da Computação em Nuvem; demonstrar as vantagens e desvantagens ao usar Computação em Nuvem.

Para a realização deste trabalho, a metodologia utilizada foi uma Pesquisa de Revisão Bibliográfica. Para tanto, buscou-se auxílio em livros, revistas e artigos das bases de dados Google Acadêmico e Sciello, que pudessem oferecer referenciais teóricos condizentes com o tema apresentando, dando subsídio para a construção do trabalho. Foram utilizados os materiais acadêmicos publicados nos últimos cinco anos (2017 a 2022). As palavras-chaves na utilizadas na pesquisa foram: Computação em Nuvem; Tecnologia; Dados; e Segurança de Rede.

2. A COMPUTAÇÃO EM NUVEM

Entende-se que a Computação em Nuvem é uma tecnologia que disponibiliza recursos computacionais de forma remota e compartilhada por todos que estão conectados. De acordo com Ferreira e Carvalho (2020, p.21):

A Computação em Nuvem, do inglês Cloud Computing ou apenas cloud, é o termo utilizado para definir um modelo de computação em que os recursos e serviços são disponibilizados em uma rede de servidores e utilizados de forma compartilhada através da internet.

Para Camboim e Alencar (2018), o termo nuvem vem sendo utilizado como sinônimo de internet. Esse uso inicialmente derivou-se da sua estrutura representativa em diagramas de rede, esboçando uma nuvem, utilizado para demonstrar a movimentação de dados por meio de backbones que pertenciam à nuvem.

Segundo Silva Neto, Bonacelli e Pacheco (2021), o conceito de nuvem surgiu em 1961, quando o professor John McCarthy propôs que a tecnologia teria o poder de levar a um futuro em que a computação poderia ser comercializada por meio de um modelo de negócio utilitário. Com a virada do milênio, o conceito foi revitalizado e a expressão Computação em Nuvem passou a ser utilizada nos ambientes e cenários tecnológicos (PEREIRA, 2019).

Ainda de acordo com Pereira (2019), a expressão Computação em Nuvem diz respeito à disponibilidade sob demanda de recursos computacionais como armazenamento e processamento, sem o gerenciamento nem o gasto de recursos direto do utilizador. Após o surgimento da internet a Computação em Nuvem surgiu, mas foi só depois de 1995 que ela deixa de ser unicamente de uso acadêmico e começa a ser explorada por empresas de forma comercial. Com o custo de utilização de serviços sendo mais baixo que o de uma montagem e gerenciamento de uma infraestrutura completa, a Computação em Nuvem começou a ser explorada comercialmente.

De acordo com as palavras de Tamanaha (2020), com os avanços tecnológicos e econômicos em diversas áreas, a forma de consumo de determinados produtos e serviços foi se moldando com essa evolução. Alguns serviços básicos como eletricidade, gás e água são utilizados de forma muito simples, mas, toda infraestrutura por trás de tais serviços é gerenciada por uma empresa que faz a cobrança desse serviço de acordo com a demanda do mesmo e não pelo valor que seria gasto por uma pessoa comum em toda a infraestrutura responsável pelo fornecimento de tal produto. “Computação em Nuvem é uma tendência recente de tecnologia cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso.”Portanto, seguindo a mesma ideia dos outros serviços, a Computação em Nuvem é um serviço oferecido que é cobrado pela demanda de seus usuários.

A Figura 1 apresenta o exemplo de uma organização contratante que não custeia os investimentos em equipamentos e sua manutenção, tendo em vista que a empresa contratada disponibiliza a manutenção dos equipamentos e os compartilha com demais usuários.

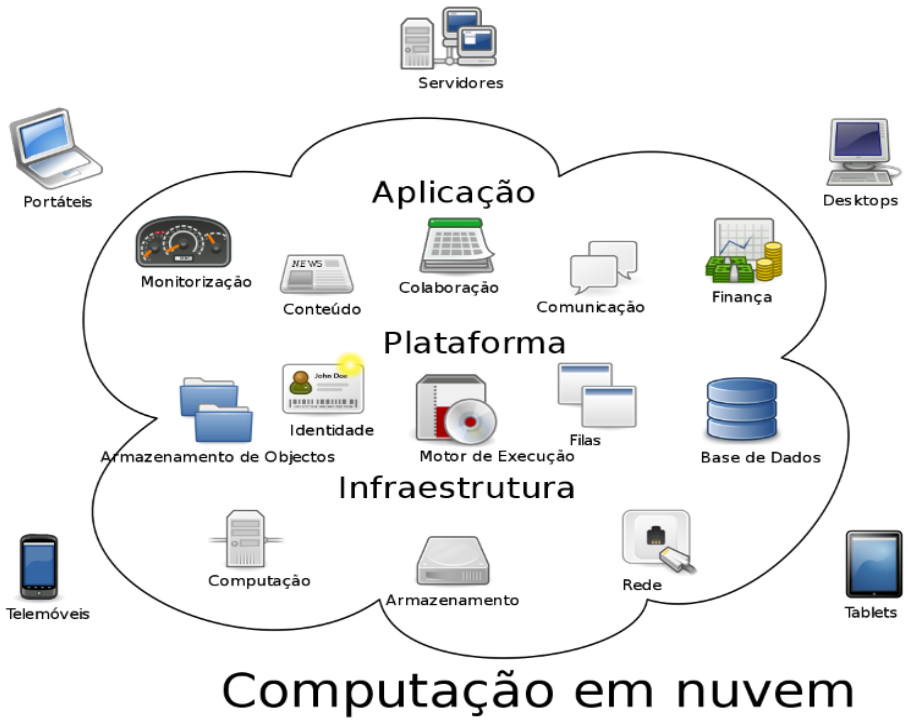


Figura 1: Como a Computação em Nuvem hospeda aplicações

Fonte: Martins (2019).

Segundo as palavras de Avinte, Nascimento e Nascimento (2019), a Computação em Nuvem pode ser também conceituada como a entrega de recursos de TI sob demanda através da internet, cujo uso estabelece um preço de pagamento. Sendo assim, ao invés de comprar e ter que manter servidores, o usuário tem a possibilidade de acessar os serviços por meio de banco de dados, de acordo com a sua necessidade, usando provedores.

Para Arnold e Zanella (2022), entende-se que a Computação em Nuvem diz respeito ao fornecimento sob demanda de recursos da Tecnologia da Informação por meio da internet. Ao invés de utilizar hardwares ou softwares que estão no local, a tecnologia utilizada é aquela disponível em um banco de dados remoto. Mesmo que, muitas vezes sejam gratuitos, a maior parte dos serviços de Computação em Nuvem são pagos.

Sendo assim, a Computação em Nuvem é vista por muitos autores como uma evolução natural dos sistemas de computação atual e a sua exploração leva à um novo patamar de criação de aplicativos. Desse modo, uma empresa pode tanto contratar um servidor de serviços em nuvem como utilizar seu data e realizar esse serviço.

Neste sentido, a Figura 2 apresenta as origens da Computação em Nuvem:

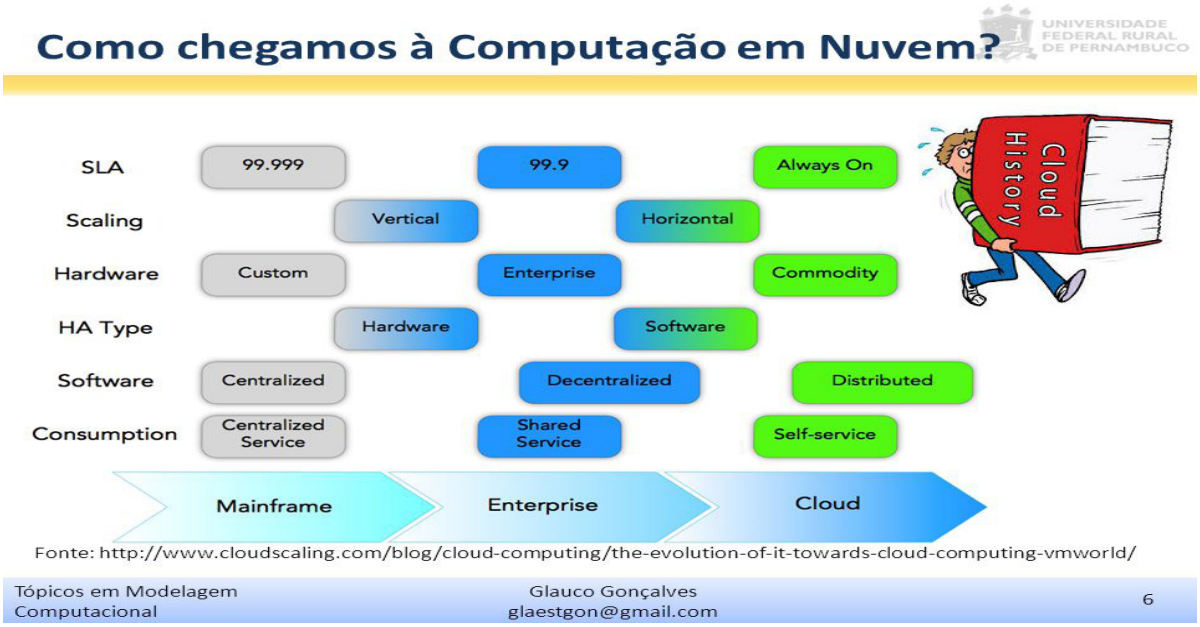


Figura 2: Origens da Computação em Nuvem

Fonte: Martins (2019).

Frente a isso, alguns elementos merecem destaque na origem da Computação em Nuvem, sendo eles:

- Utility Computing – Corresponde à entrega de recursos de computação a um determinado cliente que paga por essa demanda quando há necessidade. O seu objetivo é utilizar os serviços de maneira eficiente, reduzindo assim os custos. Esse termo é comumente empregado na comparação do uso deste tipo de recurso computacional com os fornecedores de energia elétrica, por exemplo (CARVALHO; ARAÚJO, 2021).
- Grid Computing – Refere-se à aplicação do poder de processar diversos recursos computacional em rede, a fim de resolver especificamente um problema. Representa uma maneira de processamento paralelo executado em uma rede de computadores. Nesse sistema, os servidores, as redes e o armazenamento combinam-se, a fim de formar nós fortes e poderosos, correspondendo a um recurso que pode ser configurado de modo dinâmico, de acordo com a necessidade do usuário (ARNOLD; ZANELLA, 2022).
- Autonomic Computing – Diz respeito ao funcionamento de um sistema de computadores, sem a necessidade de controles externos. Esse termo baseia-se no sistema nervoso autônomo do corpo humano, que controla as suas diferentes funções. Assim, o seu objetivo é fazer com que o computador execute complexas funções, sem necessidade de intervenções relevantes do usuário (FRANCO et al., 2021).
- Platform Virtualization – Esse elemento corresponde à repartição logica dos recursos computacionais em ambientes de múltipla execução, onde se incluem servidores, sistemas operacionais e aplicativos. A virtualização baseia-se no conceito de uma máquina virtual que é executada sobre uma plataforma física. A virtualização da plataforma é controlada através de um Monitor de Máquina Virtual (VMM), também conhecido como Hypervisor Xen. Este, é um dos recursos computacionais mais utilizados na Computação em Nuvem.
- Software as a Service (SaaS) – Este elemento refere-se à distribuição de software e modelo de implementação onde as aplicações são disponibilizadas aos usuários

como um serviço. Sendo assim, eles podem ser adequadamente executados em sistemas dos usuários ou ainda, em servidores do seu provedor, prevendo a eficácia no gerenciamento de patches, bem como a colaboração (NETO et al., 2020).

- Service Oriented Architecture (SOA) – Esse recurso compreende um conjunto de serviços que comunicam-se entre si, tendo suas interfaces descritas e seu uso pode ser empregado em diversas organizações. A interface desses serviços é especificada em XML (Extensible Markup Language) (FRANCO et al., 2021).

Desse modo, observa-se que esses elementos possuem significativa relevância para a Computação em Nuvem, representando recursos que podem ser utilizados e que contribuem para seu o bom funcionamento.

Nesse sentido, Souza e Oliveira (2019, p.14) argumentam que:

> Como um novo estilo de computação em que os recursos dinamicamente escaláveis e muitas vezes virtualizados são fornecidos como serviços através da Internet. Computação em Nuvem se tornou uma tendência tecnológica significativa, e muitos especialistas esperam que a Computação em Nuvem irá reformular a tecnologia da informação (TI) os processos e o mercado de TI. Com a tecnologia de Computação em Nuvem, os usuários usam uma variedade de dispositivos, incluindo PCs, laptops, smartphones e PDAs para acessar programas, armazenamento e aplicação de desenvolvimento de plataformas pela Internet, através de serviços oferecidos por provedores de Computação em Nuvem.

Para Picoto, Crespo e Carvalho (2021), com a popularização das redes wireless, e a grande quantidade de dispositivos conectados como smartphones, tablets e notebooks a Computação em Nuvem cresce a cada dia, por conta do seu processamento e baixo custo de utilização. “A computação na nuvem ou Cloud Computing é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independentemente da plataforma, bastando para isso ter um terminal conectado à “nuvem”’.

Portanto, a facilidade de acesso a arquivos e aplicações e a comodidade de utilização dos serviços a tendência é que essa tecnologia se desenvolva ainda mais com o passar dos anos.

3. SEGURANÇA NA NUVEM

Diversos níveis de segurança são importantes em um ambiente de nuvem, destacando-se o gerenciamento de identidades, controle de acesso, autorização e autenticação. De acordo com Gomes (2022, p.31):

> Uma rede virtual privada (VPN) é uma maneira de gerenciar a segurança de dados durante o transporte em um ambiente de nuvem. Uma VPN faz essencialmente a rede pública de sua própria rede privada em vez de usar a conectividade dedicada. Uma VPN bem projetada deve incorporar duas coisas: Um firewall- Pode agir como uma barreira para a Internet entre público e privado de qualquer rede (como na empresa); Criptografia- Para proteger seus dados sensíveis contra hackers.

“Devido ao fato de que a computação em nuvem e a virtualização podem ajudar as empresas a ultrapassarem a barreira física entre os usuários e a infraestrutura, as ameaças de segurança devem ser combatidas e superadas”, como destaca Peixoto (2022, p.11)

Além das questões de segurança e privacidade, há questões jurídicas a serem consideradas. Por exemplo, o que acontece ao seu aplicativo e dados, se o provedor de nuvem sai do negócio? Quem é responsável por informações perdidas? Quais são os recursos que você tem, se o acordo de nível de serviço não for atendido?

Portanto, a solução para a segurança propõe que os provedores de computação em nuvem levem em consideração as práticas de segurança padrão, a fim de garantir a confiabilidade e prevenir contra o ataque de hackers.

Talvez a maior desvantagem percebida de desenvolvimento nas nuvens é o mesmo, um que assola todos os aplicativos baseados na web: É seguro? Aplicativos baseados na Web têm sido considerados potenciais riscos de segurança. Por esta razão, muitas empresas preferem manter seus aplicativos, dados e operações de TI sob seu próprio controle (TAURION, 2019, p.40).

De acordo com Carvalho e Alencar (2018), existem os riscos associados ao uso de serviços de computação em nuvem, pode-se citar a questão da confiabilidade, tendo em vista que o provedor de serviços pode apresentar problemas técnicos, ou ainda os usuários podem acabar expondo seus dados para usuários não autorizados.

Com base nesse pensamento, Carvalho e Araújo (2021, p.31) expõem que:

> Dois desafios devem ser perfeitamente endereçados em um ambiente de computação em nuvem: a gestão da segurança e privacidade e a gestão dos equipamentos móveis. Na verdade, estes dois desafios estão entrelaçados e não podemos resolver um sem, pelo menos parcialmente, resolvermos o outro.

Empresas que utilizam seu próprio datacenter podem sofrer significativas falhas de segurança. A segurança para o armazenamento em nuvem inicia-se no browser, considerado o ponto de entrada para iniciar os serviços em nuvem. O browser pode estar sendo executado em um smartphone, laptop, notebook ou desktop. Existe ainda o agravante de que um dispositivo móvel pode ser roubado ou perdido. Pode-se criptografar os dados antes de armazená-lo na nuvem, dessa forma, levando em consideração tal fato e as medidas de segurança executadas pelo fornecedor da nuvem, os dados podem estar armazenados com segurança (PEREIRA, 2019).

Por exemplo, a política do Google estabelece que a companhia compartilhará dados com o governo, caso este último aja de boa fé no que diz respeito à necessidade deste acesso para cumprir as postulações de acordo com a lei. Em alguns casos, se os provedores receberem citações judiciais, o provedor é proibido por lei de contar aos clientes que os dados foram fornecidos ao governo (CARVALHO; ARAÚJO, 2021, p.40)

No caso de arquivos que são editados online, ao contrário de serem armazenados na web, não podem ser criptografados quando salvos na nuvem, como é o aso de planilhas eletrônicas ou arquivos de texto. Os hackers podem comercializar as informações registradas para que o concorrente possa criptografar os dados armazenados ou ainda, apagar todas as informações, justificando tal ação por meio de crenças ideológicas (NETO et al., 2020).

O pior dos casos, os hackers que atacam utilizam botnets para executar negações

distribuídas dos ataques de serviço (DDOS). Uma das principais empresas de Tokio teve de pagar 3 milhões de yens (cerca de U$ 31.000) depois que a rede foi levada a uma parada enlouquecedora por um ataque botnet (CARVALHO; ARAÚJO, 2021, p.40).

Faz-se necessário, portanto, que o governo implemente ações e políticas que regulem a computação em nuvem. Essa é considerada uma linha de pensamento, porém, há que acredite que o governo deva se eximir dessa participação, ficando de fora e deixando que as forças de mercado guiem a computação em nuvem (GOMES, 2022).

O uso dos denominados clientes thin cria maiores chances para armazenamento centralizado de dados, o que possibilita menores chances de que os dados vazem. O SSL VPN é considerado uma significativa solução de segurança, pois permite que o acesso às aplicações ocorra de modo eficiente, barato e com maior facilidade. Ele é um protocolo que administra a segurança de dados na internet, empregando um sistema principal privado e público de criptografia, chamado de RSA (NETO et al., 2020).

Outra opção é conectar ao provedor de serviços diretamente utilizando wide área network (WAN) (normalmente uma conexão MPLS/VPN). Esta configuração garante a confidencialidade, largura de banda garantida, e SLAs de disponibilidade, latência e perda de pacotes (TAURION, 2019, p.40).

Criptografar os dados, bem como assegurar que eles sejam configurados para serem destruídos assim que a chave de armazenamento for destruída, é fundamental. Sendo assim, é importante acompanhar as chaves no servidor, que incluem, de acordo com Santos (2018):

- Chaves de transporte;
- Chaves de autenticação
- Símbolos de autorização;
- Criptografia de arquivo-chave
- Armazenamento de hardware-chave;
- Chaves de revogação;
- Certificado.

A segurança dos dados é um ponto muito controverso, quando o tema é computação na nuvem. Ainda se tem dúvidas se é possível garantir a segurança total dos dados em trânsito, sem que haja chances de vazamento de informações confidenciais das organizações (GOMES, 2022).

A Figura 3 apresenta o ciclo de vida da segurança de dados na nuvem:

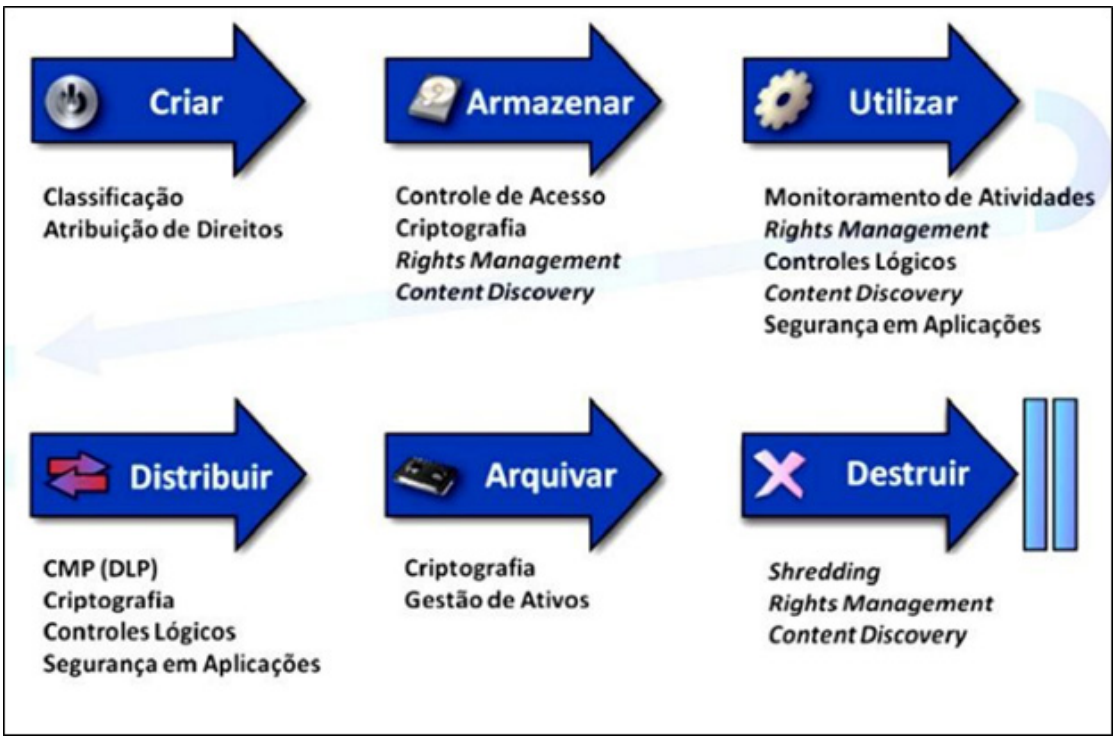


Figura 3: Ciclo de vida da segurança de dados na nuvem

Fonte: Martins (2019).

Considerando a segurança no que diz respeito aos controles que o contratante possui, na camada IaaS, existe um controle total sobre o hardware, entretanto, não é possível o acesso diretamente ao hardware da máquina. Na camada PaaS, também não ocorre o controle do hardware da máquina, mas sim as configurações de ambiente e instalação de software, bem como provê a contratação de tal tipo de serviço. Já no Saas, não existe qualquer tipo de controle sobre o hardware, no entanto, a customização sobre a sua aplicação pode ser possível (SANTOS, 2018).

Existe uma grande preocupação no que se refere à segurança e à privacidade. Ao usar o sistema, o usuário coloca à disposição e cuidados de outra empresa os seus dados e informações, o que para muitos usuários é uma questão difícil, causando uma sensação de vulnerabilidade, ao contrário dos dias atuais, em que os dados e informações são guardadas com segurança por seus proprietários (GOMES, 2022).

Renomadas instituições de pesquisas, como a Cloud Security Alliance – CSA e a European Network and Information Security Agency - Enisa evidenciam diversos problemas de segurança que devem ser tratados no que se refere à computação em nuvem. Esses problemas devem ser combatidos, não somente com o objetivo de tornas as soluções mais seguras, assim como para aumentar o nível de adoção da tecnologia a ser utilizada, tanto pelo meio acadêmico como pelo mercado (TAURION, 2019).

Sendo assim, de acordo com as palavras de Peixoto (2022), os problemas de segurança em computação em nuvem são classificados em sete categorias: segurança de rede, interfaces, segurança de dados, virtualização, governança, conformidade e questões legais.

No entanto, de acordo com as palavras de Gomes (2022), esses problemas não representam provas de que o modelo de computação em nuvem seja completamente inseguro. As ameaças de segurança são referentes a ambientes a ambientes online, de modo independente à adoção ou não do formato de computação em nuvem.

4. VANTAGENS E DESVANTAGENS DA COMPUTAÇÃO EM NUVEM

Dentre as principais questões organizacionais abordadas ao se tratar sobre a computação em nuvem, destacam-se os benefícios e riscos provenientes do uso dessa tecnologia. Quando uma empresa resolve por adotar esse modelo para implantar seus recursos operacionais, ou ainda, aumentar a gama de serviços oferecidos aos seus consumidores, os seus gestores devem considerar o custo-benefício de se transferir a sua capacidade funcional para terceiros (ARNOLD; ZANELLA, 2022).

Sendo assim, de acordo com Avinte e Nascimento (2019), pode-se mencionar como principais benefícios da computação em nuvem para as empresas:

- Escalabilidade – Uma das características principais da computação em nuvem é a possibilidade de reduzir ou aumentar recursos, conforme a demanda operacional de cada empresa.
- Otimização – Por ser um ambiente virtual, é possível alterar procedimentos, sem a necessidade de estabelecer novos recursos e equipes, e notificar todos os colaboradores sobre quem fez a alteração automaticamente.
- Controle de acesso – A ferramenta de controle de acesso de usuários cria permissões de acordo com as tarefas de cada colaborador. Assim, os gestores têm visibilidade de quem acessa as aplicações da empresa.
- Disponibilidade- A computação em nuvem permite retirar qualquer elemento ou sistema dos serviços da empresa para reparo, manutenção ou substituição, sem afetar os processos de TI.
- Segurança – O armazenamento na nuvem utiliza computação avançada, além de ser capaz de fazer backup e identificar vulnerabilidades.

De acordo com Sousa, Moreira e Machado (2019), uma das principais vantagens da computação em nuvem, é o fato de que o usuário paga somente pelo que utiliza. Há um certo tempo atrás, se um usuário optasse por utilizar um software complexo como um ERP, ele deveria adquirir seus próprios servidores, para então poder instalar um software. Este mesmo usuário deveria comprar as licenças nos seus respectivos bancos de dados, bem como ter que pagar caro por serviços especializados para a manutenção do sistema.

Taurion (2019) destaca também que era comum, há anos atrás, que a empresa comprasse um poderoso maquinário, a fim de atender um período em que o processamento atingisse seu pico. Isso fazia com que a organização apresenta-se capacidade ociosa ou ainda, que necessitasse de uma renovação do seu maquinário e computadores, pois esses se tornavam ultrapassados. Sendo assim, uma alternativa para essa problemática seria a computação em nuvem, pois as empresas que passam a utilizar essa ter que alugar a capacidade de hardware que desejam utilizar por um determinado período de tempo, pagando somente pelo que utilizam (SANTOS, 2018).

Isso também é valido para os softwares que a empresa necessita. Em vez de comprar uma licença de uso e ter que adquirir servidores para a sua instalação, na computação em nuvem o usuário paga somente um valor mensal para o fornecedor do sistema. Além da funcionalidade do sistema, que costuma ser na hora, os custos são bem menores (SANCHEZ; CAPELLOZZA, 2022).

Outra grande vantagem da computação em nuvem é a sua flexibilidade. Ou seja, o cliente tem o poder de decidir pelo aumento ou pela diminuição da infraestrutura tecnológica que for utilizar, no momento que quiser, de maneira eficiente e ágil. Se a organização cresce de maneira rápida, não se faz necessário investimentos significativos e grandes

planejamentos. O cliente simplesmente pode escolher ter mais recursos à sua disposição em um apertar de botões, aumentando o espaço em seu banco de dados nas nuvens (CARISSIMI, 2017).

Quando o usuário utiliza um software armazenado na nuvem, o fornecedor é responsável por isso. Através de técnicas automatizadas que garantem a disponibilidade, não importa a quantidade de usuários naquele momento, pois o próprio fornecedor se responsabiliza pelo processamento do software. Isso ocorre através de métodos automatizados que garantem que sempre existirá tal disponibilidade. Essa função é considerada bastante útil para aqueles que lidam com negócios temporários e sazonais, que apresentam quedas e picos de movimento (HEDLER et al., 2018).

Mais uma das vantagens do Could Computing é que as empresas, ainda que possuam pequeno porte, conseguem acessar recursos de tecnologia de ponta. Antes, adquirir recursos tecnológicos complexos de sofisticados não era uma realidade para empresas pequenas. Atualmente, levando em consideração o modo de funcionamento da computação em nuvem, observa-se uma grande quantidade de pequenas empresas utilizando os mesmos recursos que utilizam as grandes organizações. Antigamente, adquirir um sistema sofisticado de gestão, era uma realidade distante para pequenas empresas, fato que vem mudando nos dias atuais. Essa realidade só ocorre porque cada empresa paga pelo que utiliza. Sendo assim, os preços acabam sendo ajustados ao porte da organização e a sua necessidade de uso (GOMES, 2022).

A respeito dos benefícios da Cloud Computing para seus usuários, Peixoto (2022, p.21) destaca que:

> Cloud Computing é a área, mas o cliente pode utilizar este conceito em software ou hardware. Existem vários tipos serviços de Computação em Nuvem. Por exemplo, o cliente pode “alugar” um espaço num servidor e utilizar como precisar, ou pode alugar um software para atender uma ou mais áreas de sua empresa, com tudo já pronto, sem ter que configurar nada. Além de ser mais acessível e flexível, o modelo de software como serviço (Empresas SaaS) tem outras vantagens.

Conforme destaca Parchen e Freitas (2021), o modelo cloud computing vem modificando consideravelmente a relação estabelecida entre cliente e vendedor, tendo em vista que a excelência e qualidade dos serviços oferecidos devem ser contínuas. Caso não esteja satisfeito com o serviço oferecido, o usuário pode trocar de fornecedor, sem que seu negócio sofra impactos significativos. Isso exige que o fornecedor apresente uma atenção especial, a fim de que consiga manter seus clientes satisfeitos e conquistar novos mercados. Sabe-se que a Cloud Computing possui vantagens e desvantagens. No entanto, também é sabido e evidente que as vantagens da implantação desse sistema têm sido cada vez mais significativas.

De maneira sucinta, Vieira e Meireles (2022) afirmam que dentre as vantagens da computação em nuvem, podem ser destacadas: a) compartilhamento de dados; b) memória livre; c) acessibilidade; d) backup e restauração de dados; e) fácil uso por pessoas leigas; f) não necessita de manutenção; g) útil para todos, podendo ser ofertada em versões pagas e gratuitas.

A Figura 4 apresenta os principais benefícios da computação em nuvem:

Figura 4: Principais benefícios da computação em nuvem

Fonte: Martins (2019).

No que se refere às desvantagens da computação em nuvem, Taurion (2019) destaca que uma delas é o custo, pois para cada atividade realizada pela organização, existe um custo a ser pago, e isso não seria diferente no caso da computação em nuvem, pois é necessário que o usuário contrate um servidor. Isso inclui também a obtenção de um serviço mais complexo e robusto, assim como mais espaço de armazenamento. Além disso, faz-se necessário que haja uma internet de qualidade, consistente e confiável, a fim de aproveitar as vantagens dessa tecnologia.

De acordo com Sousa, Moreira e Machado (2019), uma das maiores desvantagens é que os provedores podem enfrentar falhas técnicas, em função de motivos como por exemplo, a conectividade baixa da internet, quedas de energia, entre outros. Quando a conexão com a internet é suspendida, o acesso aos servidores torna-se indisponível, comprometendo o bom andamento do trabalho. Dessa forma, é necessário garantir que a falta de energia não prejudique ou comprometa o acesso à internet, devendo-se levar em consideração a possibilidade de aquisição de geradores de energia elétrica e planos de internet móvel.

Mesmo que existam opções gratuitas, organizações e empresários que geram e acessam grandes volumes de arquivos, necessitam de planos pagos para atender às suas demandas e necessidades. Ainda que os arquivos sejam criptografados, a partir do momento em que são guardados na nuvem, existem chances da ocorrência de ataques cibernéticos e da captura de logins e senhas, o que representa um grande perigo e transtorno para essas empresas. Desse modo, é necessário que se busque por serviços seguros e confiáveis (SANTOS, 2018).

De acordo com Taurion (2019), os fornecedores de serviços na nuvem também podem entrar em falência. Dessa forma, existem sempre a possibilidade de uma empresa alterar o seu serviço ou falir. Assim que avalia os fornecedores de serviços na nuvem, é importante que o usuário descubra de que modo pode obter seus dados de volta, caso o fornecedor sofra falência.

Santos (2018) ressalta que, para que as empresas possam utilizar as ferramentas sedeadas na nuvem, necessitam de uma conexão mais segura e confiável. Então, se o acesso à internet é inconsistente e a velocidade ou largura da banda representam um problema, os serviços na nuvem poderão ser comprometidos e representar um problema.

Corroborando com o assunto, Carissimi (2017, p.21) afirma que as principais desvantagens da computação em nuvem são:

- **Custo:** para cada ação realizada pela empresa, existe um custo a ser adicionado no orçamento e no caso da computação em nuvem não seria diferente, já que você terá de contratar um servidor para atender especificamente às necessidades de seus colaboradores. Isso inclui a obtenção de um serviço mais robusto ou maior espaço de armazenamento.
- **Internet:** é necessário ter uma internet de qualidade, confiável e consistente para aproveitar os benefícios da tecnologia em nuvem.
- **Tempo de inatividade:** uma das maiores desvantagens da tecnologia em nuvem. Seus provedores podem enfrentar interrupções técnicas devido a motivos como perda de energia, baixa conectividade da internet, entre outros.
- **Preço:** existem opções gratuitas, mas empresas e empresários que criam e acessam grande volume de arquivos podem precisar de planos pagos para atender às suas necessidades.
- **Confiança:** apesar dos arquivos serem criptografados, a partir do momento em que são armazenados na nuvem, seus dados podem sofrer ataques de cibercriminosos e ter logins e senhas capturados, o que pode gerar um grande transtorno para a empresa no futuro. Por isso é necessário buscar um serviço seguro e confiável.

Sendo assim, pode-se afirmar que o custo, a dependência de uma internet confiável e segura, o tempo de inatividade, o preço e os riscos de sofrerem ataques cibernéticos, representam algumas das principais desvantagens do uso da computação na nuvem.

5. CONSIDERAÇÕES FINAIS

A presente pesquisa buscou identificar questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem. Constatou-se com essa pesquisa que a Cloud Computing, refere-se ao armazenamento e compartilhamento de arquivos na internet. Ela está associada a um espaço virtual, onde é completamente possível o acesso às informações armazenadas. Esses dados podem ser compartilhados com outros usuários, tanto por meio do acesso direto à ferramenta de computação escolhida, como através do envio de links que permitirão o acesso aos arquivos desejados.

Também observou-se com a pesquisa que Diversos níveis de segurança são importantes em um ambiente de nuvem, destacando-se o gerenciamento de identidades, controle de acesso, autorização e autenticação. Além disso, diversas empresas estão voltando o seu olhar para a Cloud Computing, principalmente mediante aos benefícios que ela proporciona, podendo-se citar: agilidade, segurança, flexibilidade de acesso às informações, escalabilidade, otimização, controle de acesso e disponibilidade.

Entretanto, também existem as desvantagens, como o tempo de inatividade, a falta de atenção dos usuários e o fato de que dados criptografados na nuvem podem sofrer ataques cibernéticos. Diante disso, pode-se afirmar que, com essa pesquisa, foram identificadas as questões de segurança da informação para a proteção e privacidade dos dados em serviços que utilizam computação em nuvem e o objetivo deste trabalho foi alcançado.

Referências

ARNOLD, Felipe Matheus Wust; ZANELLA, Renata. COMPUTAÇÃO EM NUVEM: um estudo sobre o Google Drive como ferramenta colaborativa aplicada a educação. **Trajetória Multicursos**, v. 12, n. 2, p. 110-136, 2022.

AVINTE, Eduardo Frias; NASCIMENTO, Manoel Henrique Reis; NASCIMENTO, Aline Santos. COMPUTAÇÃO EM NUVEM: REDUZINDO GASTOS EM PEQUENAS E MÉDIAS EMPRESAS. **ITEGAM-JETIA**, v. 5, n. 19, p. 41-47, 2019.

CAMBOIM, Kádna; ALENCAR, Fernanda MR. Requisitos não Funcionais e Sustentabilidade para Computação em Nuvem: uma Revisão Sistemática da Literatura. **WER**, 2018.

CARISSIMI, Alexandre. Desmistificando a Computação em Nuvem. **Instituto de Informática–Universidade Federal do Rio Grande do Sul (UFRGS) –Porto Alegre–RS** , 2017.

CARVALHO, Leonardo Rebouças; ARAUJO, Aleteia Patricia Favacho. Function-as-a-Service: Desenvolvendo Aplicações na Próxima Geração da Computação em Nuvem. **Sociedade Brasileira de Computação**, 2021.

FRANCO, Carlos Leonardo Freitas Viveiros et al. VANTAGENS DA COMPUTAÇÃO EM NUVEM PARA EMPRESAS DE MENOR PORTE. **South American Development Society Journal**, v. 7, n. 20, p. 255, 2021.

GOMES, Carina Nobre. **Estudo do paradigma: computação em nuvem**. 2022. Tese de Doutorado.

HEDLER, Helga Cristina et al. Aplicação do modelo de aceitação de tecnologia à computação em nuvem. **Perspectivas em Gestão & Conhecimento**, v. 6, n. 2, p. 188-207, 2018.

MARTINS, Ana Paula. CLOUD GAMING: Computação em Nuvem nos jogos digitais. **Revista Interface Tecnológica**, v. 16, n. 1, p. 158-170, 2019.

NETO, Francisco et al. Computação em Nuvem e aprendizado de máquina para análise de grandes volumes de dados educacionais. In: **Anais do XVII Encontro Nacional de Inteligência Artificial e Computacional**. SBC, 2020. p. 58-69.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen Almendra. Computação em Nuvem e Aspectos Jurídicos da Segurança da Informação. **Revista Jurídica Cesumar-Mestrado**, v. 13, n. 1, 2021.

PEIXOTO, Maycon Leone Maciel. **Oferecimento de QoS para computação em nuvens por meio de metaescalonamento**. 2022. Tese de Doutorado. Universidade de São Paulo.

PEREIRA, Thiago Martins. COMPUTAÇÃO EM NUVEM: PLATAFORMA COMO SERVIÇO. **MARTINS, Ernane Rosa. Fundamentos da Ciência da Computação**, v. 2, p. 116-125, 2019.

PICOTO, Winnie Ng; CRESPO, Nuno Fernandes; CARVALHO, Filipa Kahn. A influência da estrutura tecnologia-organização-ambiente e da orientação estratégica no uso da Computação em Nuvem, mobilidade empresarial e desempenho. **Revista Brasileira de Gestão de Negócios**, v. 23, p. 278-300, 2021.

SANCHEZ, Otávio Próspero; CAPPELLOZZA, Alexandre. Antecedentes da adoção da computação em nuvem: efeitos da infraestrutura, investimento e porte. **Revista de Administração Contemporânea**, v. 16, p. 646-663, 2022.

SANTOS, Tiago. **Fundamentos da computação em nuvem**. Senac, 2018.

SILVA NETO, Victo José da; BONACELLI, Maria Beatriz Machado; PACHECO, Carlos Américo. O sistema tecnológico digital: inteligência artificial, Computação em Nuvem e Big Data. **Revista Brasileira de Inovação**, v. 19, 2021.

SILVEIRA, Tiago; CARVALHO, Leonardo Filipe Batista Silva. Benefícios de Redução de custo na Infraestrutura da Migração de Serviços de Computação em Nuvem. **PROJETOS E RELATÓRIOS DE ESTÁGIOS**, v. 2, n. 1, 2020.

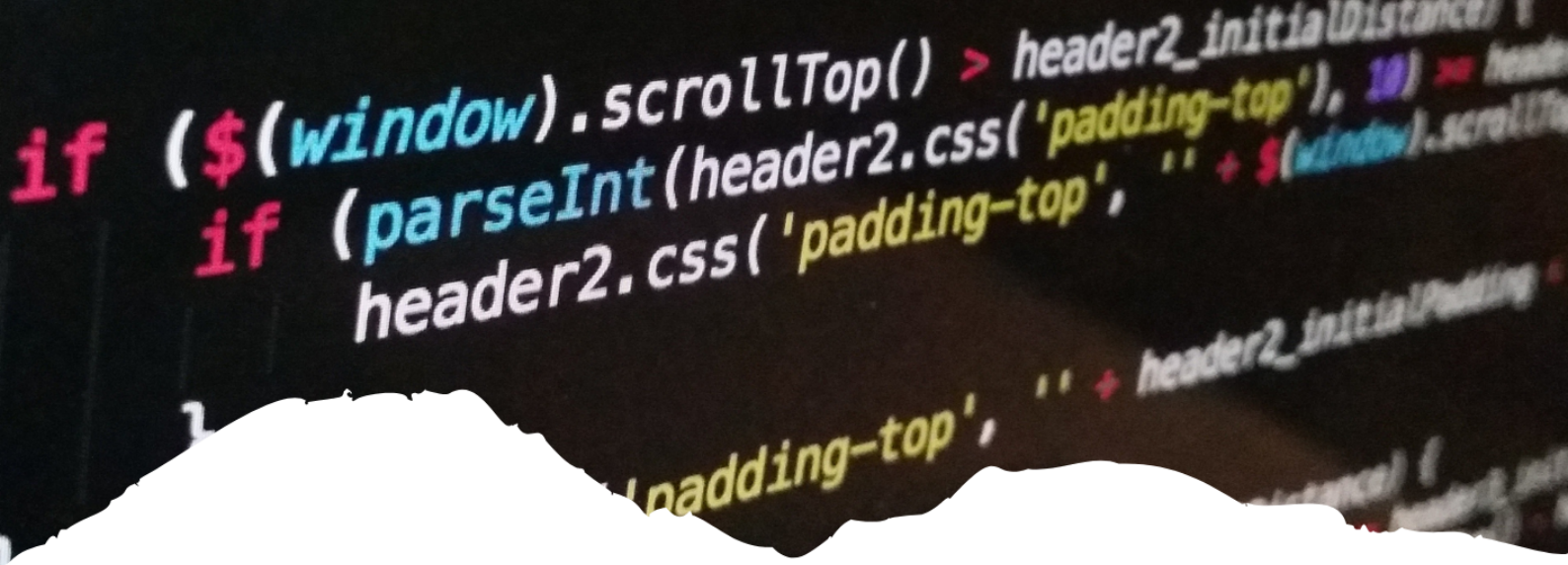
SOUSA, Flávio RC; MOREIRA, Leonardo O.; MACHADO, Javam C. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. **II Escola Regional de Computação Ceará, Maranhão e Piauí (ERCEMAPI)**, p. 150-175, 2019.

SOUZA, Mathias Rodrigues; OLIVEIRA, Taciano Balardin. ESTUDO DE CASO SOBRE SISTEMAS DE COMPUTAÇÃO EM NUVEM. **Revista da Mostra de Iniciação Científica e Extensão**, v. 5, n. 1, 2019.

TAMANAHA, Rodolfo Tsunetaka. **Tributação e economia digital: análise do tratamento tributário dos rendimentos da Computação em Nuvem**. 2020. Tese de Doutorado. Universidade de São Paulo.

TAURION, Cezar. **Cloud computing-computação em nuvem**. Brasport, 2019.

VIEIRA, Claudia S.; MEIRELES, F. S. Computação em Nuvem: Análise bibliométrica da produção científica sobre os fatores que influenciam as empresas no seu uso. **Revista Eletrônica Gestão e Serviços**, v. 6, n. 2, p. 1215-1230, 2022.



16

ARQUITETURA DE MICROSSERVIÇOS

MICROSSERVICES ARCHITECTURE

Rayllanderson Gonçalves Rodrigues

Resumo

A presente pesquisa apresenta uma revisão de literatura sobre a arquitetura de microsserviços, visa compreender os microsserviços para ajudar na tomada de decisão na escolha deles como arquitetura de software. Os microsserviços surgiram por meio de lições aprendidas de outras arquiteturas, eliminando muitos problemas de longa data no desenvolvimento de software. Para elaboração desse estudo foi utilizado a Pesquisa Bibliográfica como metodologia, viabilizando discussão sobre: histórico e conceitos da arquitetura de microsserviços; uma comparação com uma arquitetura muito conhecida e utilizada, a monolítica; e, por fim, as vantagens, desvantagens e casos de uso dos microsserviços. Assim, os resultados a pesquisa evidenciam que a arquitetura de microsserviços pode ser uma opção viável para tomada de decisão de arquitetura de software, por solucionarem diversos problemas dos desenvolvedores com outras arquiteturas, resultando em uma maior velocidade na entrega, com testes executados mais rapidamente, equipes trabalhando de forma paralela, maior diversidade de tecnologias e escalabilidade.

Palavras-chave: Microsserviços, Monolito, Arquitetura de microsserviços, Arquitetura monolítica

Abstract

The present research presents a literature review on microservices architecture, aims to understand microservices to help in decision making in choosing it as a software architecture. Microservices emerged through lessons learned from other architectures, eliminating many long-standing problems in software development. For the elaboration of this study, Bibliographic Research was used as a methodology, enabling discussion on: history and concepts of microservices architecture; a comparison with a well-known and used architecture, the monolith; and, finally, the advantages, disadvantages and use cases of microservices. Thus, the research results show that the microservices architecture can be a viable option for software architecture decision making, as they solve several problems of developers with other architectures, resulting in a greater speed in delivery, with tests executed faster, teams working in parallel, greater diversity of technologies and scalability.

Keywords: Microservices, Monolith, Microservices architecture, Monolithic architecture.

1. INTRODUÇÃO

É de conhecimento geral que os Microsserviços estão cada vez ganhando mais espaço no mercado de desenvolvimento para escolha de solução como arquitetura. Isso se dá devido a evolução de vários conceitos anteriores, como SOA (Service Oriented Architecture) e arquiteturas monolíticas, no qual diversas lições foram aprendidas, eliminando uma série de problemas de longa data no desenvolvimento de software. A ideia central por trás do Microsserviços, são aplicações que possuem poucas responsabilidades, transformando serviços grandes em serviços menores, cada um com sua própria responsabilidade, geralmente construídos em torno de regras de negócios, trazendo consigo uma ideia geral de concentrar-se em uma tarefa e fazer ela bem.

A presente pesquisa tem como tema Arquitetura de Microsserviços, sendo importante esse estudo para demonstrar seus benefícios, seus casos de uso, vantagens e desvantagens, que podem proporcionar uma melhor tomada de decisão ao escolher uma arquitetura durante o desenvolvimento de software. Torna-se relevante esta pesquisa, pois nem sempre o seu uso é adequado e o uso incorreto pode trazer uma série de problemas para os envolvidos. Por esse motivo, muitos se fecham para ela, buscando continuar na arquitetura que lhe é mais confortável, sem entender os casos de uso em que ela se encaixa e os benefícios que traz. Assim, a presente pesquisa visa responder o seguinte questionamento: quando utilizar a arquitetura de Microsserviços em meio a outras arquiteturas? Desse modo, temos como objetivo geral: compreender os Microsserviços para ajudar na tomada de decisão na escolha dela como arquitetura.

Para alcançarmos esse objetivo geral, temos os objetivos específicos: conceituar arquitetura de Microsserviço; comparar com a arquitetura Monolítica; apresentar vantagens, desvantagens e casos de uso dos Microsserviço diante de da arquitetura Monolítica. O tipo de pesquisa realizado neste trabalho, foi uma revisão de literatura, no qual foi realizada uma consulta a dissertações, sites e por artigos científicos selecionados através de busca nas seguintes bases de dados: “livros”, “sites acadêmicos”, “vídeos” etc. O Período dos artigos pesquisados foram os trabalhos publicados no período de 2014 a 2022. Os principais autores utilizados são: Martin 14 (2014), James (2014), Newman (2022). As palavras-chave utilizadas são: Microsserviços, Monolito, Arquitetura de microsserviços, Arquitetura monolítica.

2. CONCEITO DA ARQUITETURA DE MICROSSERVIÇOS

A arquitetura de Microsserviços vem ganhando cada vez mais espaço no mercado de desenvolvimento de software, mas esse termo não vem de hoje. Inicialmente, um dos primeiros autores a falar sobre o termo “Micro-Web-Service” foi Dr. Peter Rodgers em 2005 durante uma conferência de computação em nuvem, argumentando contra o pensamento tradicional de manter tudo em um único serviço e promoveu a componentização de software. O termo “Microsserviços” só apareceu um pouco mais tarde. De acordo com Habib (2016), “o termo microsserviços estreou em uma conferência de arquitetos de software na primavera de 2011”, e, segundo Miller (2015), “Google Inc., Amazon.com Inc. e Facebook Inc. administram microsserviços há mais de uma década”. Então, embora o termo “Microsserviços” tenha surgido por volta de 2011, a aplicação do conceito do Dr. Peter Rodgers, já vinha sendo usado desde 2005 e 2006 pelas grandes organizações.

No entanto, ainda existem desenvolvedores que continuam olhando com desprezo

para esse tipo de arquitetura. Na visão de Fowler e Lewis (2014), "[...] nossa inclinação natural seja ignorar essas coisas com um olhar de desprezo, esse pouco de terminologia descreve um estilo de sistemas de software que estamos achando cada vez mais atraentes." Isso se dá devido a diversas novas formas de produzir software que surgem a todo momento no mundo do desenvolvimento, tornando-se cada vez mais difícil acompanhar as tendências.

2.1 O que são os Microsserviços?

Mas, afinal, o que são os Microsserviços? Para a Amazon ([2022?]) "Microsserviços são uma abordagem arquitetônica e organizacional do desenvolvimento de software na qual o software consiste em pequenos serviços independentes que se comunicam usando APIs bem definidas" e, para Newman (2022), eles "[...] podem ser lançados de forma independente e são modelados com base em um domínio de negócios", e, então, "podemos desenvolver um único aplicativo como um conjunto de pequenos serviços, cada um executando seu próprio processo e se comunicando com mecanismos leves" (FOWLER; LEWIS, 2014).

A ideia central dos Microsserviços é transformar ou criar grandes aplicações por meio de pequenos serviços, cada um deles trabalhando de forma independente, com suas 16 respectivas responsabilidades, concentrando-se apenas em seu domínio, encapsulando seu próprio banco de dados, podendo ter sua própria stack de tecnologia, e possuindo seus objetivos bem definidos. Eles são tipicamente pequenos, porém, não há nada que implique que um microsserviço deva ser pequeno, por isso, não significa que cada microsserviço será um serviço pequeno sempre, apesar do nome.

Para a Amazon ([202?]), "se os desenvolvedores acrescentarem mais código a um serviço ao longo do tempo, aumentando sua complexidade, ele poderá ser dividido em serviços menores". Então, ele faz parte de um processo, um nível de evolução, e, isso quer dizer que, conforme as empresas vão crescendo ou lançando novas atualizações, esse microsserviço tende a ficar maior e seus objetivos definidos inicialmente pode começar a não fazer mais sentido e mudar esse objetivo definido inicial. Por isso que, quando isso acontece, esse microsserviço pode ser divido em dois ou mais serviços, separando-os baseados em responsabilidades diferentes, que, anteriormente, era tratada como uma única responsabilidade geral, garantindo que cada serviço seja responsável por apenas por um único contexto, uma única responsabilidade, seguindo o princípio de responsabilidade única.

2.2. Comunicação entre serviços

Os Microsserviços se concentram em suas responsabilidades, fazem parte de um ecossistema, de um domínio claro da aplicação, por isso, se comunicam o tempo todo com outros serviços, cada um deles pode hospedar uma funcionalidade de negócios em endpoints da rede, sejam eles APIs (Application Programming Interface) REST (Representational State Transfer) ou sistemas de mensageria como Apache Kafka ou Amazon SQS (Simple Queue Service). Os interessados nessas informações são conhecidos como consumidores, e "os consumidores, não importa se sejam outros microsserviços ou outros tipos de programas, acessam essas funcionalidades por meio desses endpoints na rede" (Newman, 2022), como observado na Figura 1:

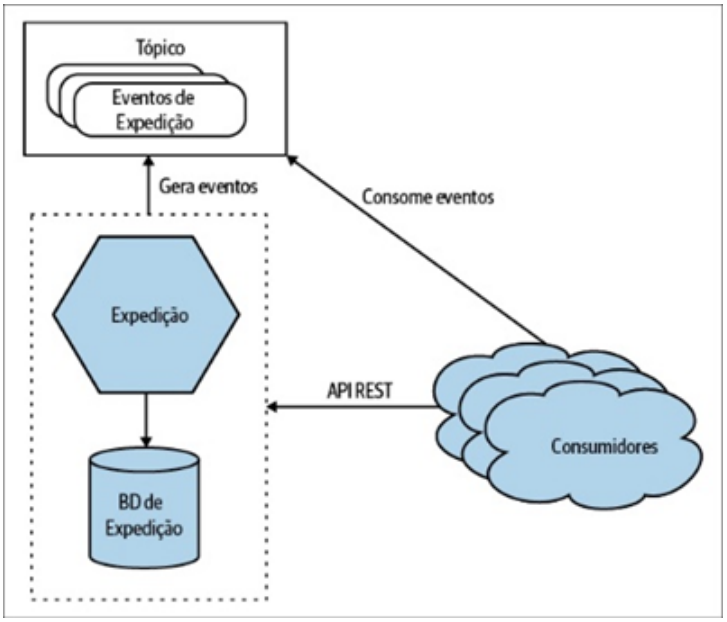


Figura 1 – Um microsserviço expondo sua funcionalidade por meio de uma API REST e um tópico

Fonte: Newman (2022)

Com a comunicação utilizando API REST entre serviços, é possível com que a resposta seja enviada de forma síncrona, ou seja, o consumidor envia sua solicitação ao microsserviço, espera ele aplicar a sua lógica e, assim que finaliza, retorna essa solicitação para o consumidor. Esse tipo de comunicação é conhecido como síncrono bloqueante e, para Newman (2022), devem ser usadas quando o resultado da solicitação é necessário para futuras operações. Por exemplo, um microsserviço chamado processador de compras, ao realizar uma compra, é necessário conferir o microsserviço de estoque para verificar se há estoque disponível para aquele produto antes de prosseguir, como mostra na Figura 2:

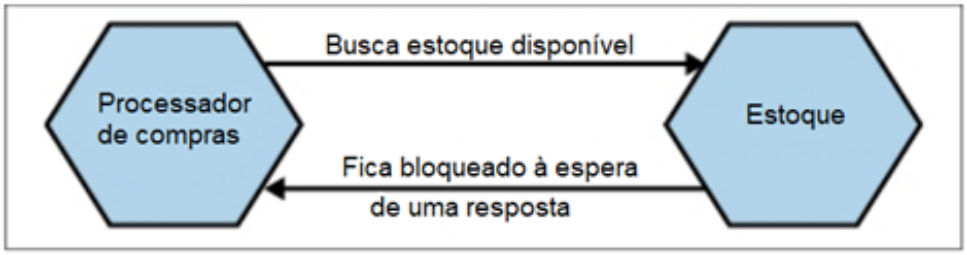


Figura 2 – Processador de compras fica bloqueado a espera de uma resposta

Fonte: Autoria própria

Se há estoque disponível, o microsserviço de processador de compras pode dar continuidade no processo. Se não há estoque disponível, ele não dá continuidade no processo, podendo retornar que não há estoque disponível para o cliente. É importante notar que o Processador de compras depende do microsserviço de Estoque, ele precisa estar disponível, caso contrário, o Processador de compras não irá conseguir prosseguir com nenhuma compra.

Já com a comunicação utilizando sistemas de mensageria, a resposta vem de forma assíncrona, então aqui o consumidor envia sua solicitação e ele não precisa esperar pelo retorno e nem ficar bloqueado operações subsequentes, ele é capaz de continuar essas operações. Esse tipo de comunicação é conhecido como assíncrono não bloqueante e, para Newman (2022), devem ser utilizadas quando não precisamos dos resultados da solicitação de forma imediata ou quando essa solicitação demorar muito para ser processada.

Então, por exemplo, Processador de compras concluiu uma compra e agora ele precisa enviar o produto para o cliente. Para fazer isso, ele precisa solicitar ao microsserviço de Estoque que faça isso, como mostra na Figura 3:

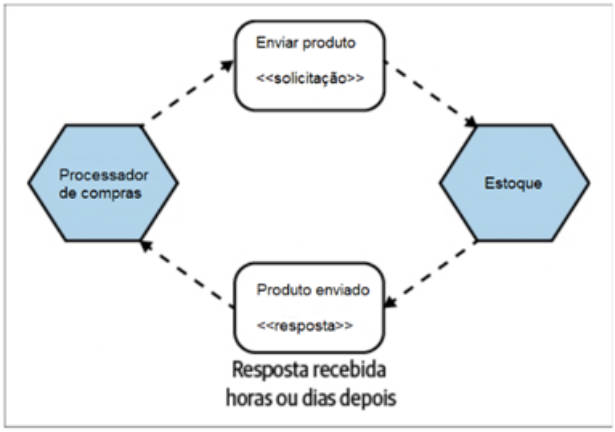


Figura 3 – Processador de compras inicia processo de enviar produto

Fonte: Autoria própria

Como o processo de enviar pedido pode levar dias ou horas, se a comunicação fosse síncrona bloqueante, o Processador de compras precisaria bloquear o processamento por esse mesmo tempo, impedido com que outros processamentos subsequentes fossem processados. É importante observar que utilizando comunicação assíncrona não bloqueante, o microsserviço de Estoque não precisa estar disponível quando o Processador de compras enviar a solicitação, já que a resposta não precisa vir de forma imediata, podendo receber essa mensagem quando tiver disponibilidade.

2.3 Ocultação de informações

Na visão de Newman (2022), os microsserviços, como o Processador de compras ou Estoque da Figura 3, devem ser tratados como uma caixa preta e os detalhes de como esse Microsserviço foi implementado não devem ser expostos e não deve interferir na regra de negócio, já que os microsserviços "[...] podem ser escritos em diferentes linguagens de programação e usar diferentes tecnologias de 20 armazenamento de dados" (FOWLER ; LEWIS, 2014).

Isso significar que, caso haja a necessidade futura desse Microsserviço alterar sua linguagem de programação, seu banco de dados ou framework, não deva influenciar na maneira de como os dados serão expostos para os consumidores, evitando a quebra de contrato ou incompatibilidade entre o serviço e os seus consumidores. É importante "Ter uma separação clara entre detalhes internos de implementação e o contrato externo de um microsserviço pode ajudar a reduzir a necessidade de mudanças que causem incompatibilidade com versões anteriores" (NEWMAN, 2022), pois, se esse contrato for quebrado, os consumidores terão que, obrigatoriamente, se adequar as mudanças e para se adequar a elas, é preciso tempo. "No entanto, às vezes, é necessário fazer alterações importantes e incompatíveis em uma API de serviço." (MICROSOFT, 2022). E quando alterações importantes e incompatíveis são lançadas, não há como forçar todos os consumidores a se adaptarem à mudança de forma imediata.

Por isso, na visão da Microsoft (2022), "[...] um serviço deve dar suporte a versões mais antigas da API por algum período. Se você estiver usando um mecanismo baseado em HTTP como REST, uma abordagem deverá inserir o número de versão da API na URL ou

no cabeçalho HTTP", deixando um serviço responsável pela versão antiga e outro serviço responsável pela nova versão, ou utilizar somente uma instância de serviço que mantém ambas as versões.

Para Amazon ([202?]) "Cada serviço do componente de uma arquitetura de microsserviços pode ser desenvolvido, implantado, operado e escalado sem afetar o funcionamento de outros serviços". Isso significa que os Microsserviços podem evoluir de forma independente, desde que os serviços honrem o contrato da API e utilizem versionamento em suas APIs para eventuais mudanças, buscando deixar suas fronteiras estáveis.

2.4 Organização em torno do negócio

Os Microsserviços têm como diretriz o Princípio da Responsabilidade Única, eles possuem um escopo de negócios limitado, por isso, para Fowler e Lewis (2014), eles também podem ser gerenciados por equipes diferentes, logo, ao trabalhar com uma arquitetura de Microsserviços, você pensa em outras equipes de desenvolvimento. "Isso permite que as equipes dimensionem corretamente as necessidades de infraestrutura, meçam com precisão o custo de um recurso e 21 mantenham a disponibilidade quando um serviço experimenta um pico de demanda." (Amazon, [202?]). Como cada equipe desenvolve sua unidade de software, "é possível desenvolver vários microsserviços ao mesmo tempo. Isso significa que você pode ter mais desenvolvedores trabalhando simultaneamente na mesma aplicação, o que resulta em menos tempo gasto com desenvolvimento." (RedHat, 2018). Com o tempo de desenvolvimento reduzido, a aplicação vai para o mercado mais rapidamente, permitindo que os usuários finais realizem testes na aplicação ou nas novas atualizações de maneira ágil.

2.5 Implantações independentes

A definição de Microsserviços, para Newman (2022) é que eles "são serviços que podem ser lançados de forma independente [...]", isso permite que o serviço seja testado de forma independente, porque "[...] podemos fazer uma alteração em um microsserviço, implantá-lo e disponibilizar essa alteração aos nossos usuários, sem ter de implantar outros microsserviços" (Newman, 2022), não tendo a necessidade de reconstruir a aplicação inteira a cada atualização lançada, facilitando teste de novas ideias ou um rollback caso ocorra algum problema durante essa atualização ou precise retornar a versão antiga. Para a Amazon ([202?]), isso "facilita a atualização do código e acelera o tempo de introdução de novos recursos no mercado". Portando, permitindo criar aplicativos mais confiáveis, com maior resiliência e melhor desempenho.

3. DIFERENÇAS ENTRE MONOLITOS E MICROSSERVIÇOS

Para entendermos melhor os Microsserviços, é importante entender o que são os Monolitos. Define-se "monolito" como "Monumento formado de uma única pedra" (MONOLITO, 2022), e essa definição não está longe da definição de uma arquitetura monolítica. Segundo a Google (2021), "Um aplicativo monolítico é um aplicativo de software de nível único em que módulos diferentes são combinados em um único programa." Um exemplo citado por Fowler e Lewis:

Aplicativos Corporativos geralmente são construídos em três partes principais: uma

interface de usuário do lado do cliente [...], um banco de dados [...] e um aplicativo do lado do servidor. O aplicativo do lado do servidor lidará com solicitações HTTP, executará lógica de domínio, recuperará e atualizará dados do banco de dados e selecionará e preencherá visualizações HTML a serem enviadas ao navegador. Este aplicativo do lado do servidor é um monólito - um único executável lógico. Quaisquer alterações no sistema envolvem a criação e implantação de uma nova versão do aplicativo do lado do servidor (FOWLER; LEWIS, 2014)

Então, um Monolito é a junção de toda aplicação e toda a sua lógica em um único serviço, compartilhando o mesmo banco de dados, sendo uma única unidade de implantação, fazendo com que seja necessário implantar toda a aplicação para que o sistema seja atualizado. Outras arquiteturas podem se encaixar nas definições apresentadas, mas quando é falado sobre Monolito, é discutido dois tipos com mais frequência: Os sistemas monolitos acoplados e os sistemas monolitos modulares.

Os sistemas monolitos acoplados são aqueles em que todo código da aplicação está em um único processo. Nesse tipo de monolito, nossas entidades se relacionam com toda a aplicação, não há divisão entre os componentes e eles estão muito conectados. Na visão de Willians (2022), "[...] a maior característica desse tipo de sistema é que os contextos delimitados (pensando em DDD: Domain-Driven Design) estão todos juntos. Ou seja, você não consegue definir direito quais são as partes do sistema porque tudo está conectado." Qualquer nova implementação corre-se o risco de ela influenciar diretamente outra parte da aplicação, tornando difícil a implementação de novas atualizações e testes, além de também ter que implantar toda a aplicação para cada nova atualização no sistema

Já os Sistemas monolíticos modulares, são "[...] uma variação na qual o processo único é composto de módulos separados. É possível trabalhar em cada módulo de forma independente, porém tudo precisa ser combinado para a implantação" (Newman 2022). Com os monolitos modulares, a aplicação é dividida por módulos, assim, sendo possível trabalhar em cada módulo de forma independente, permitindo equipes trabalharem de forma paralela, porém, assim como os Monolitos acoplados, a cada implantação, todas as dependências da nova atualização precisará ir junto, "A consequência disso é que as dependências ficam tão grandes que para o deploy de apenas um, você precisa fazer o deploy de outro" (Willians, 2022). Então, por exemplo, se o houver uma atualização no módulo de Pagamentos e essa atualização depender do módulo de Notificações, vai precisar combinar a implantação para subir os dois juntos, caso contrário, irá causar um grande problema de incompatibilidade. Portanto, toda implantação precisa ser combinada pelas equipes responsáveis por cada módulo.

3.1 Frustações dos Monolitos

Esses Monolitos podem ser bem-sucedidos, mas cada dia mais pessoas estão se frustrando com eles, porque um Monolito deve ser muito bem elaborado para crescer bem. Na opinião de Fowler e Lewis (2014), "a maneira lógica é projetar um monólito com cuidado, prestando atenção à modularidade dentro do software, tanto nos limites da API quanto em como os dados são armazenados." para que, dessa forma, quando esse monólito se tornar um problema, consiga migrar de Monolito para Microsserviço sem grandes esforços.

3.1.1 Implantações

Todavia, ainda com um Monolito bem estruturado, é difícil contornar situações como as implantações abordadas anteriormente. Para Fowler e Lewis (2014), “Os ciclos de mudança são vinculados - uma mudança feita em uma pequena parte do aplicativo requer que todo o monólito seja reconstruído e implantado”, além disso, por um monolito ser comumente grande, o tempo de início será maior, logo, as implantações serão mais demoradas. Já com os microsserviços, é possível ter implantações independentes, em que cada microsserviço será implantado individualmente, sem a necessidade de subir toda a aplicação junta. Além disso, eles tipicamente menores que os monolitos, portanto, seu tempo de início será menor.

3.1.2 Trabalho em equipe

Mesmo bem estruturado, com equipes grandes trabalhando em conjunto a todo momento nessa aplicação, fica difícil alterar apenas uma unidade do Monolito, fazendo com que essa alteração, que deveriam ser em apenas uma unidade, acabe afetando outras em que outros membros da equipe estão atuando. Com os microsserviços, segundo a Amazon, ([2022?]), “Os microsserviços promovem uma organização de equipes pequenas e independentes que são proprietárias de seus serviços”, por isso, esses conflitos entre equipes são menores, embora ainda existam dentro da própria equipe.

3.1.3 Confiabilidade

Como todos os módulos estão sendo executados no mesmo processo, um bug em qualquer módulo, como um Memory Leaks (vazamentos de memória), pode potencialmente derrubar todo o processo. Além disso, como todas as instâncias do aplicativo são idênticas, esse bug afetará a disponibilidade de todo o aplicativo. Isso influencia diretamente nos testes, pois, uma pequena alteração, pode afetar todo o sistema. Então, a cada nova atualização, é provável que precise fazer um extenso teste na aplicação, para garantir que tudo está funcionando normalmente, mesmo módulos que não foram alterados diretamente, visto que, todo a aplicação está diretamente ligada. Já “Com os microsserviços, os aplicativos lidam com a falha total do serviço degradando a funcionalidade, sem interromper todo o aplicativo”, (Amazon, [2022?]). Isso significa que os testes serão mais contextualizados e centralizados, testando apenas aquele serviço específico, sem precisar testar outros módulos como é no monolito.

3.1.4 Manutenibilidade

Na opinião de Camelo, (2020), “as aplicações monolíticas são excepcionalmente simples de manter no início. A base de código [...] é pequena, tudo está no mesmo lugar, é fácil fazer uma correção ou adicionar uma função. Mas, com o tempo, a base de código começa a aumentar [...]”. Ou seja, a aplicação vai se tornando cada vez maior, e o código presente vai ficando cada vez mais difícil de entender, por isso, fazer alterações simples e rápidas, levam mais tempo em um monolito grande. Já com os microsserviços, nem sempre eles serão pequenos, mas eles são especializados, o que significa que eles são dedicados à solução de um problema específico, que facilita o entendimento. Além de que eles podem ser divididos em outros serviços.

3.1.5 Escalabilidade

Utilizando uma aplicação monolítica, não é possível dimensionar componentes individuais, sendo assim, não podemos dimensionar uma função individualmente, é necessário que todo a aplicação seja dimensionada em conjunto. Por isso que, 27 segundo Camelo (2020), “Aplicações monolíticas têm facilidade de escala vertical, que consiste [...] em aumentarmos a capacidade do servidor onde está a aplicação. Então aumentamos a memória, o número de CPUs”, ou seja, a medida com que os acessos na aplicação vão crescendo, os monolitos tendem a escalar horizontalmente, mesmo que esses acessos sejam em apenas um módulo da aplicação. Já “Os microsserviços permitem que cada serviço seja escalado de forma independente para atender à demanda do recurso de aplicativo oferecido por esse serviço”, (Amazon, [2022?]). Portanto, se há um grande volume de acesso somente para um módulo específico, somente ele precisará ser escalado, e não mais a aplicação inteira.

4. AS VANTAGENS, DESVANTAGENS E CASOS DE USO DOS MICROSSERVIÇOS

É necessário entender muito bem os Microsserviços para ter ciência de quando utilizá-los, por isso, é importante ter conhecimento sólido a respeito do seu conceito, no qual irá demonstrar suas vantagens e desvantagens de acordo com o cenário na qual a aplicação se desenvolverá, ou, talvez, transformar um Monolito em Microsserviço.

4.1 Vantagens

Os Microsserviços possem uma grande variedade de vantagens. Newman (2022) acredita que muitas dessas vantagens podem ser atribuídas a qualquer sistema distribuído, porém, as vantagens para os microsserviços possuem um grau mais elevado, devido a combinação do conceito de ocultação de informações com a eficácia dos sistemas distribuídos, o que proporciona mais vantagens sobre qualquer outra arquitetura distribuída.

4.1.1 Diversidade de tecnologias

Com uma aplicação composta por vários microsserviços, é possível ter uma heterogeneidade de tecnologias maior, “Isso permite escolher a ferramenta correta para cada tarefa, em vez de selecionarmos uma única abordagem padronizada, que sirva para qualquer propósito [...]” (Newman, 2022). O que não seria tão fácil assim em uma arquitetura Monolítica, pois, se necessário realizar uma alteração de linguagem de programação, banco de dados ou framework em um Monolito, seria necessário um grande esforço porque mudanças como essas afetariam boa parte da aplicação.

4.1.2 Robustez

Sempre haverá a possibilidade de uma aplicação falhar. O hardware pode falhar. O software pode falhar devido, por exemplo, ao uso imprevisto ou dados corrompidos. Se um Monolito falhar, tudo para de funcionar, e, portanto, a aplicação fica indisponível. Para diminuir os impactos, comumente sobem várias máquinas e cada uma rodando a aplica-

ção, assim, se uma falhar, haverá outras prontas. Com os microsserviços é bem provável que ocorram falhas de comunicação com frequência devido à quantidade de comunicação com serviços externos. Por isso, os microsserviços são projetados para lidar com falhas, isolando o problema para que o resto do sistema continue funcionando. Além disso, pode-se criar outros microsserviços que saibam lidar com a falha de outros microsserviço. Por exemplo, 30 um serviço é responsável por debitar da conta do cliente, mas, após o débito, ele falha. Nesse momento, pode ser acionado um comportamento no sistema que faz com que outro serviço realize o estorno do débito para o cliente.

4.1.3 Escalabilidade

Se houver uma grande demanda para um módulo de um Monolito, vai ser necessário escalar todos os módulos juntos, mesmo que esse módulo seja o menor deles. Em uma aplicação desenvolvida com Microsserviços, é possível escalar apenas os serviços que precisam ser escalados. Richardson (2015) diz que, "Você pode implantar apenas o número de instâncias de cada serviço que satisfaça suas restrições de capacidade e disponibilidade. Além disso, você pode usar o hardware que melhor atende aos requisitos de recursos de um serviço", portanto, além de poder escalar somente os serviços que desejar, também é possível escolher um hardware menor, com menos desempenho, deixando a escalabilidade daquele serviço com menor custo.

4.1.4 Implantações com mais facilidade

As implantações são um problema para os Monolitos. Eles correm um grande risco a cada nova funcionalidade adicionada. Se essa nova funcionalidade vir a falhar, ela tem a capacidade de deixar todo o sistema fora do ar, por isso, que, na opinião de Newman: [...] implantações como essas acabam ocorrendo raramente em virtude de um temor compreensível. Infelizmente, isso significa que nossas alterações continuarão se acumulando entre as versões, até que a nova versão de nossa aplicação, a ser colocada no ambiente de produção, tenha um grande volume de alterações. E, quanto maior a diferença entre as versões, maior será o risco de haver algo errado! (NEWMAN, 2022, n.p.) Já com a arquitetura de Microsserviços, é possível que cada aplicação seja implantada de forma isolada, permitindo que atualizações sejam implantadas com mais rapidez, facilitando a adição de novas funcionalidades para o sistema. Em caso de uma dessas funcionalidade vir a falhar, o problema está isolado naquele serviço, e poderá reverter para versão anterior ou uma mais estável.

4.1.5 Facilidade no entendimento

Aplicações com arquitetura de Microsserviços englobam cada contexto de negócio em serviços específicos, consequentemente menores, permitindo que a compreensão do serviço e do código fiquem mais simples. Em uma aplicação monolítica, o código e o serviço enorme atrapalham os desenvolvedores mais novos na equipe e até mesmo os mais experientes, dificultando a manutenção e a inclusão de novas funcionalidades ao sistema. De acordo com Richardson (2015), "os serviços individuais são muito mais rápidos de desenvolver e muito mais fáceis de entender e manter." Nesse sentindo, ao desenvolver baseado em Microsserviços, novos membros na equipe devem se tornar rapidamente pro-

dutivos e o aplicativo deve ser fácil de entender e modificar.

4.2 Desvantagens

Apesar de solucionar diversos problemas de outras arquiteturas, a arquitetura de Microsserviços tem desvantagens e traz consigo diversas complexidades. É importante ter conhecimento sobre elas para que seja colocado em palta na escolha dos Microsserviços como tipo de arquitetura para a aplicação.

4.2.1 Comunicação entre as aplicações

Uma grande desvantagem é a complexibilidade pelo fato de os Microsserviços serem um serviço distribuído. É preciso escolher uma forma de comunicação entre as aplicações, como mensageria, protocolo HTTP ou RPC. Além disso, o desenvolvedor precisa estar preparado para lidar com possíveis problemas que podem vir a ocorrer durante a comunicação entre os Microsserviços, segundo Richardson (2015), “eles também devem escrever código para lidar com falhas parciais, pois o destino de uma solicitação pode estar lento ou indisponível.” Para os monolíticos isso não seria um problema, pois todos os módulos estão na mesma aplicação e para haver comunicação entre eles, é necessário apenas para chamar o outro módulo.

4.2.2 Latência

Em um Monolito, todas as execuções são efetuadas em um único processador, portanto, as informações fluem em um único processo. Já os Microsserviços, as informações fluem entre serviços por meio da rede. Essa é uma prática comum entre eles, constantemente um serviço precisa buscar informações em outros serviços. Isso significa que a latência aumenta em comparação com os Monolitos. Por isso, para Newman (2022), a recomendação é sempre avaliar o impacto dessa latência no sistema.

4.2.3 Testes

Outro grande problema são os testes. Para testar um fluxo fim a fim (teste End to End), é necessário que todos os Microsserviços da aplicação estejam disponíveis para teste, pois, se um desses serviços estiverem indisponíveis não há como realizar o teste, pois ele falhará. Portanto, não há como testar todo o fluxo sem aquele serviço específico. Para os monolíticos, todo o fluxo está presente na aplicação, então tudo estaria disponível.

4.3 Casos de uso

Embora seja uma ótima arquitetura, nem sempre seu uso é o ideal. Para adotar a arquitetura de Microsserviço, é preciso entender bem seu conceito e avaliar o contexto da aplicação. A decisão não deve ser tomada somente porque todos estão usando. Para Newman (2022), elas são mais uma abordagem de arquitetura e não a única abordagem. Uma arquitetura Monolítica pode suprir muito bem uma aplicação quando está começando a criá-la, principalmente para equipes pequenas. Construir uma aplicação como

Microsserviço para uma equipe pequena, na visão de Newman (2022), é um problema. Para ele, o problema é que essa nova aplicação não tem garantia de sucesso a ponto de ser altamente escalável e que o produto entregue não seja aquilo que se imaginou no início, fazendo com que passe por diversas mudanças, e, na opinião de Flower (2015), "refatoração de funcionalidade entre serviços é muito mais difícil do que em um monólito ". Por isso, Fowler (2015) defende que "você deve criar um novo aplicativo como um monólito inicialmente, mesmo que ache que é provável que ele se beneficie de uma arquitetura de microsserviços posteriormente", pois dessa forma, é possível lançar uma versão da aplicação de forma mais rápida, validando se a aplicação é útil ou não para os usuários. Pensando no caso de a aplicação ser bem-sucedida, uma abordagem comumente utilizada é começar a transformar o monolito em um microsserviço pelas bordas mais externas, por exemplo, separar o front-end do back-end, dividindo a camada de visualização da camada da lógica do negócio. Para Richardson:

Existem três estratégias que você pode usar: implementar novas funcionalidades como microsserviços; dividir os componentes de apresentação dos componentes de negócios e de acesso a dados; e converter os módulos existentes no monólito em serviços. (RICHARDSON, 2015).

Utilizando essas estratégias, a aplicação, que, inicialmente foi construída na arquitetura de monolitos, vai, aos poucos, se transformando em uma arquitetura de microsserviços, na qual desfrutará de suas vantagens, como flexibilidade nas escolhas de tecnologias, escalabilidade e robustez, mas, em contrapartida, é adicionado um grau de complexidade no sistema. Para Fowler (2015), os microsserviços "[...] são úteis com sistemas mais complexos" e a principal razão para grandes organizações utilizarem os microsserviços é para permitir que equipes trabalhem de forma paralela na mesma aplicação, sem ficarem uns nos caminhos dos outros. Na visão de Newman:

Uma empresa [..] com uma centena de pessoas, provavelmente achará que seu crescimento será muito mais fácil se ela tiver uma arquitetura de microsserviços devidamente alinhada com seus esforços de desenvolvimento de produtos. (NEWMAN, 2022, n.p.)

Quando há centenas de pessoas trabalhando em um mesmo sistema, as dores da arquitetura monolítica vêm à tona, tornando o trabalho dos desenvolvedores difícil. Seria viável uma grande organização com aplicação monolítica pensar em migrá-la para arquitetura de microsserviços, porém, ainda é preciso entender e analisar para que essa complexidade se justifique. Entendendo os conceitos e implementando eles em um cenário adequado, a arquitetura de microsserviço pode contribuir para construção de aplicações fortes, robustas e produtivas.

5. CONSIDERAÇÕES FINAIS

O presente estudo trouxe à tona o tema a arquitetura de microsserviços. Justificou-se o tema escolhido por nem sempre seu uso ser adequado e o uso incorreto pode trazer uma série de problemas para os envolvidos. Uma vez compreendido a arquitetura de microsserviços, é possível proporcionar tomadas de decisão assertivas acerca de arquiteturas de desenvolvimento de software.

Nessa perspectiva, a presente pesquisa buscou resposta para o seguinte problema: quando utilizar a arquitetura de Microsserviços em meio a outras arquiteturas? teve como objetivo compreender os microsserviços para ajudar na tomada de decisão na escolha dela como arquitetura. Para tanto, três capítulos descreveram um pouco sobre os conceitos da

arquitetura de microsserviço, a comparação dela com a arquitetura monolítica, vantagens e desvantagens e casos de uso dos microsserviço diante da arquitetura monolítica.

Sobre a arquitetura de microsserviço, surgiu por meio de dores de outras arquiteturas, que busca eliminar problemas de longa data no desenvolvimento de software. Pode parecer um termo atual e recente, mas para grandes empresas o seu uso já é usado antes mesmo do termo ficar conhecido. Os microsserviços se concentram em separar uma aplicação grande em pequenos serviços, fazendo com que eles se comuniquem através da rede, muito semelhante a um sistema distribuído.

Em relação a comparação entre os monolitos e os microsserviços, a discussão demonstra a diferença entre as duas arquiteturas, uma vez que os monolitos se concentram em manter tudo em um grande serviço, compartilhando o mesmo banco de dados e sendo uma única unidade de implantação, os microsserviços são o oposto, trazendo uma abordagem diferente de desenvolver softwares.

A respeito das vantagens, desvantagens e casos de uso, é demonstrado suas vantagens em contraste com a arquitetura monolítica, utilizando-se dos problemas que ela tem que são solucionados na arquitetura de microsserviço. Assim como suas desvantagens, que não estão presente na arquitetura monolítica. Por isso, é importante entender seus casos de uso, para que aplique a arquitetura de microsserviço de forma adequada.

Mediante ao estudo realizado, a arquitetura de microsserviços pode viabilizar um desenvolvimento de arquitetura de software de forma mais assertiva, deve-se 35 conhecer suas vantagens, desvantagens e casos de uso e levá-las em consideração ao escolher uma arquitetura de software para o sistema. A luz da teoria, exploradas na fundamentação teoria desta pesquisa bibliográfica, torna-se possível afirmar que os objetivos específicos e geral foram alcançados nesse estudo científico.

Por mais que tenham ficado explícitos os benefícios que os microsserviços podem proporcionar aos envolvidos no desenvolvimento de software, por meio deste estudo bibliográfico, é possível avançar em novos estudos. Dessa forma, como proposta para futuras pesquisas, sugere-se estudos mais aprofundados sobre: modelagem de microsserviços e seus tipos de acoplamentos; as principais tecnologias para comunicação entre os microsserviços; aspectos de segurança nos microsserviços.

Referências

AMAZON. **O que são microsserviços?**. [S. l.], [2022?]. Disponível em: https://aws.amazon.com/pt/microservices/. Acesso em: 18 nov. 2022.

CAMELO, Ricardo. **Monólitos, Serviços e Microsserviços: impactos nos negócios**. [S. l.], 30 nov. 2020. Disponível em: https://softdesign.com.br/blog/monolitos-servicos-e-microsservicos-impactos-nosnegocios/. Acesso em: 18 nov. 2022.

FOWLER, Martin. **MonolithFirst**. [S. l.], 3 jun. 2015. Disponível em: https://martinfowler.com/bliki/MonolithFirst.html. Acesso em: 29 abr. 2022.

GOOGLE. Introdução a microsserviços. [S. l.], 24 jun. 2021. Disponível em: https://cloud.google.com/architecture/microservices-architecture-introduction. Acesso em: 28 abr. 2022.

HABIB, Omed. **A Quick Primer on Microservices:** The post you've all been waiting for: a from-the-beginning explanation of what Microservices are and why you should care. [S. l.], 16 mar. 2016. Disponível em: https://dzone.com/articles/a-quick-primeron-microservices. Acesso em: 21 set. 2022.

LEWIS, James; FOWLER, Martin. **Microservices:** a definition of this new architectural term. [S. l.], 25 mar. 2014. Disponível em: https://martinfowler.com/articles/microservices.html. Acesso em: 29 abr. 2022.

MILLER, Matt. **Innovate or Die:** The Rise of Microservices. [S. l.], 5 out. 2015. Disponível em: https://www.wsj.

com/articles/BL-CIOB-8145. Acesso em: 21 set. 2022.

MICROSOFT. **Criando, evoluindo e fazendo o controle de versão de APIs e de contratos de microsserviços.** [S. l.], 22 set. 2022. Disponível em: https://learn.microsoft.com/pt-br/dotnet/architecture/microservices/architect- 37 microservice-container-applications/maintain-microservice-apis. Acesso em: 17 nov. 2022.

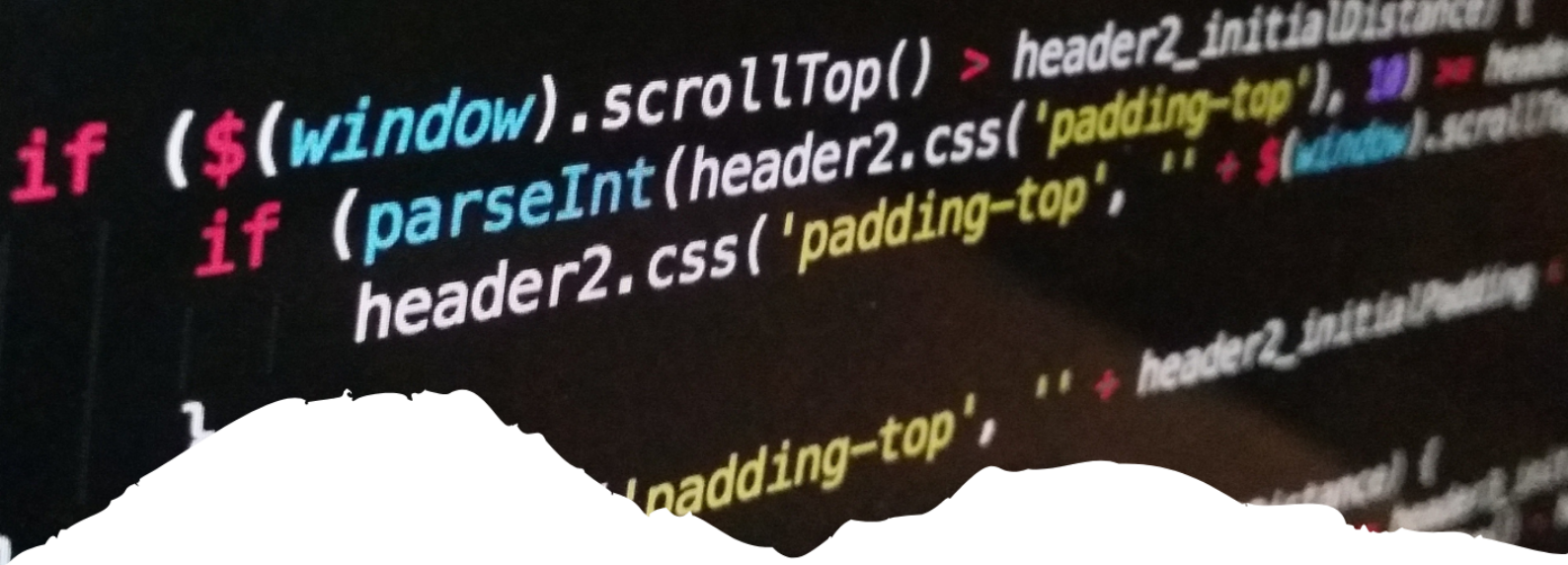
NEWMAN, Sam. **Criando Microsserviços:** Projetando sistemas com componentes menores e mais especializados. 2. ed. atual. [S. l.]: Novatec Editora, 2022. E-book.

REDHAT. **O que é arquitetura de microsserviços?**. [S. l.], 13 abr. 2018. Disponível em: https://www.redhat.com/pt-br/topics/microservices/what-are-microservices. Acesso em: 17 nov. 2022.

RICHARDSON, Chris. **Introduction to Microservices**. [S. l.], 19 maio 2015. Disponível em: https://www.nginx.com/blog/introduction-to-microservices. Acesso em: 30 abr. 2022.

RICHARDSON, Chris. **Refactoring a Monolith into Microservices**. [S. l.], 8 mar. 2016. Disponível em: https://www.nginx.com/blog/refactoring-a-monolith-intomicroservices. Acesso em: 29 abr. 2022.

WILLIANS, Wesley. **Os 4 tipos de Sistemas Monolíticos**. [S. l.], 30 jun. 2022. Disponível em: https://fullcycle.com.br/os-4-tipos-de-sistemas-monoliticos/. Acesso em: 17 nov. 2022



17

ENTRE REALIDADES: REALIDADE VIRTUAL X REALIDADE AUMENTADA

BETWEEN REALITIES: VIRTUAL REALITY X AUGMENTED REALITY

João Julio Lima Paixão

Resumo

A realidade virtual proporciona a experiência de um ambiente real num ambiente virtual, também é possível através da realidade virtual, fornece a cada usuário a inspiração e as ferramentas para ampliar sua forma de ver o mundo sem sair de determinada localidade. Com esse processo evolutivo de tecnologias, a realidade virtual apresenta uma gama de direções em que ela pode ser aplicada. Com o aumento de dispositivos que ofereçam uma melhor experiência virtual, seja essa experiência para o lazer ou para fins coorporativos, a realidade virtual pode vim a mudar parcialmente ou até mesmo completamente o atual modo de compreensão de relacionamentos e a compreensão de realidade. Este trabalho descreve conceitos de Realidade Virtual e Realidade Amentada, e mostra a utilização dessas tecnologias nos tempos atuais.

Palavras-chave: RA; AR; Virtualidade; virtual.

Abstract

Virtual reality provides the experience of a real environment in a virtual environment, it is also possible through virtual reality, provides each user with the inspiration and tools to broaden their view of the world without leaving a particular location. With this evolutionary process of technologies, virtual reality presents a range of directions in which it can be applied. With the rise of devices that offer a better virtual experience, whether for leisure or for corporate purposes, virtual reality may come to partially or even completely change the current way of understanding relationships and understanding reality. This paper describes concepts of Virtual Reality and Augmented Reality, and shows the use of these technologies in current times.

Keywords: RA; AR; Virtuality; Virtual.

1. INTRODUÇÃO

A Industria tecnológica está em uma crescente evolução exponencial, hoje a maioria das empresas dependem de sistemas computacionais. E inserida nesses sistemas computacionais, está a realidade virtual/aumentada. A realidade virtual/aumentada é responsável pela implantação de técnicas e ferramentas que possibilitam uma experiência mais otimizada para seu usuário; essa realidade virtual/aumentada pode ser implantada em diferentes áreas de aplicações como: sistemas de informações corporativos, publicidades, aplicações em telefones celulares etc.

A realidade virtual proporciona a experiência de um ambiente real num ambiente virtual, também é possível através da realidade virtual, fornece a cada usuário a inspiração e as ferramentas para ampliar sua forma de ver o mundo sem sair de determinada localidade.

Com esse processo evolutivo de tecnologias, a realidade virtual apresenta uma gama de direções em que ela pode ser aplicada. Com o aumento de dispositivos que ofereçam uma melhor experiência virtual, seja essa experiência para o lazer ou para fins coorporativos, a realidade virtual pode vir a mudar parcialmente ou até mesmo completamente o atual modo de compreensão de relacionamentos e a compreensão de realidade.

Este trabalho descreve conceitos de Realidade Virtual e Realidade Amentada, apresenta também suas possibilidades de utilização e mostra a utilização dessas tecnologias nos tempos atuais. E no capítulo três, é discutido os impactos que a tecnologia RV e RA pode vir a causar na formação das futuras gerações.

Para composição desse artigo, será realizado uma revisão bibliográfica em livros, artigos, e sites da internet, o período dos conteúdos explorados tendo sido publicado nos últimos trinta anos. A pesquisa será desenvolvida de maneira exploratória qualitativa, onde será feito um estudo profundo da utilização da Realidade Virtual e Aumentada, identificando e definindo suas principais características e benefícios, para a sociedade.

2. CONHECENDO A REALIDADE VIRTUAL

Realidade virtual é uma ferramenta tecnológica que se baseia em uma interface avançada entre um usuário e um sistema operacional. Tendo como objetivo recriar ao máximo a sensação que o usuário teria no mundo real, levando-o a validar essa interação como uma experiência de suas realidades temporais. Para isso, essa interação é realizada em tempo real, com o uso de técnicas e de equipamentos computacionais que ajudem na ampliação do sentimento de presença do usuário.

O termo “realidade virtual” foi cunhado em 1989 por Jaron Lanier, porém só se popularizou nos anos 90, graças ao avanço tecnológico que possibilitou a execução da computação gráfica interativa em tempo real.

Segundo Kirmer (2006) a Realidade Virtual (RV) é, antes de tudo, uma “interface avançada do usuário” para acessar aplicações executadas no computador, tendo como características a visualização de, e movimentação em, ambientes tridimensionais 3D em tempo real e a interação com elementos desse ambiente. Além da visualização em si a experiência do usuário de RV pode ser enriquecida pela estimulação dos demais sentidos como tato e audição. Para um melhor entendimento do que é RV é preciso entender os concei-

tos de interfaces.

2.1 Interfaces Gráficas

As interfaces permitem que computadores possam interagir com outras máquinas, da mesma forma que organismos interagem entre si e o ambiente. A evolução das interfaces visa fazer o homem interagir com a máquina de maneira mais natural possível. No domínio visual, a acuidade visual é tanta que se pode pensar em apagar a distinção entre o documento impresso e o manuscrito. No domínio sonoro, pode-se reproduzir vários sons digitalmente, além da síntese da voz que progride rapidamente. No domínio táctil, a sensação do toque é reforçada por aparatos como joysticks, alavancas de comando e controles manuais, ampliando assim a ilusão de realidade na interação com o mundo virtual.

As primeiras interfaces computacionais são datadas da década de 1940 e 1950, e essa interface era totalmente baseada em lâmpadas e válvulas, pois eles pertenciam ao primeiro computador conhecido como ENIAC. O ENIAC pesava cerca de 27 toneladas e media 5,50 x 24,40 metros, com duas mil válvulas e consumia cerca de 150W.

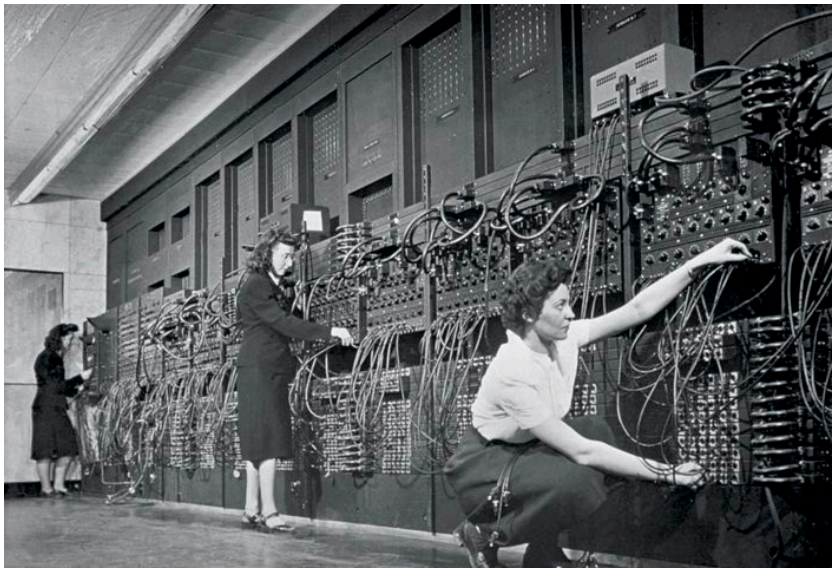


Figura 01: Computador ENIAC – 1940s

Fonte: Disponível em < www.ufrgs.br/enigma/2018/08/09/mulheres-da-computacao-as-mulheres-do-eniac >

No ano de 1962, Morton Helig patentiou uma máquina batizada de Sensorama com a finalidade de atuar na Industria do Entretenimento. Essa máquina em formato de cabine que se utilizava de vibrações mecânicas, ventiladores de aromas e um dispositivo que permitia a visão estereoscópica.

Embora todos esses conjuntos de dispositivos que faziam parte do Sensorama, proporcionar-se ao usuário uma sensação de imersão quase perfeita, Sensorama não foi um sucesso comercial.

Figura 02: Sensorama – 1962

Fonte: Disponível em < www.engadget.com/2014/02/16/morton-heiligs-sensorama-simulator >

Até os anos de 1980, os dispositivos e tecnologias eram exclusivamente feitos com objetivos militares. Em 1986 a NASA - National Aeronautics and Space Administration já possuía um ambiente virtual que simulava condições de voo onde seus pilotos podiam treinar, onde se utilizava uma luva chamada de "DataGlove" que possibilitava a manipulação de objetos virtuais por movimentos da mão.

Com o passar dos anos e a chegada do Windows, mesmo ainda restrito à limitação de tela de monitor e ao uso de representações como menus e ícones, tornou-se um diferencial em termos de interface. Houve também o surgimento das novas interfaces com a de voz, interfaces tangíveis, interfaces hápticas (joysticks) e outras mais, possibilitaram ao usuário acessar aplicações com a naturalidade de atuação do mundo real, melhorando a interação entre homem e computador.

A Realidade Virtual, então se consolidava como uma interface avançada, pois enquanto introduzia representações tridimensionais mais próximas ao mundo real do usuário, rompia também com as limitações da tela e prometia uma interação mais intuitiva.

Segundo Sherman (2003), para que a Realidade Virtual possa ocorrer, são necessários seguir três características que são fundamentais, são elas: imersão, interação e envolvimento.

A imersão é a responsável por fazer com que o usuário se sinta ativo dentro de determinado ambiente virtual. Para isso, imersão se utiliza dos sentidos de visão, audição e tato, que são mediados por um sistema inteligente.

Já a interação acontece quando o usuário consegue modificar o ambiente virtual instantaneamente, com a ajuda de dispositivos eletrônicos que permitem o usuário executar ações no ambiente virtual.

E o envolvimento é o grau de imersão que o usuário tem, ao se ver dentro do ambiente virtual. Com a ajuda dos dispositivos eletrônicos multissensoriais, que faz com que a interação com o computador seja satisfatória. Quanto maior o grau de envolvimento melhor será a interação entre homem e computador.

De acordo com Utiyama (2006), o conceito de Realidade Virtual dado por SHERMAN

(2003), seria melhor entendida como um meio composto de simulações que interagem com o usuário, respondendo ao diferente ao usuário, dependendo de cada ação do mesmo. Dando assim uma sensação de imersão mental ao usuário dentro da simulação.

Existem dois tipos de RV, são elas: a imersiva e a não imersiva, de acordo com Utiyama (2006), o usuário precisa vestir um conjunto de dispositivos tecnológicos, tais como: capacetes, fone de ouvido, luvas e rastreadores de posições, que farão com que o usuário seja "desligado" do mundo real, proporcionando o usuário vivenciar e sentir os estímulos gerados pelo sistema de simulação computacional. Já a Realidade Virtual não imersiva, é aquela onde o usuário vê o ambiente virtual por meio de um monitor projetado ou tela convencional de um computador.

> A interação do usuário com o ambiente virtual é um dos aspectos importantes da interface e está relacionada com a capacidade do computador detectar e reagir às ações do usuário, promovendo alterações na aplicação (BOWMAN, 2005 apud KIRNER; SISCOUTTO, 2007, p. 07)

Um bom exemplo de Realidade Virtual não imersiva, são os jogos eletrônicos, que apesar de usarem dispositivos de interação como luvas eletrônicas que captam os movimentos e em alguns casos, óculos de visão estereoscópica, o usuário ainda deve fixar o olhar no monitor para ver o ambiente virtual.

2.2 Dispositivos de interação

Dispositivos de interação foram feitos na tentativa de fazer com que o usuário se sinta imerso e consiga interagir com um ambiente virtual.

Eles são:

- DataGlove – DataGlover é uma luva de dados que é recoberta de captadores. Essa luva fornece informações, através de fibras ópticas, ao computador;

Figura 03: DataGlover - 2010

Fonte: Disponível em < http://rsinformaticas.blogspot.com/2010/10/luvas-de-dados-dataglove-atraves-das.html >

- Capacete de Visão – Esse dispositivo funciona melhor que os monitores, pois ele oferece a possível aparência de uma cena tridimensional.

Figura 04: Capacete usado para Realidade Virtual - 2016

Fonte: Disponível em < www.techtudo.com.br/listas/noticia/2016/03/oculos-de-realidade-virtual-tudo-que-voce-precisa-saber-antes-de-comprar.html >

- Joysticks – É um dispositivo háptico que permite a interação, muito usado em videogames.

Figura 05: Joystick - 2010

Fonte: Disponível em < www.google.com.br/imagens de joystick/p.01 >

- DataSuit – É uma roupa feito com captadores que utiliza todas as informações do corpo e envia ao computador.

Figura 06: DataSuit - 2014

Fonte: Disponível em < www.google.com.br/imagens de datasuit/p.01>

Embora, com a ajuda dos dispositivos de interação eletrônicos, a realidade virtual teve um avanço, fazendo a interação ser melhorada, ainda sim os equipamentos traziam um desconforto ao usuário, o que prejudicou a RV se tornar popular entre seus usuários.

3. REALIDADE AUMENTADA

Realidade Aumentada, o nome pode parecer meio técnico ou mesmo distante do dia-a-dia, mas na prática esse tipo de tecnologia pode estar disponível no seu aparelho celular ou no seu tablete por exemplo, na área da educação, medicina entre outras áreas, essa tecnologia tem potencial para revolucionar as formas de trabalhos, de profissionais como professores, médicos e também abre novas possibilidades para os estudantes em diferentes fases de ensino.

Essencialmente a Realidade Aumentada se originou de algo muito simples, as etiquetas. Os códigos de barras não estavam mais realizando totalmente as tarefas de carregar todas as informações que se queria obter através de sua leitura, por esta razão foram criados os códigos 2D, que por sua vez, permitiam o armazenamento de muito mais informações do que os códigos de barra. Os códigos bidimensionais são os responsáveis pela possibilidade de projetar objetos virtuais em uma gravação no mundo real, melhorando as informações exibidas, expandindo as fronteiras da interatividade e até possibilitando que novas tecnologias sejam utilizadas.

A realidade aumentada surge nesse conceito de sobreposições de imagens virtuais em cima de elementos reais, e ela se expande para convergência de o que é interface, de como pode interagir com o conhecimento digital, informação digital, com esse mundo de possibilidades de informações que existem e poderão existir, e traz também a possibilidade de hoje entender que sendo uma maneira de interagir interface, se mistura com outros conceitos como: controles, Big Data, simulações, leitura de informações e etc; então pode ser analisado como uma maneira de formar capacidades técnicas e formar conhecimento.

3.1 Conceitos

A Realidade Aumentada (RA), é definida de muitas maneiras. De acordo com o psicólogo, *Stanley Milgram em 1994,* a Realidade Aumentada é uma mistura entre os mundos reais e virtuais, que em algum ponto conecta ambientes completamente reais a ambientes completamente virtuais.

Já em 2001, o cientista Ronald Azuma definiu Realidade Aumentada como sistema que suplementa o mundo real com objetos virtuais que são gerados por um computador, fazendo parecer que o objeto virtual coexista no mundo real.

O sistema de realidade aumentada é uma combinação da visão do ambiente real com o ambiente e na maioria das vezes, utiliza óculos ou capacete com visor semitransparente, de forma que a visão do ambiente real possa ser sobreposta com a informação do ambiente virtual. Também é possível coletar a imagem real com uma câmera de vídeo e misturá-la com a imagem virtual antes de ser apresentada. Um sistema típico de realidade aumentada baseado em vídeo é composto de um capacete de visualização com sistema de rastreamento de posição, sobre o qual é disposta uma câmera de vídeo. Nesse caso, a imagem real é obtida pela câmera de vídeo montada sobre o capacete, enquanto a imagem virtual é gerada por um computador que considera o posicionamento do rastreador. Um misturador combina as duas imagens e mostra o resultado final ao usuário (VENTURELLI, 2007, p. 03).

A Realidade Aumentada enriquece a cena do mundo real com objetos virtuais, enquanto a Realidade Virtual é por sua vez totalmente gerada por computador (BIMBER, 2004).

3.2 Sistemas de RA

Os sistemas são classificados pela forma de como a realidade aumentada é visualizada. Os sistemas são baseados em diferentes sentidos da percepção: audição, visão ou toque.

3.2.1 Sistemas RA de Usuário Único

Os dispositivos utilizados também são muito variados: podem ser capacete semi-transparente, computadores de mão ou projeção dedados em objetos reais.

Museu Aumentado

Apresentado por [REKIMOTO 95] como um aplicativo da Sony NavyCam, o Augmented Museum exibe dados em um capacete semi-transparente usado por um visitante em um museu. O sistema é baseado na leitura de um código de barras organizado em um canto da obra, o que implica a exibição de dados textuais no capacete. Estes dados são relativos à tabela que o usuário está contemplando e se relaciona com o autor da obra ou as características técnicas da pintura. Os dados são configuráveis pelo usuário, ou seja, ele pode escolher o tipo de exibição de acordo com seus conhecimentos e interesses. A qualquer momento durante a visita, o usuário vê os trabalhos reais, além de dados adicionais, exibido no fone de ouvido e retornado pelo computador. Além da fase de configuração do sistema, a interação entre o usuário e o sistema é totalmente transparente para os visitantes.

O sistema RAC: Realidade Aumentada para Construção

Também com base no uso de um fone de ouvido semitransparente, este sistema apresentado por [Webster 96], visa simplificar um trabalho de montagem. Para ter em conta as características físicas e técnicas diferentes e respeitar os planos de projeto da estrutura geral, o RAC fornece ao usuário dados que facilitam a estrutura. Esses dados são de dois tipos: textuais e gráficos. Para coletar esses dados, o usuário usa um capacete semi-transparente. Dados gráficos exibidos são justapostos exatamente com a parte da estrutura já em vigor, a fim de mostrar o usuário como posicionar o novo elemento em relação às partes da estrutura já está no lugar. De fato, o usuário e a estrutur são rastreados por câmera, ou mais geralmente por um localizador. Este localizador transmite esses dados para o sistema computador que pode atualizar os dados exibidos no capacete semitransparente. O elemento real não é não visível porque ainda não está presente no campo de visão do usuário.

Uma vez que o elemento da estrutura esteja corretamente posicionado, o usuário informa sistema digitalizando um código de barras conectado a esse elemento. O uso do scanner constitui por um lado, a única maneira de identificar com precisão o elemento que acaba de ser materializa, assim, o fim da tarefa de reunir esse elemento com o restante da estrutura. O sistema pode atualizar os dados exibidos no fone de ouvido indicando o número e a posição do próximo elemento, ou mais geralmente a próximo tarefa a realizar. Outra versão deste sistema implementa outro meio: dados de som transmitidos através de um fone de ouvido estéreo ao usuário.

3.2.2 Sistemas RA Multiusuário

Os Sistemas Multiusuário são mais comumente referidos como sistemas colaborativos.

Segundo Ellis (1991), a distinção de situações colaborativas é geralmente em um esquema de classificação clássico. Este esquema caracteriza uma interação colaborativa e gira em torno de dois eixos: espaço e tempo. O primeiro eixo, o espaço, destaca dois tipos de interações relacionadas à situação de o usuário em relação ao sistema: portanto, fala-se de interação local ou remota. O segundo eixo, tempo, identifica a natureza síncrona ou assíncrona da interação de cada usuário com o sistema. No caso de sistemas RA, outra distância é levar em consideração: a distância dos usuários do objeto da tarefa, ou seja, o ambiente físico em que a tarefa é realizada.

O jogo Mah-Jong e o Sistema CAVE

O jogo de Mah-Jong (Szalavari 98) ilustra a mais recente classe de sistemas RA colaborativo (Renevier 01), reunindo sistemas nos quais todos os usuários são reunidos em torno do objeto da tarefa. Este sistema usa capacetes semitransparentes e consiste em uma mesa de jogo na qual os jogadores devem cair por sua vez combinação de “dominós” virtuais. A tabela, bem como as combinações virtuais já portanto, são comuns a todos, mas seus “dominós” e as combinações que preparar, deve permanecer oculto de outros jogadores: eles são perceptíveis no nível de um PIP (Personal Interaction Panel) por meio de fones de ouvido semi-transparente, conforme ilustrado na figura 07. Através do capacete, o usuário pode, portanto, veja o tabuleiro de jogo comum com as combinações virtuais já depositadas, bem como sua área de jogo particular, onde estão seus dominós e as combinações que ele é preparando. A manipulação de dominós virtuais no espaço privado de todos ou na mesa de jogo é conseguida através do uso de caneta manchada no espaço por um localizador magnético. Este sistema possibilita, portanto, implementar uma atividade colaborativo usando o princípio de realidade aumentada no tabuleiro de jogo comum.

Figura 07: Visão do capacete de um dos jogadores de Mah-Jongg - 2009

Fonte: Disponível em < www.google.com.br/imagens de jogadores mah jongg/p.11 >

Sistema baseado em Smartphones

Também é possível usar o telefone celular, a maioria dos smartphones atuais já vem com um aplicativo responsável por leitura de QR Code. Caso o smartphone não tenha o leitor de QR Code, é possível instalar o aplicativo em um celular com câmera digital que é acionado através do código de barras do QR Code (Quick Response Code), a tradução literal é código de resposta rápida, a imagem aparece na tela do celular.

Figura 8: Piano sobre marcador - 2013

Fonte: Disponível em < www.google.com.br/imagens de qr code piano praia/p.05 >

3.3 Vantagens e desvantagens

No caso do museu aumentado, acréscimos de textos e dados adicionais para

a cena real coloca firmemente este sistema em realidade aumentada, considerando as primeiras abordagens ao campo das Interação Homem - Máquina apresentadas (Feiner 93), (Webster 97), (Azuma97).

Do ponto de vista da abordagem de (Mackay 96), o uso do capacete semitransparente "aumenta" o usuário, assim como o código de barras "aumenta" a obra de arte.

Por duas razões diferentes, uma perceptiva e outra mais baseada em hardware, essas abordagens consideram esse sistema como parte do RA.

Se olhar para o sistema RAC, a diferença nos aspectos levados em consideração pelas abordagens de caracterização de AR é mais flagrante.

Assim como para o sistema anterior, a exibição de gráficos adicionais permite qualificar esse sistema de Sistema RA (Feiner 93), (Webster 97), (Azuma 97).

RAC reduz claramente o abismo entre o manual de construção e o real, ilustrando as abordagens para caracterização introduzida por (Rekimoto 95) e (Ahlers97).

Finalmente, a abordagem de identificação o candidato a aumentar (Mackay 96) estabelece que o usuário é aumentado em um o capacete semi-transparente.

Portanto, como antes, esse sistema aparece como sendo RA, por razões de percepção ou materiais, de acordo com a abordagem considerado. Mas a diferença na análise não para por aí. Ser capaz de fornecer os dados corretos ao usuário, dependendo dos elementos manipulados, o sistema depende do usuário: ele deve identificar o elemento da estrutura usando um leitor de código de barras.

Figura 09: QR Code - 2018

Fonte: Disponível em < www.google.com.br/imagens de q code/p.01 >

4. ONDE ESTÁ A RV/RA?

Com a popularização dos smartphones entre as pessoas nos últimos anos, viu-se a oportunidade da RA se estabelecer no mercado. Quando a câmera do aparelho celular é direcionada a um objeto com logos ou formas que a RA é capaz de reconhecer, tais elementos são substituídos por gráficos 3D enquanto todo o resto do mundo real permanece igual. O aparelho do telefone celular se torna a principal interface da RA móvel.

4.1 Na Educação

RA é uma tecnologia muito eficiente para a área da educação em geral. Os alunos podem melhorar seus conhecimentos e habilidades, se utilizando da RA. Por exemplo: na análise de objetos em 3D, na engenharia civil.

De acordo com Tim Cook (2016)[1], a AR certamente mudará para sempre a maneira como os usuários usam a tecnologia e transformará a maneira como lemos, jogamos e experimentamos as coisas ao nosso redor.

As crianças pequenas costumam fantasiar sobre serem engolidas pelas páginas de um conto de fadas e se tornar parte da história.

O MagicBook torna essa fantasia uma realidade, usando um livro normal como objeto principal da interface.

As pessoas podem virar as páginas do livro, olhar as figuras e ler o texto sem nenhuma tecnologia adicional (figura 10a). No entanto, se olharem para as páginas por meio de uma tela de Realidade Aumentada portátil, eles verão modelos virtuais tridimensionais aparecendo fora das páginas (figura 10b). Os modelos aparecem anexados à página real, para que os usuários possam ver a cena da realidade aumentada de qualquer perspectiva simplesmente movendo a si mesmos ou ao livro.

Os modelos podem ter qualquer tamanho e também são animados; portanto, a exibição de RA é uma versão aprimorada de um livro “pop-up” tridimensional tradicional. Os usuários podem alterar os modelos virtuais simplesmente virando as páginas do livro. Quando eles veem uma cena da qual gostam particularmente, podem voar para a página e experimentar a história como um ambiente virtual imersivo (figura 10c). Na visão RV, eles são livres para mover-se pela cena à vontade e interagir com os personagens da história. Assim, os usuários podem experimentar o continuum Realidade-Virtualidade completo.

Figura 10: Magic Book – Realidade (10ba) – Realidade Aumentada (10b) – Imersão Realidade Virtual (10c) - 2004

Fonte: Disponível em < www.google.com.br/imagens de magicbook_imer/p.01 >

1 CEO Apple Inc. na Utah’s Tech Tour 2016. Para mais esclarecimento acessar: https://www.youtube.com/watch?-v=DyjpQT-iXAI, visualizado em 15/11/2022.

4.2 Na medicina

Embora o potencial da realidade virtual para o treinamento de procedimentos médicos seja amplamente reconhecido e buscado, o uso da realidade aumentada para fins de ensino na área da saúde ainda está engatinhando. A maioria das pesquisas tem como objetivo usar a tecnologia de realidade aumentada para navegação cirúrgica intra-operatória intuitiva, mesclando o realce na operacional com órgãos virtuais segmentados a partir de dados radiológicos pré-operatórios.

Além disso, todos esses projetos estão limitados à fusão de dados visuais com o mundo real.

4.3 No entretenimento

Em um período relativamente curto, os smartphones transformaram os hábitos e o comportamento de busca de informações dos usuários de celulares. Com os smartphones, pessoas de todo o mundo são capazes de incorporar o poder da computação moderna em muitos aspectos de suas vidas diárias. Agora, para expandir esse poder, as empresas estão investindo em tecnologia vestível que alterará drasticamente o escopo de onde e como os computadores podem ser usados. Esses dispositivos, comumente conhecidos como wearables, existem há algum tempo, mas ainda precisam ser totalmente integrados ao cotidiano da maioria das pessoas.

4.3.1 Games

Jogos físicos podem adicionar camadas inteiras de complexidade, de jogos de cartas e tabuleiros mais antigos a jogos de RPG de mesa, como Dungeons and Dragons e Warhammer. Os aplicativos de realidade aumentada podem ser criados para revitalizar jogos antigos que ainda não haviam sido criados com essa tecnologia, mas ainda assim poderiam se beneficiar da realidade aumentada.

Na maioria dos jogos de realidade aumentada, a jogabilidade ocorre no mundo real com objetos virtuais e personagens acionados por geolocalização ou marcadores especiais, como códigos QR, como o jogo Pokemon Go.

O jogo foi elogiado por aumentar a atividade física nas pessoas — realmente tem que se movimentar para encontrar seus Pokémons.

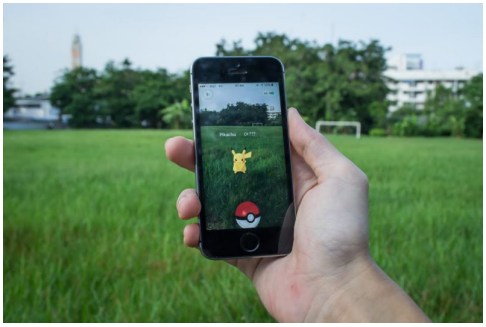


Figura 11: RA em games - 2018

Fonte: Disponível em < www.google.com.br/imagens de pokemongo/p.03 >

4.3.2 INSTAGRAM / SNAPCHAT

Os “filtros de rosto” de RA - uma realidade aumentada em forma de máscara que adiciona objetos virtuais ao rosto de um indivíduo - tornaram-se muito populares no Instagram, Snapchat e até vídeo chamadas no Face Time. Mas pouca atenção tem sido dada aos filtros de rosto como arte de RA. Muitas vezes vistos como brincadeiras, os filtros de rosto RA podem proporcionar uma experiência artística envolvente e pessoal.

Os filtros de rosto funcionam detectando a imagem de um rosto e sobrepondo elementos virtuais a esse rosto via RA. Todo o procedimento acontece instantaneamente e um novo retrato é produzido. Quando o sujeito gira a cabeça ou faz diferentes expressões faciais, ele ativa a experiência de RA. O usuário pode ativar alguns filtros de rosto tocando ou pressionando e segurando a tela. Essas ações podem acionar diferentes animações ou objetos para aparecer.

Os filtros de face RA permitem que os usuários experimentem inúmeras possibilidades físicas que são impossíveis na vida cotidiana. A RA permite que uma pessoa faça mudanças drásticas em sua aparência sem nenhuma permanência ou repercussão. Isso é diferente da ilustração tradicional, pois é imediata, reversível e facilmente compartilhada.

Figura 12: Filtro RA Instagram – 2019

Fonte: Disponível em < www.google.com.br/instagram_filtros/p.21 >

4.3.3 TV Shows/Filmes

Não há limite real para o que a realidade aumentada pode fazer para aprimorar as formas de entretenimento existentes.

Aplicativos e hardware de realidade aumentada permitirão que filmes e programas de TV se tornem mais imersivos de maneiras que os óculos 3D só poderiam sonhar em imitar. A realidade aumentada pode ser usada para trazer os filmes totalmente para fora da tela, estendendo a história visual para o “mundo real” pela primeira vez.

Mais perto de casa, a realidade aumentada pode ser usada como uma maneira de interagir com a mídia existente de maneiras novas e empolgantes. Menus e controles podem ser integrados em algum hardware bastante padrão, como óculos de realidade aumentada, que podem permitir o controle de menus usando a tecnologia simples de rastreamento ocular que já existe.

Filmes e programas de TV estrangeiros também podem receber legendas em tempo real, sem a necessidade de encontrar versões com legendas especiais, oferecendo aos filmes e programas de TV estrangeiros um alcance maior do que eles poderiam ter. Filmes interativos e programas de TV mais recentes, como o recente sucesso da Netflix, Black Mirror e Bandersnatch, poderiam aproveitar os óculos de realidade aumentada para fazer

escolhas de histórias muito mais perfeitas do que já são.

5. CONSIDERAÇÕES FINAIS

Atualmente o futuro da RA é mais promissor quando comparado a RV, porém isso se deve a tecnologia disponível hoje.

O futuro da RA como uma tecnologia de visualização parece brilhante, como mostra o interesse gerado nos círculos comerciais e industriais também como discutido em periódicos populares e pesquisas trabalhos nas áreas de educação e entretenimento. Muitas questões ainda permanecem em termos de eficiência e quando comparados aos métodos tradicionais, principalmente devido aos investimentos necessários em pesquisa e design. No entanto, há muito otimismo de RA na educação e formação para o futuro.

Pode dizer que na área da educação mesmo a leitura de um livro ou revista pode se beneficiar da realidade aumentada por conteúdo multimídia integrado na página física do livro ou revista usando óculos de leitura de realidade aumentada. Por fim, não há como dizer qual é o limite quando se trata de aplicativos de realidade aumentada e as novas inovações em realidade aumentada prometem uma ideia totalmente nova do que o entretenimento pode ser.

A Realidade Aumentada tem potencial de tornar os displays de televisão atuais um artefato de museu. Se é possível ter uma tela virtual onde pode ter um display com o tamanho que o usuário quer, por que precisá-la? Quando os telespectadores começarem a consumir televisão habilitada para RA, as emissoras e os proprietários de conteúdo perceberão que não estão mais limitados a uma forma retangular plana e criarão novas técnicas inovadoras de contar histórias para nos divertir.

Deve haver poucas dúvidas de que a RA será uma das principais maneiras de interagir com as informações nos próximos anos. Ainda não é possível saber quando, mas isso vai acontecer. Grandes empresas como Apple e Google estão liderando esta revolução e tomando as medidas necessárias para essa mudança. Em um futuro próximo, existirá óculos RA e RV socialmente aceitáveis que nos permitirão ver através das lentes, misturando os mundos virtual e real. Isso será tão revolucionário quanto a mudança de revistas e jornais impressos para a Web, ou da Web para aplicativos móveis.

Referências

ARAÚJO, R. B. **Especificação e análise de um sistema distribuído de realidade virtual**, São Paulo, Junho, Tese (Doutorado), Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica da Universidade de São Paulo, 1996.

C. Kirner, E. Zorzal. **Aplicações educacionais em ambientes colaborativos com realidade aumentada**. Anais do Simpósio Brasileiro de Informática na Educação, 1(1): 114-124, 2005.

COUCHOT, Edmond. **A tecnologia na arte: da fotografia à realidade virtual.** Porto Alegre: UFRGS, 2003. (Trad. Sandra Rey). 319 p.

DOMINGUES, Diana (Org.) **Arte, Ciência e Tecnologia: passado, presente e desafios**. São Paulo: Editora Unesp, 2007.

LÉVY, Pierre. **O que é virtual?; tradução de Carlos Irineu da Costa**. São Paulo:Ed.34, 1996. (9ª Reimpressão – 2009)

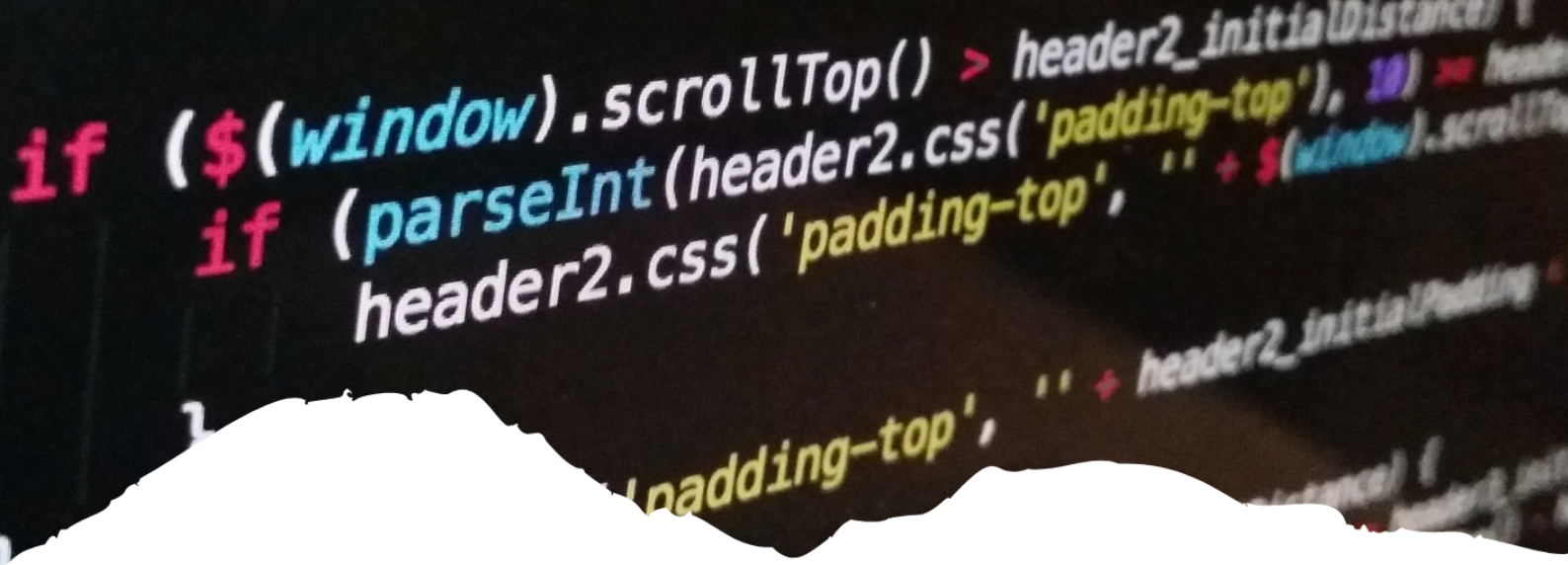
TORI, R.; KIRNER, C.; SISCOUTTO, R.A. **Fundamentos e tecnologia de realidade virtual e aumentada**, Editora SBC,2006.

Utiyama, F. ; Kirner, Cláudio . **Rastreamento e Visualização de Trajetórias para Treinamento com Realida-**

de Aumentada. VII Symposium on Virtual Reality, 2006.

WEBSTER, A; FEINER, S; MACINTYRE, B; MASSIE, W; KRUEGER, T. **Augmented reality in architectural construction, inspection, and renovation**, 2000.

R. Azuma, Y, Baillot, R. Behringer, S. Feiner, S. Julier, B, MacIntyre. Recent advances in augmented reality. Computer Graphics and Applications, 21(6): 34-47, 2001.



18

SEGURANÇA DE REDES: CRIAÇÃO, FUNCIONAMENTO E ATUALIZAÇÕES NO AMBIENTE CORPORATIVO

NETWORK SECURITY: CREATION, OPERATION, AND UPDATES IN THE CORPORATE ENVIRONMENT

Luciano Neponuceno Martins

Roberto Max Louzeiro Pimentel

Resumo

A segurança dos sistemas de informação é paradoxalmente posicionada como um custo e uma necessidade para a sobrevivência da organização. Se, por um lado, encontrar um sistema altamente seguro raramente é visto como algo de grande valor, por outro lado, o risco de ataque é completamente ignorado. Neste contexto, a segurança informática deve ser encarada como uma escolha estratégica e não apenas técnica ou administrativa, com um impacto positivo e inegável nas operações empresariais, envolvendo um conjunto alargado de medidas que permitem a inspeção, detecção e capacidade de resposta das redes informáticas para adaptar-se a potenciais ataques, permitindo reduzir e limitar o risco e o impacto das ameaças à medida que ocorrem. A pesquisa visou compreender a necessidade da preservação de redes e dados em conformidade com as condições do ambiente, exemplificando as seleções preferíveis e formas de implementação a partir dos critérios estabelecidos na revisão de literatura por meio da seleção de trabalhos publicados em revistas científicas com uma análise quantitativa do tipo narrativa, através de uma amostragem não probabilística por conveniência dos dados com ano de publicação entre 2010 e 2021 e artigos originais, compondo assim, a arquitetura da rede.

Palavras-chave: Segurança. Segurança de redes. Segurança de dados. Ambientes corporativos.

Abstract

The security of information systems is paradoxically positioned as both a cost and a necessity for the survival of an organization. On one hand, finding a highly secure system is rarely seen as highly valuable, but on the other hand, the risk of attack is completely ignored. In this context, computer security must be seen as a strategic choice rather than just a technical or administrative one, with a positive and undeniable impact on business operations. It involves a wide range of measures that allow for inspection, detection, and response capabilities of computer networks to adapt to potential attacks, thus reducing and limiting the risk and impact of threats as they occur. The research aimed to understand the need for preserving networks and data in accordance with environmental conditions, exemplifying preferable selections and implementation methods based on the criteria established in the literature review. This was done through the selection of published works in scientific journals, using a narrative quantitative analysis approach. The data was sampled using a non-probabilistic convenience sampling method, considering articles published between 2010 and 2021 and focusing on original articles, thus composing the architecture of the network.

Keywords: Security. Network security. Data security. Corporate environments.

1. INTRODUÇÃO

No atual contexto global de Tecnologia da informação e Comunicação (TIC), a informação está se tornando cada vez mais importante para as empresas, sendo estas, armazenadas em diferentes componentes técnicos, compelindo os usuários a serem cuidadosos ao manuseá-las. Assim, fraudes e enganos estão diretamente relacionados à continuidade dos negócios da organização, tornando necessário desenvolver e aplicar métodos para preveni-los.

Entre as técnicas de proteção de dados, destaca-se a segurança de rede, que é definida como as políticas, processos e técnicas desenvolvidas para proteger uma rede corporativa contra infortúnios e acessos não autorizados. Dentre suas principais prioridades, está a de controlar o acesso e prevenir a invasões e propagação de ameaças em toda a rede. Este processo é realizado por várias linhas de defesa que protegem a rede dentro e fora do perímetro.

A proteção começa com o controle de acesso, que não apenas gerencia o acesso à rede para usuários autorizados, mas também o controla para dispositivos e dados. Sendo a segunda linha de defesa mais importante, um firewall, podendo ser hardware ou software, separa uma rede de outras não confiáveis, como a por exemplo, a Internet. Os firewalls ficam responsáveis por monitorar e controlar o tráfego que entra ou sai da rede.

A segurança de rede também usa sistemas de detecção e prevenção de intrusão que analisam o tráfego de rede para identificar e responder a ameaças. Um subconjunto importante é a segurança de aplicações, que protege aplicativos da Web e softwares usados por empresas, visto que estes geralmente são mais vulneráveis a ataques. Além disso, muitas outras estratégias e técnicas são usadas para manter data centers, nuvens públicas e mais seguras.

Num ambiente corporativo os dados armazenados vão muito além de somente controle e administração internos, envolvendo também clientes e outras instituições; de igual maneira, a criação, seu funcionamento e atualizações de segurança nas redes – sendo esta um conjunto de estratégias, ferramentas e processos adotados para a preservação e manutenção de dados – protegem também a integridade e usabilidade das conexões, impedindo a utilização indevida das informações nelas contidas e possíveis modificações de invasores de uma rede de máquinas e dispositivos acessíveis por ela.

As instituições, ao investirem em proteção de suas redes com uma vasta gama de sistemas disponíveis e em operação atualmente, agregam conhecimento no que tange os mundos virtual e real, desempenhando um papel de alerta ao vazamento de informações e dados importantes do ambiente corporativo, bem como a introdução e competitividade no mercado com o fornecimento de integridade, credibilidade, organização e diligência de seus clientes e outras organizações que, por ventura, fazem parte do seu banco de dados pela rede armazenados.

A pesquisa torna-se atrativa às áreas acadêmicas, científicas e sociais no que se diz respeito aos múltiplos de demonstrativos de inovações, sendo necessária para o domínio dos meios de escolha, criação e atualizações para corporações que buscam aprimorar seus métodos de segurança aos seus clientes e instituições parceiras. Ademais, trazer a legitimação do desenvolvimento e atualizações constantes de softwares dos mais diversos tipos e expandir a proteção das redes em diversos âmbitos.

Dada a necessidade da segurança de redes e dados, em um ambiente corporativo e

institucional, sua importância carece de atenção. O artigo então, visa compreender a necessidade da preservação de redes e dados em conformidade com as condições do ambiente, exemplificando as seleções preferíveis e formas de implementação; apontar os métodos pelo qual o amparo pode ser fornecido de acordo com as demandas e necessidades do ambiente de trabalho e descrever o planejamento, abordagem e defesa de redes com as atualizações necessárias para um bom desempenho.

2. DESENVOLVIMENTO

2.1 Metodologia

Para alcançar os objetivos desse estudo, este foi delimitado a partir dos critérios estabelecidos na revisão de literatura por meio da seleção de trabalhos publicados em revistas científicas com uma análise quantitativa do tipo narrativa, através de uma amostragem não probabilística por conveniência dos dados. O levantamento bibliográfico e de dados, baseados em artigos científicos sobre segurança de redes em ambientes corporativos, foram encontrados em portais periódicos online e publicados em base de dados como Scielo, banco de teses de universidades federais, além de livros disponíveis em bibliotecas físicas. Os termos buscados foram 'Segurança', 'Segurança de redes', 'Software', 'Segurança de dados, 'Segurança de redes em ambientes corporativos'. Os filtros utilizados para a busca foram artigos de revisão de literatura após a identificação, seleção, elegibilidade e inclusão com ano de publicação entre 2010 e 2021 e artigos originais, compondo assim, a arquitetura da rede.

2.2 Resultados e Discussão

2.2.1 Evolução tecnológica e suas ameaças

Com base na dinâmica atual da sociedade, torna-se praticamente impossível sobreviver sem o suporte de redes de computadores. A demanda por dispositivos capazes de se conectar à Internet para usufruir dos diferentes serviços ofertados através da rede, cresce a cada dia com o surgimento de novas ferramentas projetadas para potencializar a execução de atividades cotidianas, minimizando os encargos envolvidos, melhorando significativamente a sua eficácia (STALLINGS, 2015).

As redes de computadores sofreram mudanças para atender à evolução das aplicações, que passaram de sistemas isolados e fechados, sobre os quais as organizações detinham total controle, para sistemas abertos e distribuídos, baseados em componentes off-the-shelf (Hardwares ou Softwares "de prateleira"), dos quais os conhecimentos e controles são limitados. Atualmente, os sistemas na quase totalidade dos casos, os sistemas de informação são escolhidos segundo as funcionalidades oferecidas e investimento inicial, em detrimento da robustez, maturidade e do retorno do investimento a longo prazo ou benefícios indiretos (NOBRE, 2007).

Com o decorrer das evoluções e surgimento de ferramentas tecnológicas, as empresas que se encarregam de usufruir desses mecanismos, reconheceram a necessidade de implementação de métodos para proteção de seus dados devido a vulnerabilidade presentes nas redes. Segundo a ISO (*International Standardization Organization* – Organização Internacional para Padronização) a vulnerabilidade refere-se a qualquer falha que possa violar um sistema ou as informações nele contidas ao conectar-se à rede, o sujeitan-

do a inúmeras ameaças como furto de dados e interceptação de tráfego, uso indevido de recursos, varredura, exploração de vulnerabilidades e ataque de negação de serviço e de força bruta (STALLINGS, 2015).

Caracteriza-se por ameaça, a possibilidade de uma violação de segurança, que existe quando ocorre uma condição capacitância, ação ou evento que pode violar a segurança e causar danos. Ou seja, uma ameaça é um possível risco de explorar uma vulnerabilidade, tornando assim, passível a ataques à segurança do sistema, derivado de uma ameaça inteligente para fugir dos serviços de segurança e violar a política de segurança de um sistema (STALLINGS, 2015).

Dentre as ameaças comumente utilizadas, é possível citar os Ransonware que se caracteriza por um tipo de malware que restringe o acesso ao sistema ou arquivos que cobra um valor de "resgate" para que o acesso possa ser restabelecido (MALWAREBYTES, 2018) e os ataques DDoS que, porventura, permitem que um invasor repasse requisições duplicadas e falsas para um servidor forçar usuários legítimos a recusarem o serviço (RAHMAN; QURAISHI; LUNG, 2019).

2.2.2 Segurança de redes

Para Macedo et al. (2018), o conceito de segurança de redes baseia-se na proteção oferecida para um sistema com a finalidade de alcançar os objetivos da tríade CIA (da abreviação da língua inglesa para *confidentiality, integrity and availability* – Confidencialidade, Integridade e Disponibilidade), sendo estes, os *firewalls, softwares, firmwares*, informações/dados e telecomunicações.

À medida que novas tecnologias e novos sistemas são criados, é razoável supor que sempre haverá novas vulnerabilidades e, portanto, novos ataques. Como por exemplo, o surgimento de redes sem fio, que trazem benefícios significativos para empresas e usuários, mas também apresentam novas vulnerabilidades que podem colocar o negócio em risco. A própria história exemplifica as inovações em técnicas de ataque, tornando a defesa mais difícil que o habitual (NAKAMURA; DEGEUS, 2007).

A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISSO/IEC 27002:2005) (DANTAS, 2011, p.11). De acordo com Vancim (2016), todo processo em uma organização precisa de informações. A comunicação é necessária para que as informações possam ser trazidas com segurança entre os responsáveis por essas tarefas. Essas informações são um dos ativos mais importantes e fundamentais nos processos de uma organização. Consequentemente, pode-se afirmar que a informação é de suma importância para um bom resultado das negociações.

Nos dias atuais, devido aos infortúnios que as empresas podem sofrer em caso de ataque de hackers ou vírus na rede, as instituições buscam manter um nível de segurança que dê algumas garantias para o fluxo de suas informações confidenciais na rede e, portanto, o negócio de rede torna-se o maior investidor e usuário de ferramentas de segurança (MORAES, 2010).

2.2.3 Planejamento, abordagem e defesa de redes

No que concerne ao *start* de pensamento das medidas de segurança de informações contidas nas redes, para Nakamura e Geuse (2007), a confiabilidade, integridade e disponibilidade desta estrutura obrigatoriamente necessitam estar alinhados e em conformidade de modo que sejam necessários para o bom andamento das organizações, que devem ser protegidos. Com isso, segundo os autores, a informação deve chegar aos destinatários de forma abrangente e confiável.

Para garantir a integridade de seus dados, as empresas devem seguir uma política de segurança correspondente a um conjunto de regras, que especificam o que pode ou não ser feito, bem como as penalidades as quais estão sujeitos os usuários que dela não cumprem, tais como: estabelecimento de regras para o uso de senhas e credenciais de acesso, definição de cronograma de backup e controle de acesso aos espaços físicos e graus de acessibilidade, além da criação de planos de contingência e de gerenciamento de riscos e política de atualização de softwares. O estabelecimento de uma (ou mais) políticas de segurança de forma clara e objetiva, seguida da explanação e envolvimento dos usuários que utilizam a rede, permite minimizar problemas de segurança conhecidos e adicionar-lhe uma camada adicional de proteção (MACEDO et al., 2018).

A implantação de segurança para as redes, baseia-se na criação de mecanismos de defesa, sobretudo os *firewalls* para auxiliar e impedir que *hackers* ou *softwares* mal-intencionados consigam acesso a um computador por meio de uma rede ou da Internet (FACHINELLI; AHLERT, 2019). Tem por função proteger informações entre uma rede privada e a Internet ou outras redes. Para dispor de um *firewall* eficiente, é necessário que o mesmo seja configurado de forma correta, tenha bons recursos implementados e esteja corretamente posicionado na rede em questão (PEIXINHO; FONSECA; LIMA, 2013).

Para o bom desempenho de um *firewall*, é necessário um bom serviço de *Proxy*, que consiste em acondicionar, em uma zona de pronto acesso, informações já alcançadas por outro usuário, impossibilitando a propagação destas informações e disponibilizando-as ao usuário em um tempo restrito, ou seja, um servidor que atua como intermediário para atender requisições de clientes ao solicitarem recursos de outros servidores (NORTHCUTT, 2002).

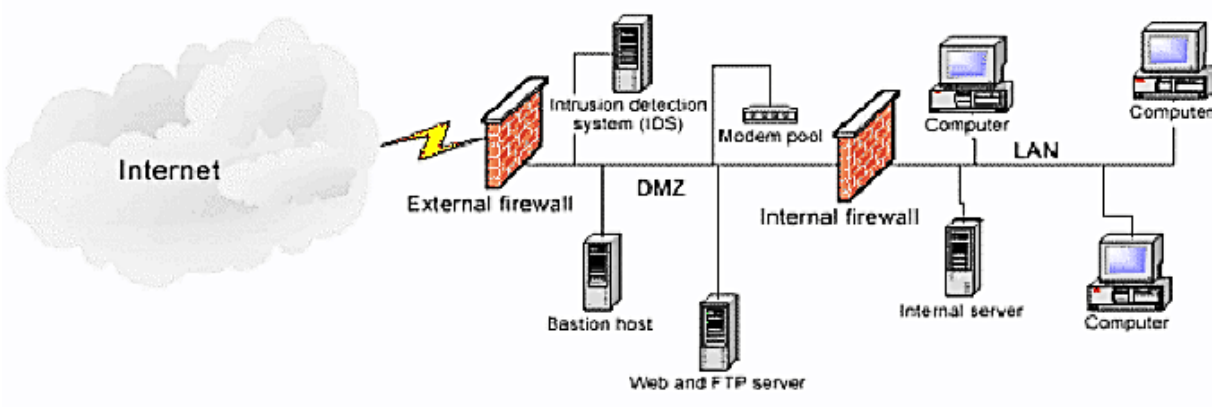


Figura 01: Funcionamento de um Sistema de Detecção de Invasão

Fonte: http://itm455.itmbsu.net/Notes/L8_NetworkSec.htm

Com base no descrito por Goedert e Péricas (2012), ainda sobre as ferramentas de segurança, precisa-se adotar dispositivos automatizados e inteligentes que detectam tentativas de invasão em tempo real, chamadas de sistemas de detecção de invasão (*Intrusion Detection System* – IDS) que, além de ser capaz de detectar invasões, bloqueia o acesso

do intruso, com o auxílio de outra ferramenta em conjunto chamada de Sistemas de Prevenção de Invasão (*Intrusion Prevention System* – IPS) responsáveis por registrar em log as intrusões e enviar alertas aos administradores da rede ao detectar ameaças.

Para auxiliar na aplicação dos métodos protetivos, são criados *softwares*, sendo considerados classes de sistemas que agem na identificação, prevenção e bloqueio de possíveis invasões e ameaças. A arquitetura de *software* denomina-se pelo conjunto de decisões significativas sobre a organização de um sistema de software, a seleção de elementos estruturais e suas interfaces, juntamente com o comportamento especificado nas colaborações entre estes elementos, a composição destes elementos em subsistemas progressivamente maiores e o estilo arquitetural que guia esta organização (NHIMI, 2016).

Implantar um sistema de segurança não é uma tarefa simples, visto que, para isto, é necessária qualificação profissional em conhecimento em redes e em tecnologias atualizadas para o preparo da infraestrutura que melhor atenda a corporação (GOEDERT; PÉRICAS, 2012). O enfoque em ambientes corporativos no que se diz respeito à segurança, passa de 'impedir o acesso' para 'controlar os usuários que acessam a rede', dessa maneira, ter o controle dos recursos que cada usuário pode acessar torna-se indispensável, além da certeza de que farão exatamente aquilo para o qual têm permissão explícita é uma questão vital para o sucesso do sistema de segurança. Para isso, somente o controle não é eficiente, sendo necessário também monitorar as atividades dos usuários (NAKAMURA; DE GEUS, 2007).

A garantia da proteção de informações comerciais, torna imprescindível que exista um Sistema de Gestão de Segurança da Informação (SGSI), conforme definido por Palma (2016); SGSI inclui estratégias, planos, políticas, medidas, controles e várias ferramentas usadas para implementar, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Existem diretrizes definidas pela ISO para a implementação de um SGSI. Neste caso particular de implantação empresarial, é utilizado o certificado ISO/IEC 27001. A norma incentiva os usuários a entender a importância de entender os requisitos e as necessidades de informação. Estabelecer políticas de segurança, estabelecer e operar controles de gerenciamento de riscos de segurança da informação, monitorar e analisar criticamente o desempenho e eficácia do SGSI e promover a melhoria contínua com base em medições objetivas (FONTES, 2012).

3. CONCLUSÃO

A segurança em redes é uma atividade contínua pela busca de melhorias, uma vez que as técnicas e ferramentas utilizadas por potenciais invasores estão em constante evolução. Em organizações onde, devido ao fluxo de processos, há uma rotatividade considerável dos membros que ocupam função específica na segurança da rede, é necessário agilizar e antecipar o aprendizado de novos indivíduos que venham a ocupar lugar nesta área. Rotineiramente, são divulgadas novas vulnerabilidades em programas e sistemas operacionais. No entanto, o ambiente computacional de uma organização deve estar sempre a postos em resistir a eventuais situações.

A topologia, princípios e ferramentas expostos neste trabalho visaram servir de alicerce para que cada administrador busque a métodos e recursos adequados à sua realidade. De acordo com os objetivos estabelecidos no início do trabalho, a cadeia de processos proposta mostrou-se um importante instrumento de padronização da segurança de rede em ambientes corporativos, sendo possível, a partir de suas aplicações, garantir que a segurança de rede seja efetiva e muito bem planejada.

A definição da política de segurança é de suma importância em quaisquer ambientes, porém, em corporações, a implantação desta política é necessária para que as definições de segurança sejam conhecidas por todas as pessoas que fazem uso dos recursos disponibilizados. Garantir que os acessos aos dados da organização sejam seguros, íntegros e confiáveis envolve também a conscientização e instrução das pessoas que utilizam fazem dos recursos, assim como a implementação de cadeias de processos e softwares.

No concerne o fator acadêmico do trabalho, foi de fundamental importância para análise dos aspectos teóricos e conhecimento das melhores soluções adotadas e, também, outras ferramentas de segurança e seus métodos de aplicabilidade. Combinando-se os conhecimentos, teórico e prático, adquiridos no decorrer do trabalho, no que se diz respeito a prospecções futuras, serão de grande serventia para aplicabilidade no mercado de trabalho e outros projetos a serem desenvolvidos para o ambiente acadêmico.

Referências

DANTAS, L.M. **Segurança da Informação** - Uma Abordagem Focada em gestão de Riscos. Olinda. Livro Rápido, 2011.

FONTES, Edson. **Políticas e Normas para a Segurança da Informação: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações**. Rio de Janeiro: Brasport Livros e Multimídia, 2012.

GOEDERT, Willian; PÉRICAS, Francisco Adell. DETECÇÃO E BLOQUEIO DE ACESSOS INDEVIDOS EM SERVIDORES WEB LINUX. **FURB – Universidade Regional de Blumenau**, Santa Catarina, v. 2, n. 2, p. 1-10, 11 dez. 2012. Disponível em: https://www.revistas.udesc.br/index.php/reavi/article/download/2914/2184. Acesso em: 26 out. 2022.

MACEDO, Ricardo *et al*. **Rede de Computadores**. 1. ed. Santa Maria: [*s. n.*], 2018. 196 p. Disponível em: https://www.ufsm.br/app/uploads/sites/358/2019/08/MD_RedesdeComputadores.pdf. Acesso em: 27 out. 2022.

MATEUS FACHINELLI; EDSON MOACIR AHLERT. FIREWALL DE PRÓXIMA GERAÇÃO - FORTINET. **Revista Destaques Acadêmicos**, v. 11, n. 4, 2019. Disponível em: <http://univates.br/revistas/index.php/destaques/article/view/2385/1602>. Acesso em: 30 out. 2022.

MORAES, Moraes Alexandre Fernandes de, Segurança **em Redes – Fundamentos**, Primeira Edição, São Paulo, Editora Érica 2010.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. 1. ed. [*S. l.*]: Novatec, 2007. 488 p. v. 1.

NHIMI, Filipe Tório. Princípios e Práticas em Arquitetura de Software. **Instituto de Gestão em Tecnologia da Informação**, [*s. l.*], p. 1-63, 2016. Disponível em: https://www.machado.mg.gov.br/files/concursos/1cf11cf161fe4eb688dfeec880d6b4d9.pdf. Acesso em: 27 out. 2022.

NOBRE, J. C. A.. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos UniFOA** , Volta Redonda, ano 2, nº. 5, dez. 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao/05/11.pdf>

NORTHCUTT-Winters, Scott, Northcutt, Stephen.Frederick, Karen.Zeltser, Lenny.Ritchey,Ronald Desvendando Segurança de Redes. Ed. Campos.São Paulo – 2002.

PALMA, Fernando. **Sistema de Gestão de Segurança da Informação (SGSI)**, 2016. Disponível em: <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em: 18 fev 2023.

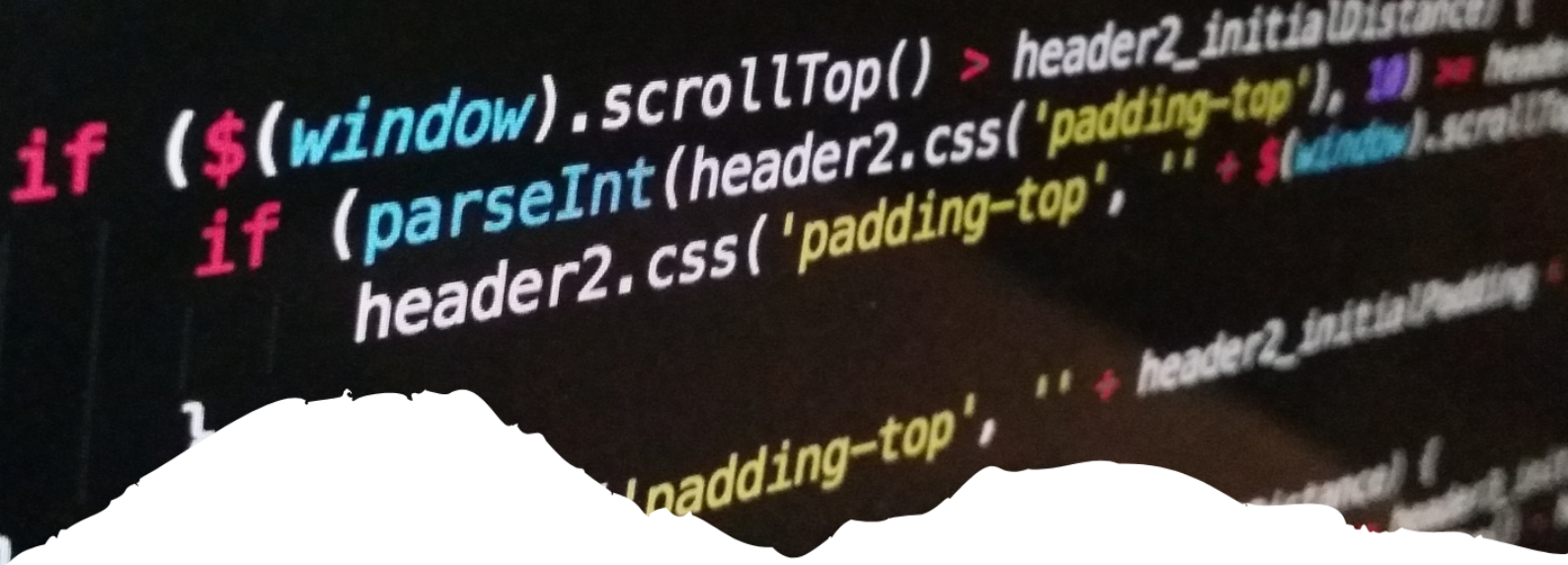
PEIXINHO, Ivo de Carvalho; FONSECA, Francisco Marmo da; LIMA, Francisco Marcelo. **Segurança de Redes e Sistemas**. Rio de Janeiro: RNP/ESR, 2013.

RAHMAN, O.; QURAISHI, M. A. G.; LUNG, C.-H. Ddos attacks detection and mitigation in sdn using machine learning. In: **IEEE. 2019 IEEE World Congress on Services** (SERVICES). [S.l.], 2019. v. 2642, p. 184–189.

STALLINGS, William. **Criptografia e Segurança de Redes**. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 578 p. Disponível em: https://www.docdroid.net/BebtXZO/criptografia-e-seguranca-de-redes-6a-ed-2014-pd-

f#page=5. Acesso em: 26 out. 2022.

VANCIM, F.F.N. **Gestão de Segurança da Informação**. Rio de Janeiro; SESES, 2016.



19

SEGURANÇA DE INFORMAÇÃO DA INTERNET

INTERNET INFORMATION SECURITY

Ermando Oliveira Silva Filho
Carolina Gomes Araujo Garreto

Resumo

O artigo aqui produzido teve por temática a segurança de informação da internet, onde objetivou compreender a relevância exercida pelos sistemas de informações no contexto tecnológico que a sociedade moderna se encontra inserida. No tocante a problemática teve-se como questionamentos como a tecnologia e suas ferramentas podem possibilitar a segurança de informações na internet? Há como erradicar a falta de segurança da internet? No que pese a justificativa do presente estudo destaca-se como argumento válido a sua elaboração a narrativa que, com todo o amparado digital que envolve a sociedade atual a qual se encontra mais conectada do que nunca é imprescindível garantir condições seguras aos seus consumidores, cuidando da guarda de informações relevantes de futuros desastres, por exemplo, e poder recuperá-las depois. Mencionando-se os objetivos específicos este artigo vislumbrou-se estudar as ferramentas disponibilizadas para melhoria da segurança; apontar os riscos existentes nas redes; descrever ideias que ajudem na segurança de dados do indivíduo; e por fim compreender acerca da segurança de informações da internet. Quanto ao método, optou-se por utilizar a pesquisa bibliográfica, obtendo-se como principal aporte teórico os estudos de GETSCHKO (2020) e PEREIRA (2005). Chegando-se ao final de toda a explanação tem-se como principal conclusão do estudo que, de certo, hoje grande parte dos usuários, de uma forma geral, conseguem constituir uma proteção para a segurança dos sistemas de informação de seus aparelhos tecnológicos.

Palavras-chave: Internet, Proteção de dados, Sistemas e Segurança da informação.

Abstract

The article produced here had Internet information security as its theme, where it aimed to understand the relevance exercised by information systems in the technological context that modern society is inserted. With regard to the problem, questions such as how technology and its tools can enable the security of information on the Internet? Is there a way to eradicate the lack of internet security? Despite the justification of the present study, the narrative stands out as a valid argument that, with all the digital support that involves today's society, which is more connected than ever, it is essential to guarantee safe conditions for its consumers, taking care of keeping relevant information from future disasters, for example, and being able to retrieve it later. Mentioning the specific objectives, this article envisaged studying the tools available to improve security; point out the existing risks in the networks; describe ideas that help secure the individual's data; and finally understand about the security of information on the internet. As for the method, it was decided to use the bibliographical research, obtaining as the main theoretical contribution the studies of GETSCHKO, 2020 and PEREIRA, 2005. Coming to the end of all the explanation, the main conclusion of the study is that, certainly, today most users, in general, manage to provide protection for the security of the information systems of their technological devices.

Keywords: Internet. Data protection. Systems and Information Security.

1. INTRODUÇÃO

O presente estudo aqui desenvolvido teve por temática a segurança de informação da internet, onde objetivou compreender a relevância exercida pelos sistemas de informações no contexto tecnológico que a sociedade moderna encontra-se inserida, bem como apreciar as possibilidades existentes quando se trata da utilização das ferramentas disponibilizadas pela tecnologia para obter uma maior segurança quando do acesso à grande rede mundial de computadores (internet).

Para tratar da temática da segurança da informação faz-se pertinente mencionar que esta se encontra inserida na gama de serviços e dispositivos que a tecnologia da informação abarca, onde se incumbe à segurança o papel de proteger todos os acessos realizados por seus usuários.

No que pese a construção do presente estudo destaca-se como argumento válido a sua elaboração a narrativa que com todo o amparado digital que envolve a sociedade atual a qual se encontra mais conectada do que nunca é imprescindível ter informações bem guardadas, sistemas seguros de hackers e destacando-se a necessidade de cuidar da guarda de informações relevantes de futuros desastres, por exemplo, e poder recuperá-las depois. Uma vez que é relevante ter essa conscientização do cuidado que se deve ter com o controle de segurança, e assim compreender a importância de se proteger esses canais de comunicação.

No tocante a problemática que norteou o referido artigo, este tivera como embasamento os questionamentos de como utilizar a tecnologia e suas ferramentas para possibilitar a segurança de informações na internet? Bem como se questionou se haveria como erradicar a falta de segurança da internet?

Mencionando-se os objetivos específicos que estruturam esta pesquisa vislumbrou-se estudar as ferramentas disponibilizadas para melhoria da segurança; em seguida apontar os riscos existentes nas redes; adiante buscou-se descrever ideias que ajude na segurança de dados do indivíduo; e por fim atentou-se para compreender mais sobre a segurança de informações da internet.

Para alcance dos objetivos traçados optou-se por utilizar como base teórica e metodológica a Revisão da literatura, onde está permitiu que houvesse o aprofundamento do conhecimento sobre o tema proposto, e assim possibilitasse a ampliação do entendimento sobre as dificuldades que existentes no contexto da segurança de informações na internet. Obtendo-se com isso como principal aporte teórico os estudos de Getschko (2020) e Pereira (2005).

Ante todo o exposto é possível inferir que estratégias que visem a segurança de informações encontradas em meio digital são de grande valia para evitar o acesso de indivíduos de má fé a dispositivos físicos como computadores, redes como a internet e os sistemas computacionais de uma pessoa, de uma empresa ou em sentido mais amplo, até mesmo de todo um nicho social ou sistema público necessário a população.

2. SISTEMAS DE INFORMAÇÃO

Apresentando-se a priori uma breve conceituação, entende-se que a segurança da informação nada mais é do que um conjunto de estratégias que são adotadas para proteger

dados e informações que são armazenados em ambientes tecnológicos (SILVA, 2021, p. 05).

Expondo-se as palavras sistema e informação tem-se a definição apresentada no estudo de Gomes (2017, p. 13, grifos nossos), o qual diz que o sistema vem a ser um conjunto integrado de elementos dinamicamente inter-relacionados, sendo este conjunto o responsável por desenvolver atividades que visam atingir objetivos comuns a todos os integrantes do conjunto.

Referindo-se a conceituação da palavra informação Gomes (2017, p. 13), utiliza da análise já consolidada por Chiavenato, onde este explana as fontes da informação sugerindo que estas podem provir do ambiente externo e interno, compreendendo como externo os locais fora da organização, como o mercado de trabalho, agências reguladoras, outras organizações, entre outras.

Quanto ao ambiente interno da organização, este correspondendo a todo o fluxograma da instituição, o que se afirmar englobar desde os "cargos e respectivos salários na organização, pessoas que nela trabalham homens/horas trabalhadas, até aspectos relacionados a volume de produção e de vendas, produtividade alcançada, etc." (CHIAVENATO, 2002, 02).

Passando-se a um simplório destaque em seu percurso histórico, percebe-se que ao longo dos anos, que caracterizam a história da raça humana, o indivíduo, mesmo nos tempos mais remotos da antiguidade, tem como característica nata a busca constante por ter o controle das coisas, das informações, de tudo em sua volta que considera importante (CARUSO; STEFFEN, 1999, p. 20).

O principal intuito pretendido com esse controle é o que baseia a área da Segurança da Informação, tratando-se, portanto, da proteção de determinadas informações e/ou coisas, com a intenção de que os indivíduos/organizações que buscam protegê-las consigam obter êxito nesta tarefa manter, bem como manter seus respectivos valores.

Como mencionado no caput deste capítulo essa vontade de manter protegidas e intactas as mais variadas coisas, atrelada a forma como essas informações chegam (antes fisicamente, agora digitalmente), fez com que fossem aperfeiçoadas as formas de registro e armazenamento das informações, premissa essa que justifica a criação e inserção recorrente dos sistemas de informação e a utilização dos seus sistemas de segurança (GOMES, 2017, p. 35).

Nesse contexto preliminar e de movimentos para o surgimento de um mundo que atendesse as suas demandas, de início pode-se aludir que foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas, em face, principalmente que no contexto anterior havia uma quantidade considerada pequena de informações a serem armazenadas, tanto no âmbito da Pré-história, quanto nos primeiros milênios da Idade Antiga (CARUSO; STEFFEN, 1999, p. 21).

Por esse fluxo pequeno de pessoas e consequentemente de informações, utilizava-se como principal meio de armazenamento e registro de informações a memória humana, mesmo sabendo que está era falha e assim muitos dados seriam perdidos e/ou deturpados, pois não seriam reproduzidos de forma fidedigna (SANDRI, 2014, p. 15).

Prosseguindo-se no momento histórico é possível então noticiar que o advento dos primeiros alfabetos fez com se adotasse, em caráter assistencial, aos de guarda e segurança das informações. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas (CARUSO; STEFFEN, 1999, p. 21).

Avançando no percurso organizacional da sociedade, no que pese especificamente

Sistemas de Informação a entrada deste no contexto global é atrelada ao surgimento dos computadores, visto que é por meio dessas máquinas e dos softwares nelas instalados que as informações e os dados são recebidos, manipulados e devolvidos.

Ao sistema de informações atribui-se a reponsabilidade de coletar e transmitir dados que sejam úteis ao desenvolvimento de produtos ou serviços das empresas, organizações e de demais projetos, estes serão juntados utilizando-se os computadores.

Estas são algumas de suas subordinações, sendo, portanto, oportuno expor que o sistema de informações não se limita à coleta, análise e processamento destas informações de cunho externo, reportando-se a ela a avaliação também de informações internas decorrentes da operação da própria empresa (SCHULTZ, 2016, p. 25).

É ainda por meio destes sistemas que ocorre a aprendizagem necessária para a criação e gerenciamento dos programas e softwares, bem como contemplam as modificações usando linguagens de programação, bibliotecas, frameworks e bancos de dados.

O sistema de informações, por definição, constitui também um sistema pelo qual são obtidos dados para as operações de controle e planejamento da empresa. Em síntese, o sistema de informações gera dados de forma esquematizada e ordenada, os quais fornecem subsídios para o processo de tomada de decisões (SCHULTZ, 2016, p. 28).

Como decorrência imediata desta definição, nota-se que o sistema de informações recebe inputs que, após processados, transformam-se em outputs, que são utilizados para a tomada de decisões administrativas, as quais seriam mais arriscadas, sem que houvessem sido processadas informações que reduzissem as condições de incerteza, ditadas pela interação do sistema-empresa e o ambiente externo (LAMAS; MORAES, 2022).

Nesses moldes, entende-se que um sistema de informações deve ser estruturado como um processo contínuo de comunicações, cujos inputs são informações internas e cujos outputs são informações processadas para a tomada de decisões.

Com relação aos aspectos de segurança que dá reverência aos a proteção de dados de computadores, Laudon e Laudon (1999, p. 7) diz que os “Três importantes aspectos da segurança são: garantir a segurança dos dados, proteger os computadores e redes e desenvolver os planos de recuperação dos desastres que afetam os sistemas de informação”. Estes aspectos exigem muita mais atenção hoje do que antes, isso devido ao aumento de indivíduos dependentes das redes e internet.

Ainda sobre a ótica dos autores Laudon e Laudon (1999, p.7), para que esse sistema de informação quando aplicado às organizações, seja eficaz, necessitará da integração de três componentes, sendo eles as organizações (as empresas), as pessoas e os fatores ligados à tecnologia e as pessoas.

Analisando-se esses componentes entende-se que todos estes fatores são influenciados pelo ambiente externo, bem como exercem influência uns sobre os outros e estes movimentam os sistemas de informação.

De acordo com Fontes (2012, p. 2), “informação é muito mais que um conjunto de dados. Transformar estes dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional”.

Assim fora mencionado que informação é não se resumo em um conjunto de dados, ou seja, é mais que isso. Pois transformá-los estes dados em uma informação é alterar-se a um recurso de valor para a vida do indivíduo.

No que diz respeito ao assunto proposto é imprescindível atentar-se ao fato de que informações e conhecimento, por sua alta capacidade de adicionar estima a processos,

produtos e serviços, constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais. Outro ativo valioso para as organizações, as informações críticas para o negócio devem ser protegidas contra as ameaças que podem levar a um estrago, indisponibilidade temporária, adulteração ou até divulgação não autorizada (BEAL, 2008, p. 13).

É de suma importância o valor das informações, seja ela para empresas quanto para pessoas "comuns» da nossa sociedade que as utilizam, pois as informações, podem ser às vezes, tida como bem mais precioso que uma empresa ou indivíduo pode ter.

Conforme Fontes (2012, p. 2), você pode não ter se dado conta, mas "a informação é um recurso que move o mundo, além de nos dar conhecimento de como o universo está caminhando".

Portanto, compreender a dimensão dessa segurança é importante de se adquirir mais cedo ou mais tarde, uma vez que ela é indispensável para a atividade do indivíduo seja lá onde ele estiver se este está ao alcance de uma rede é relevante manter-se seguro.

De acordo com Sêmola (2003, p.9) o ciclo de vida da informação, "é composto e identificado pelos momentos vividos pela informação que a colocam em risco".

Entende-se que momentos vivenciados justamente quando a tecnologia e os seres humanos fazem uso da informação. Como exemplo desse ponto, pode-se citar as redes sociais que a cada dia que passa só crescem, no quesito quantidade de informações armazenadas, bem como aumentam exponencialmente as chances da real ameaça da aplicação de golpes utilizando, dentre outros mecanismos da fragilidade dos sistemas e também a falta de informação e preparo de quem se usa a tecnologia (BERNARDO, 2011, p. 04).

Corroborando com o mencionado Gaivéo (2008, p.12) infere que associado às questões de segurança da informação, existem ameaças, vulnerabilidades, ataques e riscos que podem afetar a atividade dos SI nas organizações, pelo que é essencial proceder à sua identificação e caracterização para uma melhor resposta e proteção dos Sistemas da Informação no caso de se verificar alguma destas ocorrências.

3. SEGURANÇA DA INFORMAÇÃO INTERNET

3.1 Política De Segurança

A segurança da informação faz parte de um novo contexto social, o qual é baseado no poder exercido comunicação atrelado ao avanço da tecnologia, evidenciando que estes, no mundo da globalização são processos interligados, com a consequente transformação do conhecimento e da informação.

Conforme já mencionado no caput, no início do processo civilizatório marcado pela construção dos primeiros alfabetos, o armazenamento de qualquer informação se dava única e exclusivamente pela memória humana, mas principalmente em decorrência do crescimento populacional o surgimento das tecnologias se tornou de grande valia para permitir que tanto instituições públicas, quanto privadas, consigam coletar informações pessoais dos indivíduos. A evolução desses mecanismos tecnológicos tem sido tão considerável que se torna preciso dizer que se chegou ao ponto em que as empresas têm mais informações sobre o indivíduo do que ele próprio (GETSCHKO et al., 2020, p. 09).

É direito e dever dessas empresas manter a privacidade desses dados. Sendo assim, a segurança desses dados passa a ser repensada, a coleta intensa de dados pessoais e, principalmente o cruzamento destes dados, abrem espaço para o debate a respeito da

proteção e segurança desses dados pessoais. Somente 41% das empresas brasileiras têm políticas de segurança estabelecidas (CANALTECH, 2021).

De acordo com estudos, ainda são poucas as empresas que proporcionam treinamentos envolvendo questões como gestão de risco de segurança digital, cursos online sobre o tema ou orientações internas, que visam proteger dados pessoais. Com a baixa porcentagem, observa-se que as empresas não investem como deveriam em maneiras de proteger os dados dos funcionários e cliente, pois, com esse tipo de informação em mãos erradas, aumenta o índice de números de fraudes (CANALTECH, 2021).

Com isso, além de trazer danos as empresas, que podem ser subordinadas por criminosos para ter seus dados de volta, acarreta outros prejuízos financeiros. Por isso percebe-se a importância de investir em um bom sistema de segurança de dados, evitando assim, custos desnecessários como multas, auditorias e até mesmo perdas de associações profissionais e de clientes visto que não se sentem protegidos o suficiente (GETSCHKO et al., 2020).

Portanto as empresas devem estar atentas e ter alguns cuidados em relação a esses dados como: buscar realizar treinamentos regularmente com a equipe relacionados a gestões de conta, senhas, navegação online e proteção de dados, sempre fazer backups para evitar que informações sejam perdidas ou roubadas, utilizar softwares de segurança de qualidade comprovada, buscando sempre os manter atualizados e utilizar criptografia para proteger dados sensíveis.

De acordo com dados do *Massachusetts Institute of Technology* (MIT) o vazamento de dados no Brasil aumentou em 493%, sendo que mais de 205 milhões de dados de brasileiros foram vazados de forma criminosa em 2019.

A empresa segurança cibernética PSafe revelou recentemente que foram vazados 223 milhões de CPFs de pessoas vivas e mortas, tendo dados pessoais como identidade, data de nascimento e também informações de 104 milhões de veículos e de 40 milhões de empresas, como CNPJ, razão social, nome fantasia e data de constituição (GETSCHKO et al., 2020).

No ano de 2021 houve 181,5 casos de vazamento de dados tanto do governo como de empresas privadas. Foram registrados que entre os meses de abril e junho de 2021 houve um aumento de 220% em relação ao primeiro trimestre do ano. A maior parte deste crescimento se deve ao vazamento das credenciais do governo, este número saltou de 47.654 entre janeiro e março para 160.478 nos meses de abril e junho. Nas empresas brasileiras, houve um crescimento de 176,88% (AXUR, 2021).

Mesmo com o aumento de 20,4% na utilização de senhas com caracteres especiais, letras e números, que tende a dificultar a vida dos cibercriminosos, as pessoas sempre optam por utilizar sequências numéricas como “1234567” sendo assim a senha mais utilizada pela população em geral. Com isso 845.399 preferem utilizar as senhas mais queridas pelos cibercriminosos (GETSCHKO et al., 2020).

3.2 Riscos da Segurança da Informação da Internet

Para avaliar os riscos na segurança da informação é necessário iniciar um processo de identificação de falhas e vulnerabilidade que podem expor informações da empresa. É imprescindível levar em conta que qualquer sistema ou infraestrutura que trafegue dados estão sujeitos a alguma falha ou brecha que pode resultar em exposição dos dados confidenciais e violação de políticas de privacidade (SILVA, 2021).

A análise de risco na segurança da informação é baseada em alguns conceitos como a vulnerabilidade, ameaça e o risco. Identifica-se falha existente num determinado sistema ou recurso, caso essa falha não seja identificada, existe o fator da vulnerabilidade, como por exemplo, design mal planejado, na implementação mal realizada de um programa ou sistemas mal desenvolvidos (SILVA, 2021, p. 14).

Nos casos de ameaça, que é onde um agente interno ou externo averigua uma vulnerabilidade, causando assim, impactos negativos sobre um sistema ou recurso. E inerente aos riscos, o seu potencial associado à exploração de vulnerabilidades, pois, o que está sendo ameaçado são bens econômicos, gerando impactos como o mau funcionamento, roubo de informações, entre outras consequências (SILVA, 2021, 16).

Para Cabral e Caprino (2015, p.22, grifos nossos) “gerir os riscos deve ser a prioridade maior da segurança da informação, onde para realizar tal atividade deve-se buscar defini-los das mais diversas formas e disciplinas, valendo-se inclusive de formas genéricas que analisem a probabilidade e potencial magnitude de uma perda futura”.

Corroborando com o exposto (GOMES, 2017, p. 16), afirma que para que se possa realizar de forma correta a análise de riscos, deve-se *a priori* realizar a identificação destes, e em seguida analisá-los e por fim definir qual passo tomar, sugerindo que quando elencados os referidos riscos, dever-se-á: em caso de risco muito alto, a empresa optar por Mitigar o risco, ou seja, tomando as de precauções para reduzi-lo; como segundo orientação deve-se aceitar o risco, ferramenta utilizada quando o risco não apresenta ameaça direta a organização; e por fim, para riscos independentes do tamanho, o autor sugere que seja transferido o risco, trata-se de uma espécie de terceirização, tendo-se como principal exemplo desta prática a contratação de seguros.

Nesse sentido, as informações estão inseridas em diversos locais e a segurança depende de múltiplos fatores sendo eles, Confidencialidade, Integridade, Disponibilidade, Estados da Informação e Propriedades da Segurança da Informação. É necessário garantir que as informações sejam divulgadas somente para as pessoas que têm autorização para vê-las e também garantir que as informações não tenham sido alteradas (HOEPERS; JESSEN, 2019).

A importância da segurança dessas informações visa certificar que as metas de um sistema possam ser atingidas o tornando assim, acessível para aqueles que irão utilizar (HOEPERS; JESSEN, 2019). Por isso é necessário criar um inventário de para armazenamento de informação, ou seja, identificar os componentes dessa informação utilizar meios tecnológicos que sustentam os processos da empresa (LAMAS; MORAES, 2022).

Há algumas medidas de segurança que podem ser utilizadas para garantir a segurança da informação. Por exemplo, garantir que dados só sejam concedidos àqueles usuários que possuem permissão, sempre exigir identificação e averiguar se a informação procede, utilizar criptografia para validar a identidade dos usuários; autorizar transações bancárias; e proteger o sigilo de comunicações pessoais e comerciais (HOEPERS; JESSEN, 2019).

Nesse contexto, a segurança da informação deve ser pensada em todas as etapas que a informação percorre, seja na entrada, no processamento ou na saída das informações, ou seja, deve-se pensar em todas as a falhas e bem como as possíveis intervenções externas que esta rede de comunicação poderá ter, nos mais variados momentos, evidenciando a relevância de se cumprir “alguns requisitos básicos para garantir a segurança de toda a estrutura envolvida no processo de criação, armazenamento e distribuição das informações através do uso de sistemas” (GOMES, 2017, p. 17).

Sendo assim, garantir a segurança da informação digital é uma tarefa bastante difícil

e requer ajuda de toda a equipe. Por isso é fundamental conhecer as vulnerabilidades e fraquezas que possam existir, se são internas ou externas, quais as possíveis consequências e as melhores formas de minimizar o vazamento de informações (LAMAS; MORAES, 2022).

Com o elevado número de possíveis ataques e ameaças as informações digitais, torna-se necessária a busca de uma resposta que estabeleça a prevenção e não apenas o combate. Observa-se que da mesma forma que aumenta a quantidade de informação em formato digital na Internet, também se observa um grande aumento das ameaças e dos ataques à segurança da informação digital, trazendo assim, grandes riscos de exposições (PEREIRA, 2005).

Sabe-se que um sistema 100% seguro é mais difícil de ser acessado por terceiros. Para isso deve-se investir em uma segurança que busque de fato detectar comprometimentos o mais rápido possível e assim, se recuperar de ataques o mais rápido possível desses prejuízos. Para isso é necessário treinar profissionais para implementar as estratégias e políticas de segurança e implantar medidas de segurança que implementem as políticas e estratégias de segurança (HOEPERS; JESSEN, 2019).

4. REDES SOCIAIS E APLICATIVOS DE MENSAGENS

Em 1995, Nicholas Negroponte, presenciando um contexto tecnológico bem mais limitado que o atual, já afirmava que a informática não se baseava exclusivamente em computadores, firmando entendimento pacífico até os dias atuais que está tinha relação direta com a vida das pessoas, onde permite que haja a interação entre estas (NEGROPONTE, 1995, p.12 *apud* SPERB, 2013, p.16).

Por meio de pensamentos basilares como instituído por Negroponte, foi possível o surgimento de entendimentos acerca de ferramentas oriundas desse meio, tais como a internet que passou a ser conhecida por sua funcionalidade enquanto rede constituída por redes, onde inúmeros computadores e dispositivos informáticos diversos estão interconectados ao redor do mundo.

As redes que formam a internet podem ser consideradas como mecanismos permissivos a conexão dos computadores, ou seja, é essa rede que possibilita a comunicação entre as máquinas. Essa comunicação ocorre por meio da Web, ferramenta que pode ser compreendida como o conjunto das páginas, que podem ser visualizadas pelos computadores, ligadas umas às outras por estruturas de hipertexto (CASTELLS; MORAES, 2003 *apud* SPERB, 2013, p.16).

Entre o conjunto das páginas que compõem a web, como um dos mecanismos mais utilizados para comunicação encontra-se elencada as redes sociais. Estas frequentemente são citadas como mídias sociais, no entanto, este termo é muito abrangente, e por isso, tornam-se mais arriscadas as tentativas de definição (PEREIRA; PINCETA, 2011, p. 03).

Torna-se oportuno trazer para discussão no presente artigo a temática das redes sociais em virtude da influência considerável que estas exercem, tanto na propagação de informações, na aproximação das pessoas, visto que permite a interação, ou melhor, o contato virtual com aqueles que estão distantes. Por mais que o contexto atual permita propagação das mais diversas sem o devido filtro do que venha a atestar a veridicidade, ou seja, comprovar se o que está sendo dito é de fato verdade, as redes sociais tornaram-se um dos principais mecanismos na difusão de informação e consequentemente de conhecimento, causando assim, o desenvolvimento e evolução da espécie humana.

Sua atualização ocorre pelos próprios usuários, sendo estes de todas as idades, onde

a qualquer momento pode aparecer uma nova rede com milhares de usuários, milhares de internautas estão presentes nelas, várias empresas estão participando, patrocinando e investindo no ambiente digital, ou seja, o mundo todo está conectado e não sabe mais viver sem elas.

4.1 Informação e Conhecimento e o Compartilhamento de Ambos

As redes sociais se constituem e se proliferam em um espaço propício a informação e o conhecimento, sendo a busca por eles que movimentam as redes. Assim, é possível compreender que a informação está no domínio pessoal do receptor, isto é, é ele quem define se a mensagem recebida acrescenta algum valor ao estado anterior, estabelecendo sentido e modificando atitudes" (TOMAEL et al., 2005, p. 96).

A informação funciona como troca com o mundo exterior, o que confere seu caráter social. Quando assimilada e processada por um sujeito específico, a mesma é a base para sua integração no mundo, propiciando ajustes contínuos entre o mundo interior e o mundo exterior (TÁLAMO, 2004 *apud* TOMAEL et al., 2005).

Essa relação entre informação e conhecimento é entendida como um ciclo, necessário, onde torna-se frequente a busca e o uso de informação, bem como vice e versa. Essas etapas compõem a estrutura cognitiva interna dos indivíduos e sua organização emocional. Para Choo (1998), esse modelo representativo pode ser analisado usando-se como parâmetro a necessidade informação, a busca por essa informação e, por conseguinte o uso dessa informação (CHOO, 1998 apud GOMES, p. 42).

No que tange a necessidade de informação essa surge do elemento da dúvida, ou seja, ela é primeiramente sentida como uma incerteza, onde conforme esse sentimento vai diminuindo, a necessidade de informação progressivamente vai chegando à consciência e então a questão é formalizada, esse parâmetro contém elementos cognitivos, afetivos e situacionais.

Referindo-se a busca pela informação este segue alguns ritos, partindo0se da iniciação, em seguida o encadeamento, a pesquisa, diferenciação, o monitoramento, extração, verificação e conclusão. As três primeiras categorias são importantes para o desenvolvimento do foco e estratégia da pesquisa, as demais são fortemente influenciadas pelo ambiente cultural e organizacional, ou seja, a escolha das fontes de informação depende da inserção do indivíduo e da motivação que gerou a busca (SCHULTZ, 2016, p. 58).

Após o indivíduo sentir a necessidade de buscar a informação, em possa dela, este começa a fazer uso da informação, nesta etapa, ocorre o processamento da informação que foi buscada. deste processamento a informação resulta em um novo conhecimento ou ação. Nesse aspecto a informação é frequentemente usada para responder a questões, resolver problemas, tomar decisões, negociar posições, ou construir significados para determinada situação. As pessoas sentem satisfação e confiança quando suas pesquisas têm bons resultados, mas, quando ocorre o contrário, sentem desapontamento e frustração. (TOMAEL et. al., 2005, p. 96).

Essa relação também é abordada por Nonaka e Takeuchi (1997, p.64) quando afirmam que: "a informação é um fluxo de mensagens, e o conhecimento é criado pelo mesmo fluxo de informação, ancorado nas crenças e compromissos de seu detentor".

O processo de transformação da informação em conhecimento é discutido por muitos autores, onde a maioria afirma que para esse processo ocorrer necessita da interação das pessoas para que haja primeiro o compartilhamento dessas informações para que

em seguida ocorra a assimilação e logo após seja transformada em conhecimento para o indivíduo.

Nesse sentido, compreende-se que a informação e o conhecimento são inerentes às redes sociais, sua importância social e econômica é consequência do efeito que causam nas pessoas e nas organizações. Nesse âmbito, constatamos a necessidade frequente de compartilhamento para que assim possam trazer mudanças no contexto em que estão inseridos (TOMAEL et al., 2005, p. 96).

Para Dixon (2000), o termo compartilhar tem dois significados: o primeiro consiste em dar uma parte, o que requer generosidade, e o segundo trata-se da necessidade de ter em comum um sistema de crenças compartilhado, pois conforme explanado anteriormente, para que haja a busca pela informação é preciso que o indivíduo tenha interesse em fazer isso, e esse surge da dúvida e para que a dúvida seja produzida é necessário um ambiente, que muitos vezes será o compartilhado por um grupo de indivíduos.

Segundo Marteleto (2001) contempla a ideia de compartilhamento de valores e interesses que, para promover o fortalecimento da rede, dependem do compartilhamento da informação e do conhecimento.

Falando-se das redes de trabalho nas organizações, Yu, Yan e Cheng (2001) também ressaltam os benefícios da cooperação e compartilhamento da informação, quando afirmam que a globalização dos negócios foi acelerada nas últimas duas décadas devido ao rápido desenvolvimento da tecnologia de produção e informação, aumentando a pressão dos custos e ocasionando demanda mais agressiva dos clientes. Os esquemas de produção e distribuição foram modificados, e novos padrões de relacionamento entre fornecedores, produtores, varejistas e outras partes foram introduzidos no mercado, notadamente sob o esquema de redes.

De acordo com Hanfield e Nichols, apud Shore e Venkatachalan (2004), dois parâmetros são essenciais para integração e coordenação da rede: colaboração e tecnologia. Para esses autores, o trabalho em rede requer cuidadosa coordenação e integração. A colaboração, vista por eles como um processo social, é necessária para compartilhar a informação e, por consequência, o conhecimento, para integrar horizontalmente as operações da rede. Já o compartilhamento é visto mais como um processo tecnológico.

Mas o compartilhamento da informação e do conhecimento só terá resultados se implicar um processo de aprendizagem, pois o simples acesso sem esse processo não modifica a realidade, perde, portanto, o sentido. Assim, é preciso lembrar que se as pessoas começam a compartilhar ideias e conseguem perceber a importância desse processo, o próprio compartilhamento cria a cultura da aprendizagem.

Reportando-se a segurança do uso das redes sociais segundo Moraes (2011, p.139) “da mesma forma que as redes sociais podem ser usadas para divulgação de conteúdo útil, ela também tem sido usada por criminosos, que induzem os usuários a clicarem em links e efetuar download de malware”. Quando isso acontece, vários arquivos de computadores acabam sendo prejudicados ou até roubados, colocando assim em risco indivíduo que pode ter informações furtadas.

Pode-se evitar esse tipo de acontecimento de acordo com a autora citada anteriormente. Criar uma senha difícil é uma boa saída para ludibriar, não relatar informações que possa comprometer-se. O grande problema é que, uma vez na internet, se torna quase impossível retirar todo o conteúdo colocado uma vez que várias fontes podem ter feito cópias e as armazenando em locais diferentes.

5. CONSIDERAÇÕES FINAIS

Com a elaboração do presente estudo pode-se compreender que tratar do universo da segurança de informações que são inseridas na internet, não pode se ater em apresentar simples formas de obter segurança, devendo-se agregar a esse serviço de informação a constante apresentação e utilização de estratégias amplamente pensadas para promover a proteção de informações nela depositadas quer sejam sigilosas, pessoal entre outros.

Infere-se ainda que as estratégias adotadas permitem que pessoas com intenção de prejudicar outros indivíduos não obtenha êxito, logo a segurança da informação dificulta a invasão de sistemas, computadores, redes de internet e assim impossibilita o contato sem autorização de informações valiosas de empresas, de pessoas comuns ou não.

Mencionando-se todo o estudo levantado sobre a segurança de informação confirmou-se a extrema relevância deste, principalmente no contexto atual de expansividade em larga escala do número de navegantes, sendo assim cada vez mais necessário se resguardar de quaisquer imprevistos, infortúnios, pessoas maldosas.

Logo, a proteção de dados, informações, por parte de pessoas “comuns”, empresários, tais como um supermercadista preocupado com a gestão do seu comercio e com seu estoque de mercadoria ou uma instituição pública, não deixando de mencionar também as redes bancárias, já preveem em seus planos, levantamento com base em informações usando nada mais nada menos que computador, internet. Sendo assim tais informações devem ser bem guardadas, bem como disseminada sua relevância não só para aqueles que a utilizam na proteção de seus negócios, por exemplo, mas da sociedade como um todo para assim dirimir possíveis dificuldades na sua implantação.

Portanto, confirma-se que dentro do ambiente empresarial ou não a confidencialidade de informações por parte das pessoas envolvidas neste ambiente é de extrema relevância uma vez que pessoas mal-intencionadas descubram tais informações pode haver um dano irreparável para a pessoa, instituição, empresa, etc.

No que pese o conhecimento apresentado no referido estudo entende-se que aqueles que debruçarem-se na leitura deste artigo irão despertar para o melhor tratamento de suas informações, como também entenderão melhor o papel da segurança de informação no resguardo de futuros transtornos de ter informações roubadas, perdidas ou deletadas.

Com o exposto, faz-se necessário que estudos futuros sejam realizados, sugerindo-se como temáticas para a continuação do exposto a ampla temática da privacidade dos dados inseridos no ambiente virtual; um estudo mais aprofundado das Políticas de segurança, bem como das estratégias que são adotadas para proteger dados e informações relacionadas à tecnologia.

Referências

AXUR. Relatório de vazamento de dados no Brasil primeiro trimestre de 2021**.** In: **Plataforma de proteção contra riscos digitais**. (2021). Disponível em: https://conteudo.axur.com/pt-br/vazamento-de-dados-no-brasil-2021. Acesso em: 10 out. 2022.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2008.

BERNARDO, D. S. **Evolução na Comunicação: estudos nas Redes Sociais**. Universidade Municipal de São Caetano do Sul. São Caetano do Sul, 2011.

CABRAL, Carlos; CAPRINO, William. **Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados**. Rio de Janeiro: Brasport, 2015.

CANALTECH. Somente 41% das empresas brasileiras têm políticas de segurança estabelecidas. Disponível em: https://canaltech.com.br/seguranca/somente-41-das-empresas-brasileiras-tem-politicas-de-seguranca--estabelecidas-185806/. Acesso em: 4 nov. 2022.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2. ed. rev. e ampl. Editora SENAC. São Paulo, 1999.

CHIAVENATO, Idalberto. **Recursos Humanos: edição compacta**. 7. ed. São Paulo: Atlas, 2002.

DIXON, Nancy. **Common knowledge: how companies thrive by sharing what they know.** Harvard: Harvard Business School Press, 2000. (tradução)

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

GAIVÉO, J. M. **As pessoas nos sistemas de gestão da segurança da informação (tese de doutoramento**). Lisboa, Portugal. Disponível em: http://repositorioaberto.uab.pt/handle/10400.2/1272. Acesso em: 4 nov. 2022.

GETSCHKO, D. et al. SEGURANÇA DIGITAL: uma análise de gestão de risco em empresas brasileiras. Núcleo de informação e coordenação do ponto BR, 2020.

GOMES, Marcelo Rodrigues. **A formação profissional de TI no âmbito da segurança da informação: estudo de caso em instituições de ensino superior de Santa Catarina** / Marcelo Rodrigues Gomes; orientador, Hamilcar Boing, 2017. 68 p.

HOEPERS, C.; JESSEN, K. S. Fundamentos de Segurança da Informação. Escola de governança da internet no Brasil, 2019.

LAMAS, N. S.; MORAES, E. A. P. Elementos de Segurança da Informação que contribuem ou são percebidos para uma decisão de compra na Internet. Research Society and Development, v. 4, n. 1, 30 jun. 2022.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação com Internet**. Rio de Janeiro: LTC, 1999.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**, Brasília, v. 30, n. 1, p. 71-81, jan./abr. 2001.

MORAES, Paulo. Mente Anti-hacker - Proteja-se! **Brasport**. Rio de Janeiro, 2011.

PEREIRA, Heloísa; PINCETA, Karina Perussi. **O avanço dos meios digitais e a produção de informação:** como as redes sociais estão transformando a comunicação, o jornalismo e a sociedade. (2011). Disponível em: <http://pt.slideshare.net/karinaperussi/artigo-cientfico-redes-sociais-8460927>. Acesso em: 10 out. 2022.

PEREIRA, P. J. F. Segurança da informação digital. (2005). Disponível em: <http://eprints.rclis.org/10305/>. Acesso em: 03 nov. 2022.

SANDRI, E. D. **A importância do sistema de informações gerenciais da prodan software para a tomada de decisões**. Ijuí/RS – 2 o Semestre de 2014.

SCHULTZ, Glauco. **Introdução à gestão de organizaçõe**s / Glauco Schultz; coordenado pela SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2016

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

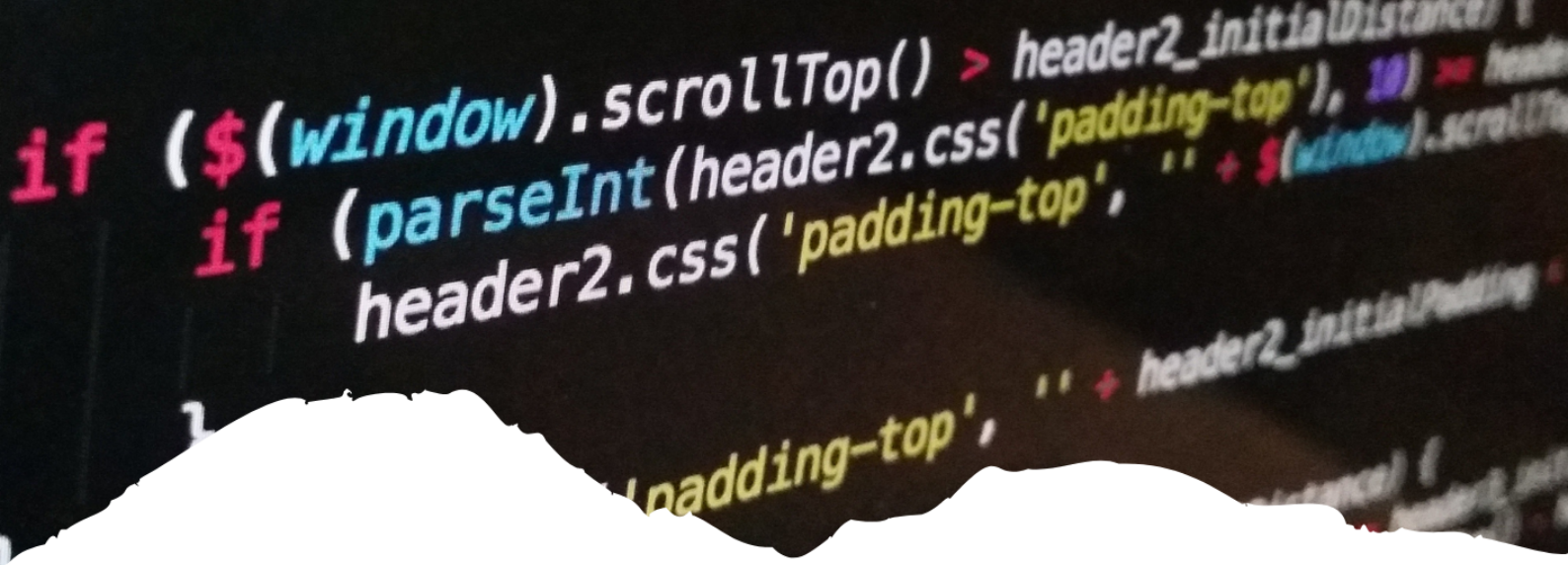
SHORE, B.; VENKATACHALAM, A. R. Role of national culture in the transfer of information technology. **Journal of Strategic Information Systems**, v. 5, n. 1, p. 19-35, 2004. (**tradução**).

SILVA, C. Entenda mais sobre a análise de risco na segurança da informação. Unico Check - Unico | Solução completa em biometria facial | Blog**,** 2021.

SPERB, Nanachara Carolins. **Redes sociais e comunicação organizacional:** O caso do Instituto Federal Catarinense. Disponível em: <http://www.insite.pro.br/2013/Janeiro/redessociais_comunicacao_organizacional.pdf>. Acesso em: 10 out. 2022.

TOMAEL, Maria Inês [et. al.]. **Das redes sociais à inovação.** (2005). Disponível em: <http://www.scielo.br/pdf/ci/v34n2/28559.pdf>. Acesso em: 10 out. 2022.

YU, Zhenxin; YAN, Hong; CHENG, T. C. E. Benefits of information sharing with supply chain partnerships. **Industrial Management & Data Systems**, v. 101, n. 3, p. 114-121, 2001.



20

ESTUDO DE FRAMEWORKS HÍBRIDOS E ANÁLISE COMPARATIVA ENTRE DESENVOLVIMENTO HÍBRIDO E NATIVO

STUDY OF HYBRID FRAMEWORKS AND COMPARATIVE ANALYSIS BETWEEN HYBRID AND NATIVE DEVELOPMENT

Arthur Yan da Silva Louzeiro

Resumo

Com o avanço da tecnologia e principalmente dos smartphones, empresas que trabalham no ramo de desenvolvimento de aplicativos mobile tiveram que lidar com grandes problemas como complexidade, custo e tempo de desenvolvimento de um app para diferentes sistemas operacionais. Com o tempo foi introduzido o modelo de desenvolvimento híbrido através de frameworks e uma dúvida sobre qual modelo seguir pois muitos até hoje não sabem quais as diferenças entre um desenvolvimento nativo e híbrido, vantagens e desvantagens de cada um e qual abordagem usar. Por meio desta revisão de literatura apresento por meio de pesquisa e comprovação empírica as diferenças e vantagens entre desenvolvimento nativo e híbrido bem como um estudo dos frameworks de desenvolvimento híbrido, apresento os dois mais famosos e mais usados frameworks de desenvolvimento nativo usados hoje, além de sanar todas as dúvidas sobre o assunto e diferenças de performance, desenvolvimento, compatibilidade, interface, custo, manutenção e segurança.

Palavras-chave: Desenvolvimento, Nativo, Híbrido, Aplicação, Estrutura

Abstract

With the advancement of technology and especially smartphones, companies working in the field of mobile application development have had to deal with major problems such as complexity, cost and time to develop an app for different operating systems. Over time, the hybrid development model was introduced through frameworks and there was a doubt about which model to follow because many still do not know the differences between native and hybrid development, the advantages and disadvantages of each and which approach to use. Through this literature review, I present through research and empirical evidence the differences and advantages between native and hybrid development as well as a study of hybrid development frameworks, I present the two most famous and most used native development frameworks used today, in addition to solve all doubts about the subject and differences in performance, development, compatibility, interface, cost, maintenance and security.

Keywords: Development, Native, Hybrid, Application, Framework

1. INTRODUÇÃO

Com a adoção de grande parte da população, a quantidade de celulares e smarthphones cresceu, e com ela, a indústria de desenvolvimento de aplicativos móveis vem se desenvolvendo em ritmo acelerado, trazendo consigo uma grande demanda desenvolvimento de aplicativos que supram todos os tipos de necessidades.

Porém, os diversos sistemas operacionais disponíveis no mercado são um empecilho para os desenvolvedores de aplicativos, pois construir um único aplicativo para todos os sistemas operacionais se torna dificultoso, já que no desenvolvimento, a codificação de um app nativo é completamente diferente de um sistema operacional para outro.

Era de se esperar que com o tempo surgissem ferramentas que auxiliariam no processo de desenvolvimento, como os frameworks, que compilam e traduzem o mesmo código, escrito em uma única linguagem, para a linguagem nativa daquela plataforma. O desenvolvimento de aplicativos móveis de plataforma híbrida ajuda na redução de custos e na economia de tempo, além de fornecer componentes para facilitar o desenvolvimento de aplicativos que proporcionam uma sensação nativa ao usuário.

Considerando a variedade de dispositivos celulares presentes hoje em dia e as diversas plataformas diferentes presente nesses celulares, era notório a enorme demanda do mercado para atender e incluir o maior número de plataformas distintas, visando agilizar o processo de desenvolvimento e a melhor qualidade do produto com o menor custo possível.

Ao se desenvolver um aplicativo para sua linguagem nativa, como por exemplo o Android que utiliza a linguagem Java e o iOS que utiliza o Swift, é necessário que o app seja construído mais de uma vez caso seja de interesse da empresa viabilizá-lo em mais de uma plataforma. Isso além de tornar todo o processo custoso e demorado não é nada vantajoso para o desenvolvedor ter que criar o mesmo app com diversos códigos fontes totalmente diferentes pra atender cada plataforma.

O problema de pesquisa deste trabalho foi: O que são frameworks híbridos e quais as vantagens e desvantagens no desenvolvimento mobile híbrido em relação ao desenvolvimento nativo?

O objetivo geral deste foi analisar e apresentar por meio de pesquisa e comprovação empírica as diferenças e vantagens entre desenvolvimento nativo e híbrido bem como um estudo dos frameworks de desenvolvimento híbrido.

Enquanto os objetivos específicos foram conceituar a ideia de desenvolvimento híbrido, apresentar modelos de frameworks híbridos e suas singularidades através de uma abordagem prática e comparar o desenvolvimento de aplicativos híbridos com o de aplicativos nativo.

Foi realizada uma revisão de literatura, onde foram pesquisados livros, dissertações e artigos científicos selecionados através de busca nas seguintes bases de dados (livros, artigos científicos, endereços web etc.) a fim de disponibilizar ao usuário um conteúdo informativo com embasamento empírico acerca do desenvolvimento de aplicações nativas e híbridas. O período dos artigos pesquisados serão os trabalhos publicados nos últimos 10 anos. As palavras-chave utilizadas na busca serão: Aplicativos, desenvolvimento e aplicativos híbridos etc.

O presente trabalho visa apresentar formas eficazes de se resolver os problemas aci-

ma citados, apresentando vantagens e desvantagens entre os tipos de desenvolvimento mobile, além de auxiliar e contribuir para com a comunidade desenvolvedores, propondo entender melhor o mundo do desenvolvimento móvel levando em consideração pontos importantes e que é possível desenvolver um app em menor tempo, menos custo e entregando uma excelente experiência no produto final.

2. APLICATIVOS MÓVEIS

Os aplicativos móveis ou mobile apps surgiram em decorrência da evolução tecnológica dos smartphones. Segundo os dizeres de Silva, Pires e Carvalho Neto (2015), os aplicativos foram desenvolvidos com o propósito de serem executados através desses dispositivos móveis. Venteu e Pinto (2014) afirmam que um aplicativo móvel pode ser baixado diretamente do aparelho eletrônico, desde que o dispositivo possua conexão com a Internet.

Os aplicativos são normalmente conhecidos como “apps” ou “app mobile”. A sigla “app” é uma abreviatura de “aplicação de software”. Em 2010, o termo se tornou tão popular q foi reconhecido como “palavra do ano” pela American Dialect Society.

2.1 Desenvolvimento de aplicativos móveis

Segundo El-Kassas et al. (2015), o desenvolvimento de aplicativos móveis diferencia-se do desenvolvimento de outros tipos de software por possuir particularidades e restrições. Os desenvolvedores devem ter em mente aspectos como as capacidades e especificações dos dispositivos móveis, a mobilidade, o design e navegabilidade de interface gráfica, segurança e privacidade do usuário. De acordo com Corral, Janes e Remencius (2012), aplicações móveis são desenvolvidas dinamicamente e lançadas no mercado em pequenos ciclos. Os produtos finais costumam ser de pequeno porte e comercializados a preços baixos. As equipes de desenvolvimento também tendem a ser pequenas.

2.2 Tipos de aplicativos móveis

No panorama geral de desenvolvimento de aplicações móveis temos 3 vertentes de aplicativos que podem ser desenvolvidos, são eles: aplicativos nativos, aplicativos híbridos e web apps. Neste trabalho analisaremos as diferenças apenas entre híbrido e nativo.

2.3 Diferenças entre nativos e híbridos

Muitos pontos devem ser levados em conta na hora de decidir em que plataforma será desenvolvida o app e qual o tipo de desenvolvimento que vai suprir as necessidades, dentre elas temos: o custo o tempo de desenvolvimento, visando as necessidades da empresa, e confiabilidade, rapidez e segurança, visando as necessidades do usuário.

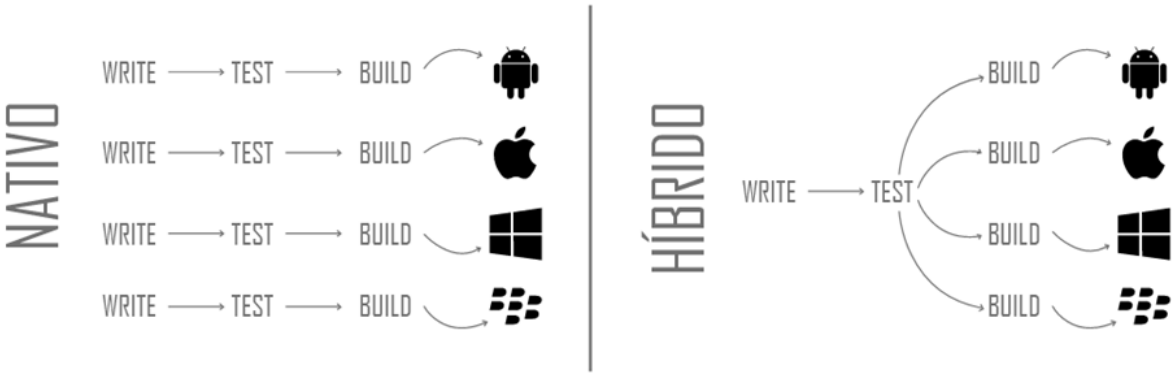


Figura 1 – Diferenças entre o desenvolvimento nativo e híbrido

Fonte: autor (2022)

2.3.1 Aplicativos nativos

Os aplicativos nativos móveis são desenvolvidos usando as ferramentas e linguagens de programação fornecidas para uma determinada plataforma móvel.

De acordo com Madureira (2017), o aplicativo nativo é programado na linguagem de cada sistema operacional, como Java no Android e Objective-C no iOS, cada plataforma apresentando suas próprias ferramentas e elementos de interface. Esses aplicativos são executados apenas em celulares com a plataforma de destino, além de levar mais tempo e ser mais trabalhoso, porém permitem que o aplicativo tenha acesso completo a funcionalidades e recursos do dispositivo.

Por serem desenvolvidos de acordo com as necessidades de um único sistema operacional, os aplicativos nativos tendem a ser mais performáticos e otimizados.

2.3.2 Aplicativos híbridos

Também conhecido como Cross-Plataform Development (Desenvolvimento Multiplataforma), o aplicativo híbrido móvel combina o aplicativo web e o aplicativo nativo. Ele é desenvolvido usando as tecnologias da Web (HTML5, CSS3 e JavaScript), como o Web App, mas é renderizado dentro do aplicativo nativo usando um controle de visualização da Web. Os recursos do dispositivo são expostos ao aplicativo híbrido por meio de uma camada de abstração (APIs JavaScript).

Não é aprovada a ideia de ter que repetir todo o trabalho mais de uma vez em linguagens de programação diferentes. Além da perda de tempo em fazer o trabalho, falhas encontradas posteriormente provavelmente também terão que ser corrigidas mais de uma vez (MADUREIRA, 2017).

O desenvolvimento desses aplicativos leva menos tempo, já que é preciso escrever o código apenas uma vez para que ele seja posteriormente compilado e distribuído em todas as plataformas, não havendo a necessidade de desenvolver o mesmo aplicativo outras vezes em outras linguagens para plataformas distintas.

O desenvolvimento híbrido é uma ótima opção para situações em que não há necessidade de alta performance do aplicativo, pois não funcionam tão rápido quanto um aplicativo nativo (MADUREIRA, 2017).

Como cita Stark (2010), em essência, aplicações híbridas são web app empacotadas em um aplicativo nativo.

3. FRAMEWORKS: O QUE SÃO E QUAIS USAR

Framework é uma “base” de onde se pode desenvolver algo maior ou mais específico. Uma coleção de códigos-fonte, classes, funções, técnicas e metodologias que facilitam o desenvolvimento de novos softwares (MINETTO, 2007, p. 17).

Segundo Silva (2000, p. 21) “Frameworks são estruturas de classes que constituem implementações incompletas que, estendidas, permitem produzir diferentes artefatos de software. A grande vantagem desta abordagem é a produção de reuso de código e projeto, que pode diminuir o tempo e o esforço exigidos na produção de software”.

Em outras palavras, frameworks são coleções de funções e ferramentas que facilitam e criam um ambiente de desenvolvimento de software reusável, aumentando a produtividade, exigindo menor esforço e oferecendo códigos consistentes e robustos, com reconhecido padrão de qualidade, legibilidade e manutenibilidade, cada framework possui suas vantagens e singularidades (CRISPINIANO, 2021, p. 6).

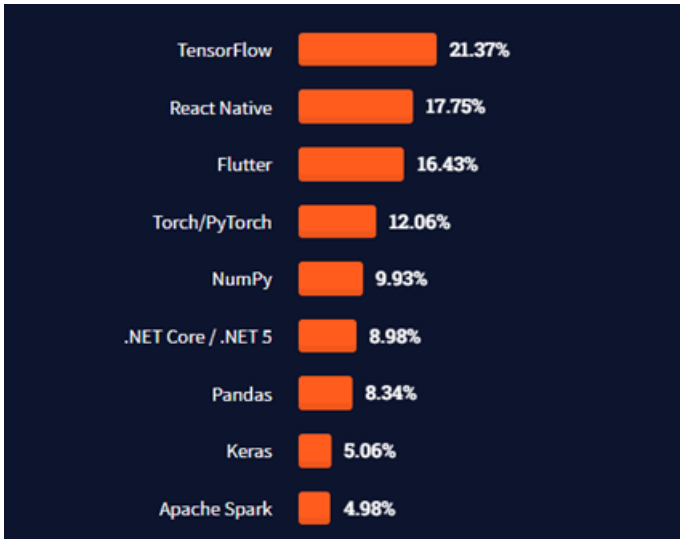


Figura 2 – Pesquisa sobre frameworks e bibliotecas mais populares em 2021

Fonte: Stack Overflow (2021)

De acordo com a pesquisa, React Native e Flutter constam, respectivamente, como os frameworks cross-platform (plataforma cruzada, ou multiplataforma) mais procurados pelos desenvolvedores.

3.1 React Native

De acordo com o livro Learning React Native (EISENMAN, 2018, p. 17) “React Native é um framework JavaScript utilizado para escrever aplicações reais e de renderização nativa para iOS e Android”.

O React Native foi lançado publicamente em 2015, usa a mesma linguagem e sintaxe do seu equivalente web, o React JS, ou seja, foi construído com base no React, esse fator o torna muito querido pela comunidade devido a sua reusabilidade de código.

O React JS foi desenvolvido por Jordan Walke, um engenheiro de software do Facebook, lançado em 2012 e sendo mantida atualmente pelo Facebook, também considerado um dos frameworks web mais utilizados no mundo, de acordo com os dados do Stack Overflow (2021).

Segundo com Cunha (2022), logo depois, em 2013, o mesmo Jordan Walke, fez uma descoberta inovadora: ele encontrou um método de gerar elementos de interface do usuário para aplicativos iOS com o JavaScript; ou seja, conseguiu desenhar uma tela de app com Javascript.

Learn once, write anywhere (aprenda uma vez e escreva em qualquer lugar), esse é o objetivo que o React quer implantar, ou seja, assim como funciona com a lógica de programação, uma vez que você aprende os conceitos do React você consiga transcrevê-las em qualquer linguagem.O React Native tem como exemplo aplicativos mundialmente famosos como Discord, Tesla, Instagram, Facebook...

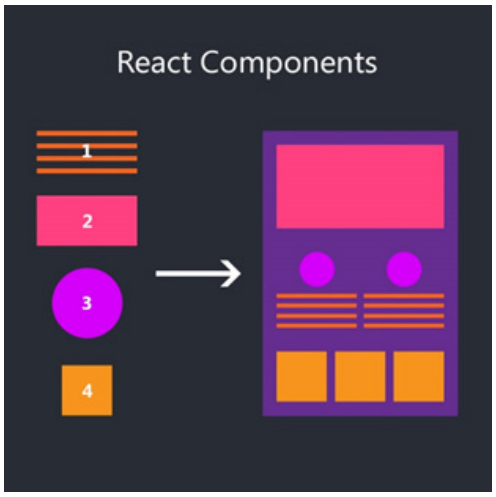


Figura 3 – Arquitetura baseada em componentes do React

Fonte: Tech Diagonal (2019)

Figura 4 – Exemplo de construção dos componentes no React Native

Fonte: Tech Diagonal (2019)

Esse framework utiliza de uma arquitetura baseada em componentes, estes que facilitam o desenvolvimento de um aplicativo multiplataforma, sendo alguns destes os mesmos componentes das aplicações nativas como View, Text and Image, que que são mapeados diretamente para os blocos de construção nativos da interface do usuário da plataforma, trazendo uma liberdade enorme e uma facilidade ao criar interfaces e sistemas tanto pro Android quanto pro iOS (REACT NATIVE, 2022)

3.1.1 Estrutura de pastas do React Native

Existe um padrão bastante utilizado pelos desenvolvedores do React Native quanto à questão de organização e estruturação de pastas e arquivos, apesar de não ser uma regra (ALURA, 2019).

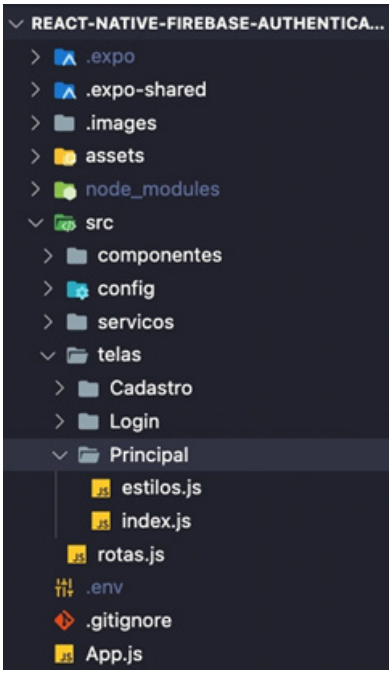


Figura 5 – Sugestão de organização de pastas e arquivos no React Native

Fonte: Alura (2019)

Normalmente uma estrutura de um App React Native é organizada da seguinte forma:

- assets: Pasta para armazenar todas as imagens, fontes etc;
- src: esta pasta é o container principal de todo o código dentro de sua aplicação, ou seja, isso significa que essa pasta guarda todo o código;
- componentes: Pasta para armazenar qualquer componente comum que você usa em seu aplicativo. Exemplo: um botão, cabeçalho, card etc;
- constantes: Pasta para armazenar qualquer tipo de constante que você tenha;
- rotas.js: arquivo para armazenar as rotas das telas do App;
- context: Esta pasta contém todos os seus Context API. Ou seja, serve para autenticação, armazenamento de dados de formulários, configurações de temas ou outras funcionalidades
- telas: Pasta que contém todas as telas/recursos do seu aplicativo;

- servicos: Controlador de API ou serviços externos.
- utils: Pasta para armazenar qualquer função comum, como formatador de data, cálculo de tempo e por aí vai.
- App.js: componente principal que inicia todo o seu aplicativo;
- index.js: Ponto de entrada do seu aplicativo de acordo com os padrões React-Native. No Expo esse arquivo não é necessário.

3.1.2 Estrutura de código do React Native

Dentro de cada tela ou componente, temos uma estrutura muito padrão conforme o código apresentado na figura abaixo:

Figura 6 – Exemplo de código de um componente de botão no React Native

Fonte: Alura (2019)

Como pode-se observar, os componentes ou telas são criadas no React Native, assim como no React, nada mais são do que funções e, dentro dela, temos diversos elementos do React Native, como View, Text, TouchableOpacity e entre outros.

3.2 Flutter

Os aplicativos Flutter são escritos na linguagem de programação chamada Dart, que também pertence e é mantida pelo Google. É bastante utilizado no mercado e vem se destacando ainda mais pelos seus recursos e componentes que facilitam a construção de UI e facilidade de aprendizado. O Flutter continua em constante atualização e, como cita Alberto, agora permite também a criação de aplicações para desktop (Linux, Windows e macOS), torando-se assim uma ferramenta bastante maleável no mercado (ALURA, 2022).

Como cita Windmill (2019, p. 1) “é uma plataforma que fornece tudo o que você precisa para criar aplicativos: mecanismo de renderização, componentes da UI, estruturas de testes, ferramentas, um host e muitos outros recursos necessários para criar um aplicativo”.

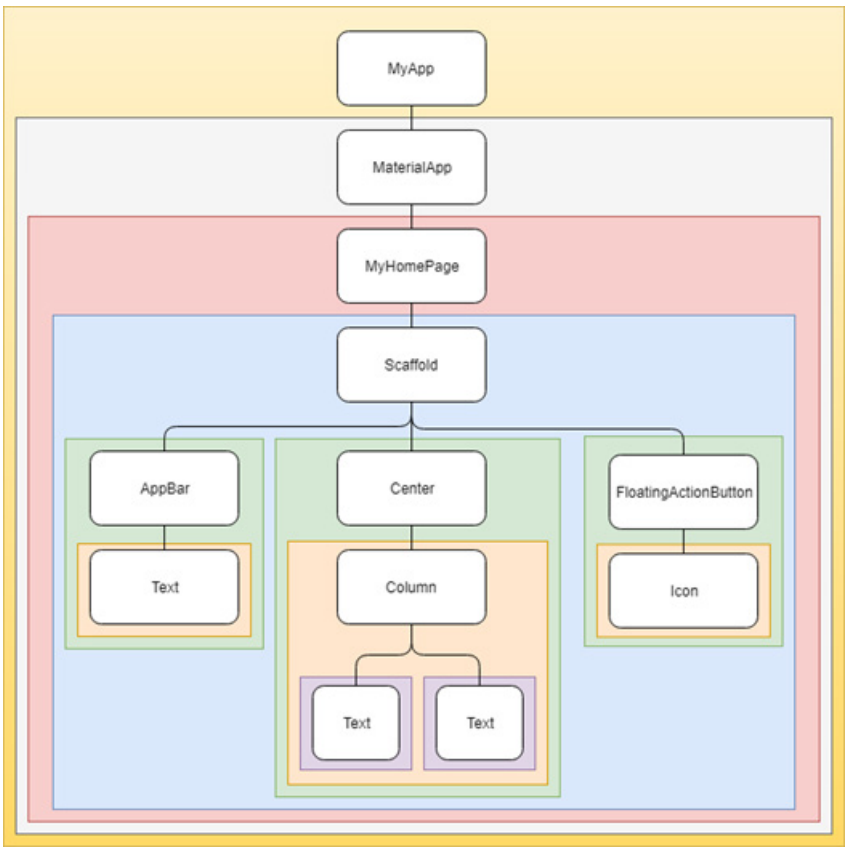


Figura 7 – Árvore de construção de widgets do Flutter

Fonte: Didier Boelens (2018)

O Flutter também conta com diversos Widgets, que são como pacotes, ou blocos de construção já prontos de elementos estruturais, como menus, opções de layout, botões e etc, que podem ser usados ou criados “do zero”, a qual os montamos e encaixamos para montar as telas de um aplicativo. Segundo Negri (2021), os widgets facilitam bastante a vida do desenvolvedor, tornando a velocidade de construção de uma aplicação relativamente rápida.

3.2.1 Estrutura de pastas do Flutter

Assim como no React Native, é importante manter nosso projeto organizado e bem estruturado, tanto para posteriormente realizar uma melhor leitura do código, quanto para que sua manutenção e melhorias possam ocorrer mais facilmente.

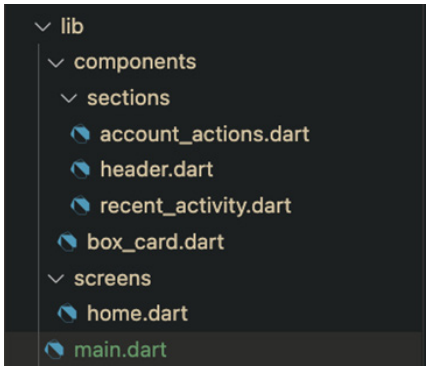


Figura 8 – Sugestão de organização de pastas e arquivos no Flutter

Fonte: Alura (2019)

Segundo Negri (2021), de acordo com as boas práticas, é recomendável deixar na raiz da pasta “lib” apenas o arquivo “main.dart”. Quaisquer outras ou componentes devem ficar dentro de outras pastas separadas e organizadas dentro da pasta “lib”.

Dentro do arquivo “main.dart” deve ficar apenas a estrutura mínima para chamar o app. E a página inicial deve ser importada da pasta “screens”.

Logo, a estrutura de pastas e arquivos fica da seguinte forma:

- lib: Pasta raíz onde deve ficar apenas o arquivos main.dart, e as demais pastas da aplicação;
- components: pasta onde vão ficar os componentes e seções da aplicação;
- sections: pasta onde ficarão alguns blocos de construção e elementos;
- screens: esta pasta onde ficam as telas da aplicação;
- home.dart: arquivo inicial da aplicação, chamado pelo main.dart;
- main.dart: inicializa a aplicação e chama a página inicial home.dart.

3.2.2 Estrutura de código do Flutter

Exemplificando uma estrutura de componente na tela inicial do Flutter, temos a seguinte imagem:

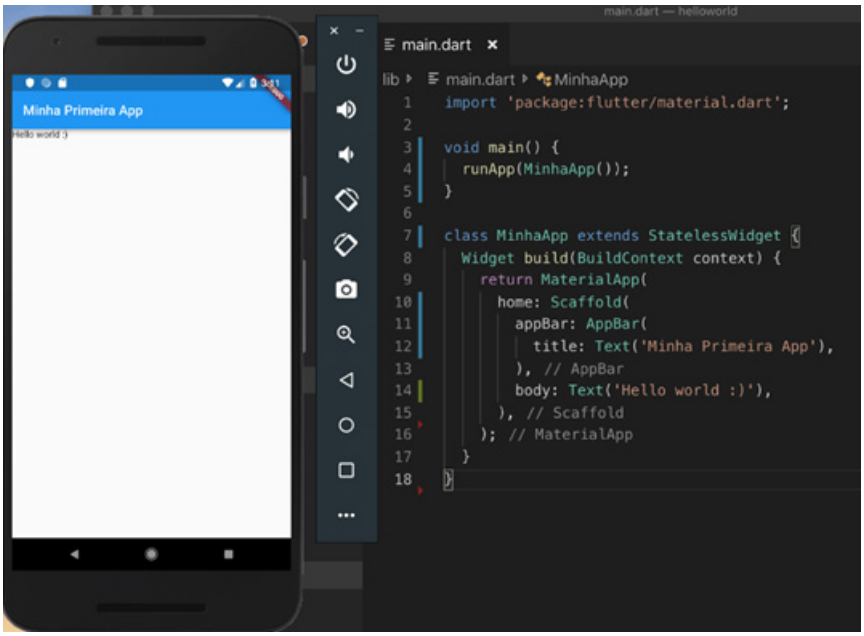


Figura 9 – Exemplo de código de um componente com material design no Flutter

Fonte: Alura (2018)

Nesse exemplo de código simples podemos ver o “main” chamando e executando a classe “MinhaApp” para rodar na tela. Já na classe “MinhaApp” construímos um widget que retorna um componente do material design.

Como cita Souto (2019), o componente “Scaffold”, serve como uma estrutura para inserirmos componentes em lugares comuns do material design como a barra do topo, um botão no Floating Action Button e uma entrada para colocarmos o corpo(body) da nossa tela, construindo uma aplicação com uma estrutura baseada no material design.

4. VANTAGENS E DESVANTAGENS

Existem vários prós e contras tanto no uso da metodologia de desenvolvimento híbrida quanto na nativa. Nesta seção discutiremos quais as vantagens desvantagens de cada uma delas.

4.1 Tempo de desenvolvimento

No geral, aplicativos são mais rápidos de se desenvolver e levam um tempo consideravelmente menor do que os nativos. É mencionado que "A longo prazo, a maior desvantagem dos aplicativos híbridos é que a empresa gastará mais tempo consertando e aprimorando o aplicativo devido a reclamações dos usuários sobre elementos da interface do usuário ou problemas de desempenho" (MAGEDA, 2021).

4.2 Custo de desenvolvimento

É mais econômico desenvolver aplicativos usando tecnologias híbridas já que você precisa codificar o app apenas uma vez e em uma única linguagem e enviá-los para diferentes plataformas (Android ou iOS).

Descrição	Projetos de pequeno/médio porte Custo médio de desenvolvimento Desenvolvimento Nativo	Projetos de pequeno/médio porte Custo médio de desenvolvimento Desenvolvimento Híbrido
Programador back-end, APIs, admin e cloud deployment	$10,000 - $20,000	$10,000 - $20,000
Desenvolvimento iOS nativo	$15,000 - $30,000	$0
Desenvolvimento Android nativo	$10,000 - $20,000	$0
Desenvolvimento Híbrido usando algum framework	$0	$10,000 - $20,000
Total	$35,000 - $70,000	$20,000 - $40,000

Tabela 1 – Estimativa do custo de desenvolvimento entre nativo e híbrido.

Fonte: Adaptado de *International Journal of Computer Applications* (0975 – 8887) Volume 118 – No.15, May 2015

Desenvolver um app usando tecnologias nativas pode sair bem mais caro pois, quase sempre, é necessário um desenvolvedor (ou um time) especialista para cada tipo de sistema operacional.

4.3 Design de interfaces

As interfaces móveis podem ser projetadas usando tecnologias nativas e híbridas. No entanto, é mais flexível no design de interfaces usando tecnologias de plataforma híbrida, como HTML5 e CSS3, ou CSS in JS usando bibliotecas como Styled-Components, tendo

em vista que se pode fazer qualquer interface com essas ferramentas. De acordo com Saccomani (2018), há certos problemas de design quando se trata de para projetar interfaces com tecnologias de plataforma híbrida, pois algumas interfaces mais complexas podem ser mais demoradas a serem desenvolvidas se consideramos alguns recursos e tecnologias de plataformas nativas, que fornecem diferentes ferramentas de design para criar interfaces padrão que não estão disponíveis com ferramentas de plataforma híbrida.

4.4 Performance e experiência do usuário

Os aplicativos nativos tendem a fornecer melhor desempenho, experiência responsiva e fluida ao usuário sem atrasos do que os aplicativos de plataforma híbrida, pois os mesmos conversam diretamente com o hardware e com o sistema. Alguns exemplos de perda de performance são:

Os cliques são mais responsivos no caso de aplicativos nativos, com o híbrido o usuário pode ter que clicar mais de uma vez para obter uma resposta específica do aplicativo, o que pode causar certa frustração e insatisfação.

A rolagem(scroll) em um aplicativo nativo é perfeita, suave e fluída, mas no caso de um aplicativo híbrido, o usuário pode sentir um atraso no carregamento de quadros na sequência, dependendo de como a interface foi construída. Como cita Saccomani (2018), as animações em um aplicativo nativo podem ser executadas com grande fluidez, mas no caso de um aplicativo híbrido, algumas animações podem não se comportar perfeitamente. Jogos por exemplo se encaixam melhor no desenvolvimento nativo, pois os mesmos necessitam de um maior desempenho e menos tempo de resposta.

4.5 Segurança

Dependendo dos requisitos de segurança do projeto, os aplicativos nativos podem fornecer um ambiente de segurança melhor, no entanto, a maioria dos problemas de segurança são criados com base na falta de conhecimento do desenvolvedor e em certos problemas de segurança do lado do servidor.

“Entretanto, aplicações nativas, por usarem APIs nativas, recorrem a protocolos de segurança conhecidos, já as aplicações híbridas recorrem a plug-ins externos para garantir uma maior segurança, porém como utilizam o mesmo código que tecnologias web, tornam-se potencialmente mais vulneráveis” (GOLD, 2022).

4.6 Manutenção

Segundo Ferroni (2021), no aspecto de manutenção, o aplicativo híbrido leva vantagem, pois é possível acrescentar funções ou fazer ajustes necessários e, devido a sua linguagem ser simplificada, este processo torna-se muito mais rápido que um nativo. Já nas aplicações nativas a manutenção tende a ser muito mais complexa e demorada, por cada plataforma utilizar um código específico, além de que exige que a manutenção de cada versão de cada plataforma seja feita individualmente.

4.7 APIs de integração

Sobre o desenvolvimento de apps, no início, o desenvolvimento nativo tinha uma grande vantagem sobre o desenvolvimento nativo, que era a integração do aplicativo com os demais recursos do aparelho móvel, pois o desenvolvimento nativo poderia usar de APIs nativas para se comunicar com outros recursos, como câmera, contatos, notificações, geolocalização etc.

Porém com o avanço de desenvolvimento web, hoje temos os mesmos recursos disponíveis no desenvolvimento de aplicativos híbridos, sendo eles:

- Câmera
- Notificações de push
- Contatos
- Acesso Offline ao app
- Geolocalização
- Upload de arquivos
- Giroscópio
- Acelerômetro
- Microfone
- Poucos recursos ainda não podem ser utilizados por aplicativos híbridos, são eles:
- Detecção facial
- Reconhecimento de fala
- Sensores de proximidade
- Geofencing

Nas tabelas logo abaixo temos uma comparação entre o desenvolvimento entre aplicativos nativos e híbridos com alguns pontos importantes.

Figura 10 – Tabela comparativa entre apps nativos e híbridos

Fonte: IGTI (2020)

Características	Nativo	Híbrido
Performance	As aplicações nativas tendem a ser sempre mais rápidas e fluidas.	Aplicações híbridas aplicam camadas de tecnologia, como WebViews e outros plug-ins, o que tem impacto na performance em comparação com aplicações nativas.
Desenvolvimento	O desenvolvimento é focado em um sistema e uma linguagem específica. Exigindo do desenvolvedor uma expertise na plataforma ao qual se deseja desenvolver.	Desenvolver de forma híbrida faz com que o profissional precise dominar HTML, Java Script e CSS. Além de ter bons conhecimentos em um framework para criação de aplicativos mobile.
Uso offline	Aplicações nativas permitem que o usuário possa utilizar determinados recursos e funcionalidades sem a necessidade de conexão com a internet.	Assim como as aplicações nativas, também permitem que o usuário possa utilizar os recursos e funcionalidade do app sem a necessidade de internet.
Compatibilidade	O foco de uma aplicação nativa é atingir uma única plataforma. Cada aplicação só tem compatibilidade a versões do sistema operacional de uma plataforma única.	O desenvolvimento de aplicações híbridas tem um foco em tornar com que o código desenvolvido tenha a maior compatibilidade possível entre plataformas diferentes.
Recursos disponíveis	Os recursos disponíveis são específicos a cada plataforma; no entanto, apresentam a vantagem de existirem APIs nativos para sistemas operativos.	Existe uma grande variedade de recursos disponíveis para aplicações híbridas, desenvolvidas em diversas tecnologias web para maior acessibilidade e flexibilidade.
Interface	Aplicações nativas beneficiam das funcionalidades de UI dos sistemas operacionais sem complicações.	Aplicações híbridas precisam de plug-ins ou técnicas complexas para imitar os UI nativos dos sistemas operacionais.
Custo de desenvolvimento	Mais caro, devido a necessidade de desenvolver-se o app para uma única plataforma e necessitar seguir os padrões da mesma.	Mais barato, levando em consideração o alcance de plataformas diferentes.
Manutenção	Ao utilizar código específico por plataforma e constringido às suas especificações, a manutenção é mais complexa, mais dispendiosa e mais demorada, para além de que exige que a manutenção de cada versão de cada plataforma seja gerida individualmente.	Ao utilizar tecnologia web partilhada por várias plataformas, aplicações híbridas têm manutenção mais fácil e mais acessível em termos de tempo e custo, sobretudo em casos de aplicações multiplataforma.
Segurança	Graças a APIs nativos, aplicações nativas recorrem a protocolos de segurança conhecidos, para além da própria segurança adicional fornecida pela interação nativa com a plataforma.	Aplicações híbridas recorrem a plug-ins externos para garantir maior segurança e utilizam código comum a tecnologias web, logo, potencialmente mais vulnerável.

Figura 11 – Tabela comparativa entre características apps nativos e híbridos

Fonte: MEDIUM (2018)

Entendo as diferenças de cada tecnologia, cabe desenvolvedor saber colocar em uma balança todos os prós e contras dos nativos e híbridos para criar um software capaz de oferecer os melhores serviços aos usuários além de trazer maiores benefícios ao desenvolvedor ou empresa.

5. CONSIDERAÇÕES FINAIS

Há uma grande variedade de frameworks para o desenvolvimento mobile, seja ele híbrido ou nativo, o que torna muito difícil a sua avaliação e escolha devido a suas diferenças, vantagens e desvantagens. O levantamento de critérios auxilia a escolha de cada método de desenvolvimento para uma determinada situação ou objetivos que a empresa ou o programador deseja alcançar, pois permite a tabulação das características de cada artefato estudado, facilitando assim a análise.

O estabelecimento de critérios, embora subjetivos, deve auxiliar futuras avaliações de não só de diferentes formas de desenvolvimento como de diferentes frameworks, permitindo que o analista investigue diretamente de forma simples e clara cada um de seus pontos.

Para a escolha da melhor metodologia deve-se também levar em consideração os objetivos das aplicações e da equipe de desenvolvimento. Entretanto, o estudo feito deve facilitar na análise numa situação específica, uma vez fez-se o levantamento e comparativo de dados e seu embasamento está incluso no trabalho.

Referências

Aplicativo nativo, híbrido e webapp: o que são e qual o melhor? Disponível em: <https://usemobile.com.br/aplicativo-nativo-web-hibrido/#nativo-hibrido-qual-melhor>. Acesso em: 20 maio. 2022.

Aplicativo nativo, híbrido ou PWA: qual é a melhor escolha? Disponível em: <https://imaginedone.com.br/blog/web-e-mobile/aplicativo-nativo-hibrido-pwa/>.

Acesso em: 20 maio. 2022.

DA SILVA, Marcelo Moro; SANTOS, Marilde Terezinha Prado. **Os paradigmas de desenvolvimento de aplicativos para aparelhos celulares**. Revista TIS, v. 3, n. 2, 2014.

CORRAL, L.; JANES, A.; REMENCIUS, T. **Potential Advantages and Disadvantages of Multiplatform Development Frameworks - A Vision on Mobile Environments.** Procedia Computer Science, v. 10, p. 1202–1207, jan. 2012. ISSN 1877-0509. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1877050912005303>. Acesso em 04 jun. 2022.

CRISPINIANO, Almir; **Estudo Comparativo entre Frameworks Frontend para a Criação de um Progressive Web App (PWA)**. Ciência da Computação, Universidade Federal de Campina Gande – PB, 2021.

CUNHA, A**. O que é React Native? Vantagens e Guia do Framework.** Disponível em: <https://www.alura.com.br/artigos/react-native. Acesso em: 2 nov. 2022>.

Diferença entre aplicativos nativos e híbridos. Disponível em: <https://mageda.digital/blog/diferenca-entre-aplicativos-nativos-e-hibridos/>. Acesso em: 16 nov. 2022.

EISENMAN, Bonnie. **Learning React Native. Building Native Mobile Apps with JavaScript.** Printed in the United States of America. Published by O'Reilly Media, Inc, Outubro de 2017. Acesso em: 10 de abr. 2022.

EL-KASSAS, W. S. et al. **Taxonomy of Cross-Platform Mobile Applications Development Approaches.** Ain Shams Engineering Journal, 2015. ISSN 2090-4479. Disponível em: <http://www.sciencedirect.com/science/article/pii/S2090447915001276>. Acesso em: 23 abr. 2022.

FERRONI, C. **Híbrido ou nativo: pontos positivos, negativos e por onde começar**. Disponível em: <https://blog.tecnospeed.com.br/aplicativo-hibrido-ou-nativo/>. Acesso em: 14 nov. 2022.

FONTES, Henrique. **Mercado de aplicativos cresce no Brasil e alunos da USP em São Carlos conquistam espaço no cenário.** Jornal da USP.São Carlos, 21 set. 2016. Disponível em: <http://jornal.usp.br/universidade/mercado-de-aplicativos-cresce-no-brasil-e-alunos-da-usp-em-sao-carlos-conquistam-espaco-no-cenario/>. Acesso em: 01 maio. 2022.

GOLD, F. **Native or Hybrid App - Which is More Secure?** Disponível em: <https://turingpoint.de/en/blog/native-or-hybrid-app-which-is-more-secure/>. Acesso em: 08 nov. 2022.

HOLLA, S. Chapter 3 – **Understanding ReactJS Components – Techdiagonal.** Disponível em: <https://www.techdiagonal.com/reactjs_courses/beginner/understanding-reactjs-components/>. Acesso em: 4 out. 2022.

KHANDEPARKAR, Anmol; GUPTA, Rashmi; SINDHYA, B. **An introduction to hybrid platform mobile application development.** International Journal of Computer Applications, v. 118, n. 15, 2015.

MADUREIRA, Daniel. **Aplicativo nativo, web App ou aplicativo híbrido?** Disponível em: <https://usemobile.com.br/aplicativo-nativo-web-hibrido/>. Acesso em: 10 abr. 2022.

MINETTO, Elton Luis. **Frameworks para Desenvolvimento em PHP.** São Paulo: Novatec Editora Ltda, 2007.

NEGRI, P. **Saiba o que é flutter e quais são as suas vantagens.** Disponível em: <https://www.iugu.com/blog/o-que-e-flutter>. Acesso em: 10 nov. 2022.

NEVES, Jonathan; JUNIOR, Vilmar Mendes. **Uma análise comparativa entre flutter e react native como frameworks para desenvolvimento híbrido de aplicativos mobile: Estudo de caso visando produtividade.** Ciência da Computação-Tubarão, 2020.

React Native. Disponível em: <https://reactnative.dev>. Acesso em: 16 nov. 2022.

SACCOMANI, P. **Native, Web or Hybrid Apps? What's The Difference?** Disponível em: <https://www.mobiloud.com/blog/native-web-or-hybrid-apps>. Acesso em 16 nov. 2022.

SILVA, Leandro Luquetti B. da; PIRES, Daniel Facciolo; CARVALHO NETO, Silvio. **Desenvolvimento de Aplicações para Dispositivos Móveis: Tipos e Exemplo de Aplicação na plataforma iOS.** II Workshop de Iniciacao Cientifica em Sistemas de Informacao, Goiania, p. 25-30, maio. 2015. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/wicsi/2015/004.pdf>. Acesso em: 22 maio. 2022

SILVA, M. **O que é melhor, desenvolver uma aplicação móvel nativa, híbrida ou um web app?** Disponível em: <https://medium.com/seedabit/o-que-é-melhor-desenvolver-uma-aplicação-móvel-nativa-híbrida-ou-um-web-app-e6cc6fd23173>. Acesso em: 10 maio. 2022.

SILVA, R. P. **Suporte ao desenvolvimento e uso de frameworks e components.** Porto Alegre, 2000, 262 p. Tese (Doutorado em Ciência da Computação) – Instituto de Informática, Universidade Federal do Rio Grande do Sul.

SOUTO, M. **Flutter e o seu primeiro hello world.** Disponível em: <https://www.alura.com.br/artigos/como-criar-um-projeto-com-flutter-hello-world>. Acesso em: 16 nov. 2022.

Stack Overflow Developer Survey 2022. Disponível em: <https://survey.stackoverflow.co/2022/#most-loved-dreaded-and-wanted-misc-tech-want>. Acesso em: 18 nov. 2022.

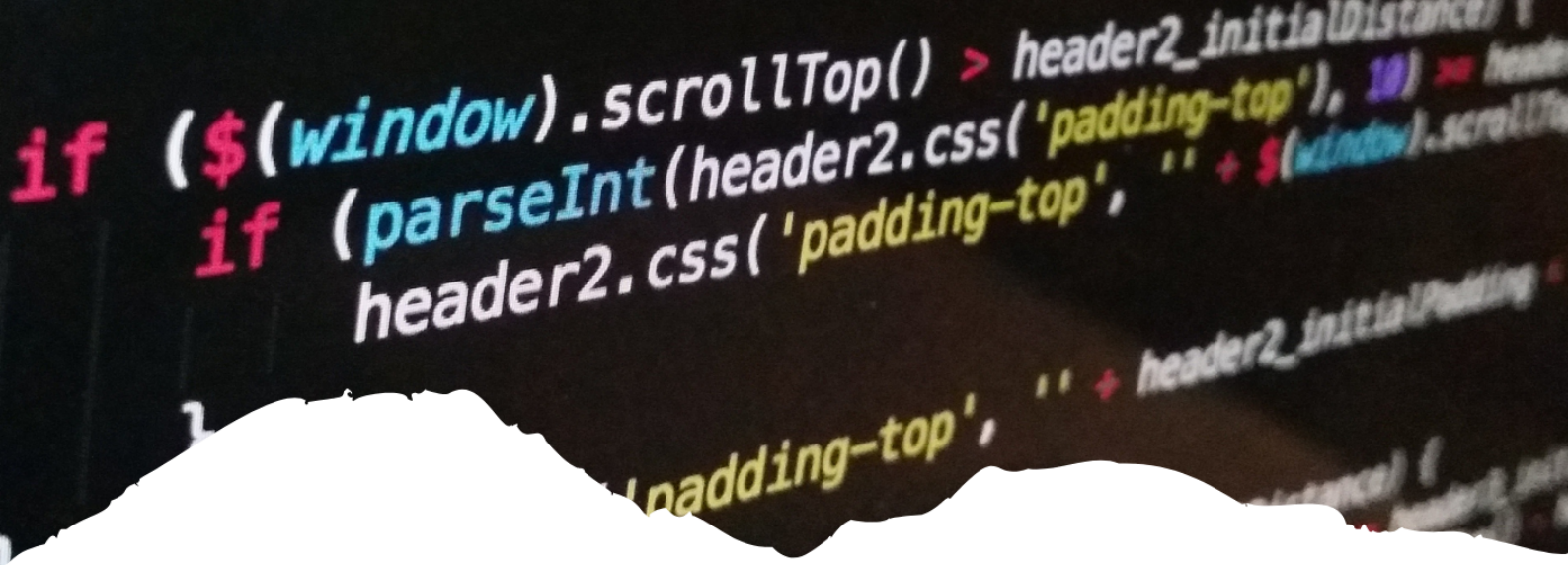
STANGARONE, J. **The Mobile App Comparison Chart: Hybrid vs. Native vs. Mobile Web (2019 Update).** Disponível em: <https://www.mrc-productivity.com/blog/2019/10/the-mobile-app-comparison-chart-hybrid-vs-native-vs-mobile-web>. Acesso em: 02 out. 2022.

VENTEU, K. C.; PINTO, G. S. **DESENVOLVIMENTO MÓVEL HÍBRIDO.** Revista Interface Tecnológica, [S. l.], v. 15, n. 1, p. 86–96, 2018. DOI: 10.31510/infa.v15i1.337. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/337>. Acesso em: 2 maio. 2022.

What is the difference between Hybrid and Native App? Disponível em: <https://sannacode.com/blog/what-difference-between-hybrid-and-native-app>. Acesso em: 12 maio. 2022.

What Web Can Do Today. Disponível em: <https://whatwebcando.today>. Acesso em: 20 maio. 2022.

WINDMILL, Eric. **Flutter in Action.** Shelter Island, New York. Manning Publications, Dezembro de 2019.



21

BANCO DE DADOS RELACIONAL

RELATIONAL DATABASE

João Victor Correia Damasceno

Resumo

A computação com seus algoritmos e suas aplicações nos mais diversos conhecimentos envolve desafios como o do armazenamento de informações nos chamados banco de dados solicitando gerenciamento. Nessa perspectiva, o objetivo geral deste estudo analisou o funcionamento do banco de dados relacional com as características e vantagens que possui. O problema de pesquisa questionou os benefícios que o modelo relacional traz para o usuário em relação a outro banco de dados. E por se tratar de um estudo do tipo revisão de literatura, qualitativa e descritiva a coleta de dados foi realizada nas informações da base de dados da *Scientific Electronic Library* Online (SciELO) e https://scholar.google.com.br/. Concluiu-se que, que o modelo de banco de dados relacional superou os modelos anteriores, pois, ainda, hoje está em evidência no mercado, porque as relações estabelecidas interagem dentro das tabelas diversificadas nas matrizes com linhas e colunas por meio da atomicidade, consistência, isolamento e durabilidade. E o outro fator é que o modelo estudado possibilitou a evolução chegando a existir outros padrões de sistemas mais recentes.

Palavras-chave: Tecnologia. Armazenamento. Sistema. Gerenciamento.

Abstract

Computing with its algorithms and their applications in the most diverse knowledge involves challenges such as storing information in so-called databases requesting management. In this perspective, the general objective of this study analyzed the functioning of the relational database with the characteristics and advantages it has. The research problem questioned the benefits that the relational model brings to the user in relation to another database. And because it is a literature review, qualitative and descriptive study, data collection was carried out using information from the Scientific Electronic Library Online (SciELO) database and https://scholar.google.com.br/. It was concluded that the relational database model surpassed the previous models, since it is still in evidence today in the market, because the established relationships interact within the diversified tables in matrices with rows and columns through atomicity, consistency, insulation and durability. And the other factor is that the studied model enabled the evolution to exist other patterns of more recent systems.

Keywords: Technology. Storage. System. Management.

1. INTRODUÇÃO

Ao longo da história da humanidade o homem utilizou diversos meios para se comunicar como gestos, palavras, sinais, símbolos e expressões do próprio corpo, que foram sendo associadas e registradas na memória humana idealizando códigos que se repetiam e se externavam quando necessário gerando sistemas de comunicação. Mas foi com a invenção da escrita que a comunicação avançou e houve a anotação de informações em pedras, tábuas, e por fim, em papel.

Tais informações registradas permitiram a compreensão e até evolução nas mais diversas formas de acúmulo desses registros. Posteriormente, com a descoberta da imprensa gerou estratégias para a preservação dos conteúdos, mas também um grande volume de papéis, sendo que muitos se extraviaram por vários motivos ao longo dos tempos.

E a Era da Tecnologia trouxe inovações como a grande vantagem da guarda de acervos digitais, e ainda, potencializou o acesso em tempo real. Este armazenamento de registros que vai além do papel trouxe celeridade, flexibilidade e mais informações disponíveis nos chamados banco de dados.

Os bancos de dados estão cada vez mais presentes no dia a dia, visto que a maioria das atividades que é realizada envolve, direta ou indiretamente, o uso de uma base de dados. Diante disso, é necessário apresentar nas seções seguintes deste documento uma introdução aos conceitos fundamentais de banco de dados.

Obter informação rápida e confiável é vital para a sociedade, sobretudo para as organizações. Bancos de dados possibilitam o controle e a disponibilização dessas informações e por isso, tornaram-se elementos indispensáveis. Desta forma, o presente trabalho se propõe a abordar alguns dos principais tópicos dessa área. Todavia devido à profundidade do tema banco de dados foi decidido que o foco seria somente no banco de dados relacional na sua estrutura e lógica de funcionamento.

Essa pesquisa tem grande relevância porque se trata de um assunto que está em constante atualização, e alcança não somente o mercado de trabalho com seus processos, mas também as finanças e os demais setores. E reservar informações para possíveis utilidades posteriores, é sem dúvida importante também para a sociedade como um todo, pois todos fazem isso de formas diferenciadas. Outro fator de relevância é para o próprio estudante, que por ser da área da tecnologia de informação, absorveu mais conhecimentos e experiências.

Ficou evidente, então, que a necessidade de se ter um banco de dados relacional gera questionamentos, já que é uma tecnologia de armazenamento com acoplamento promove certa dependência entre os objetos. E a problemática da pesquisa preocupou-se em indagar: Quais os benefícios que o modelo relacional traz para o usuário em relação a outro banco de dados?

O objetivo geral do trabalho foi analisar o funcionamento do banco de dados relacional com as características que possui e que são vantajosas quando aplicadas. E os objetivos específicos foram explicar o que é um banco de dados, modelo entidade-relacionamento (E-R), modelo relacional para compreender o padrão SQL.

2. BANCO DE DADOS

Os bancos de dados podem ser classificados em dois grandes grupos: os bancos de dados transacionais ou OLTP (*Online Transaction Processing*) os quais são usados nos sistemas informacionais dando suporte às atividades organizacionais administrativas e operacionais, e os de suporte à decisão ou OLAP (*Online Analytical Processing*). que são usados para recuperar as informações agregadas e sumarizadas para a tomada de decisão (NUNES, 2017).

Os sistemas de informação empresariais apresentam-se como manual ou informatizado., sendo basicamente que o sistema de informação nesse ambiente é o conjunto de registros e documentos referentes às operações executadas ali. Independentemente dos recursos de tecnologias de informação e comunicação (TICs), os sistemas de informação nas empresas se estruturam essencialmente na formalização dos dados gerados em suas operações (registros/documentos) orientados pelo grau de complexidade dos registros de acordo com o nível organizacional - seja operacional, gerencial ou estratégico. O que nesse aspecto entendem-se como os sistemas de processamento de transações (SPT), os sistemas de informações gerenciais (SIG) e os sistemas de apoio ao executivo (SAE) (JANUZZI *et al.*, 2014).

Segundo Date (2004, p. 10) "um banco de dados é uma coleção de dados persistentes, usada pelos sistemas de aplicação de uma determinada empresa", ou seja, um Banco de Dados é uma coleção de dados necessários para o funcionamento de uma aplicação. A aplicação de um banco de dados é armazenar dados de forma organizada para que seus usuários busquem e atualizem seus dados, gerando assim informações precisas. Esses dados quando são processados produzem informação que por sua vez ajudar na tomada de decisão de uma organização. Podendo assim ser ressaltado que antigamente esses dados eram armazenados em papéis, ocasionando em muito mais trabalho, com inúmeras desvantagens podendo ser citados, como fragilidade, demora em consultar esses dados e sua falta de confiabilidade para com os dados armazenados, pois por ser armazenado em papéis o mesmo dado poderia ter vários valores diferentes já que não são totalmente centralizados.

a) Aspecto estrutural: sua estrutura é montada somente em formas de tabelas e, dessa mesma forma, podem ser visualizadas e manipuladas;

b) Aspecto de integridade: sua estrutura pode ser relacionada, utilizando-se de restrições que possibilitem a integridade dos dados no banco;

c) Aspecto manipulativo: o modo de utilização do sistema para interação com os dados, operadores derivam tabelas de outras tabelas (DA MELO *et al*., 2013, p.).

Da Melo *et al*. (2013) estão dizendo que o sistema projetado, ou seja, modelo relacional aponta para separar o armazenamento físico dos dados do seu aspecto conceitual por meio de um embasamento matemático para o modelo, o qual segue algumas normas, não partindo de uma conceituação aleatória, isto é, valoriza a estrutura, ou seja, o aspecto da apresentação sob a forma tabular, o que facilita a identificação, classificação e uso dos dados. E o outro aspecto é a integridade, o que é muito importante na preservação. E por fim, os autores citam o aspecto manipulativo, que é a possibilidade de reprodução dessas tabelas na interação com os seus dados.

Para Elmasri e Navathe (2011, p. 3), na expressão Banco de Dados estão subentendidas as propriedades abaixo:

> [...] Um banco de dados representa alguns aspectos do mundo real, sendo chamado, às vezes, de minimundo ou de universo de discurso (UoD). As mudanças no minimundo são refletidas em um banco de dados. Um banco de

> dados é uma coleção lógica e coerente de dados com algum significado inerente. Uma organização de dados ao acaso (randômica) não pode ser corretamente interpretada como um banco de dados. Um banco de dados é projetado, construído e povoado por dados, atendendo a uma proposta específica. Possui um grupo de usuários definido e algumas aplicações preconcebidas, de acordo com o interesse desse grupo de usuários.

Um Banco de Dados é um grupo de dados relacionados, criado para determinadas aplicações. Quando é referenciado o termo aplicação, estão sendo mencionados os *softwares* que se beneficiam dos dados que estão presentes no Banco de Dados. Em um banco de dados pode ter mais de uma aplicação, e sua utilização compreende armazenar, manipular e buscar esses dados.

2.1 Sistema de Gerenciamento de Banco de Dados (SGBD)

De acordo com Elmasri e Navathe (2011, p. 3) "um sistema gerenciador de banco de dados (SGBD) é uma coleção de programas que permite aos usuários criar e manter um banco de dados." Percebe-se que um SGBD nada mais é que um software que manipula e gerencia os dados que facilita o compartilhamento dos dados entre várias aplicações e usuários. Na figura a seguir é mostrado de forma simples como o SGBD funciona.

Na figura é mostrado que um SGBD ele faz o intermédio entre o BD e as aplicações, o SGBD tem como finalidade facilitar os processos de definição, construção, manipulação e compartilhamento de um banco de dados (ELMASRI; NAVATHE, 2011).

Em um SGBD tem alguns requisitos que são: Atomicidade esta propriedade garante que todas as transações sejam atômicas (indivisíveis), ou seja, as transações sejam executadas completamente. Caso ocorra algum erro, todas as operações que constituem a transação serão descartadas. Consistência a execução de uma transação deve fazer com que o banco de dados entre em outro estado consistente de um estado consistente, ou seja, cada transação deve obedecer às regras de integridade de dados. Isolamento é um recurso do banco projetado para impedir que transações paralelas, em um sistema multiusuário, interfiram umas nas outras. Durabilidade significa que o efeito da transação é permanente (FERREIRA, 2019).

Os pontos citados acima têm que ser seguidos para se manter a integridade das transações em um banco de dados, que de acordo com Ferreira (2019) existem alguns bancos de dados que não seguem os conceitos do ACID (Atomicidade, Consistência, Isolamento e Durabilidade) que são os bancos do tipo NoSQL.

Recapitulando, já se sabe que um banco de dados é formado por dados que possuem relação, e que um SGBD, nada mais é que um conjunto de *software* que tem como objetivo facilitar o gerenciamento do banco de dados e conectar ele com as aplicações.

Werlich (2018, p. 31) "modelo relacional baseia-se na ideia de que as informações em uma base de dados podem ser representadas em tabelas cujas linhas apresentam as informações cadastradas", entende-se que o modelo relacional é organizado em tabelas com linhas e colunas com informações da base de dados e que ele se expande conforme dados são armazenados.

Formalmente, no modelo relacional cada linha é chamada de tupla, o cabeçalho da coluna é chamado de atributo e a tabela é chamada de relação. O tipo de dado que descrevem os 19 tipos de valores que podem aparecer em cada coluna são representados por

um domínio de valores possíveis. (MOURA, 2017).

De acordo com Macário e Baldo (2005, p. 2) “a maior vantagem do modelo relacional sobre seus antecessores é representação simples dos dados e a facilidade com que consultas complexas podem ser expressas”. Com isso, entende-se que o modelo relacional nada mais é do que uma forma de organizar os dados armazenados e facilitar a consulta no banco de dados.

Operadores geram tabelas de outras, estão entre eles “a restrição ou seleção, quando são extraídas linhas específicas de uma tabela; a projeção, que constitui na extração de colunas específicas da tabela; e a junção, definida como a união de tabelas, utilizando-se de valores comuns em determinadas colunas.”. E asseguram que é factível logar o conteúdo dos bancos de dados relacionais, apenas na forma de tabelas, porém deve-se apreciar essa estrutura lógica como uma abstração do modo de armazenamento físico, já que o sistema precisa de formas: arquivos sequenciais, indexação, hashing, cadeias de ponteiros, compactação, dentre outras, para esse armazenamento. (DA MELO et al., 2013).

Por ser o modelo relacional uma série de relações e seus relacionamentos, cada relação é nominada aos seus atributos e nomes, ou seja, as relações são as tabelas. Desse modo, projetar uma tabela, apenas sob observação cria uma complexidade e menos visibilidade, e o modelo de entidades e relacionamentos envolve a proposta relacional e de rede por meio de regras e classificação como se ver a seguir.

2.1.1 Entidade-Relacionamento (E-R)

O Modelo Entidade-Relacionamento, sobretudo o diagrama, é uma importante ferramenta para trabalhar os sistemas, principalmente os mais compostos e complicados de visualizar sem uma avaliação mais rigorosa. É um modelo conceitual aproveitado na Engenharia de *Software* para delinear as entidades envolvidas em um domínio de negócios, com seus carácteres e como ele se comunicam entre si. Geralmente, exibe de forma abstrata a estrutura que terá o banco de dados da aplicação. O banco de dados poderá conter diversas outras entidades, tais como chaves e tabelas intermediárias, que podem fazer significação no contexto de bases de dados relacionais. (FRANCK *et al*., 2021).

A entidade-relacionamento reduz a abstração e faz com que haja mais realidade e visibilidade nas informações armazenadas. E para que o código do programa tenha permissão de acesso claro e identificável em sua estrutura e apresentação, é necessário que haja uma linguagem estruturada.

2.1.2 Linguagem de Consulta Estruturada (SQL)

A garantia da linguagem SQL, que é concebida por comandos de definição, manipulação e controle de dados, utilizada pelos SGBDs vem dos estudos de Boyce e Chamberlin no laboratório de pesquisas da IBM® em San José, feita em 1973, quando se uniram ao projeto System R. Convencidos de que uma linguagem relacional tornaria os bancos de dados mais entendíveis a pessoas sem compreensão matemática, porém não estavam conformados com o Square, que usava um registro complicado de digitar em um teclado. O propósito era discorrer uma linguagem que consentisse atualização e administração do banco de dados, bem como consultas (NUNES, 2017).

Por ser uma linguagem de programação, a linguagem de consulta estruturada per-

mite trabalhar com uma grande quantidade de dados com rapidez e segurança, já que está vinculada à padronização, tem flexibilidade de atuação em outras plataformas, e a visualização também pode ser compartilhada.

2.2 Resultado e Discussão

Nesta investigação foram encontrados vinte (20) artigos, os quais foram lidos e selecionados somente oito (08), pois os mesmos falam exclusivamente de banco de dados relacional. Do material selecionado e inserido neste estudo, existe unanimidade entre os autores quando asseguram que este tipo de sistema aprimora as ações executadas.

Dos artigos encontrados num total de vinte nas bases de dados mencionadas, três falam do armazenamento, e cinco falam de gerenciamento sendo que todos abordam prioritariamente o banco de dados relacional.

AUTOR/ ANO	**TÍTULO**	**OBJETIVO GERAL**	**SÍNTESE DE RESULTADOS**	**REV.**
2004 Elmasri e Navathe	Sistema de banco de dados	Entender os fundamentos da tecnologia de banco de dados	Literatura	Pearson Education do Brasil Ltda.
2005 Carla Geovana do N. Macário Stefano Monteiro Baldo	O Modelo Relaciona	Descrever o modelo relacional, identificando suas principais características e vantagens e apresentando comandos em linguagem SQL para implementação destas características	Apresentou regras para promover o mapeamento de um esquema no modelo Entidade Relacionamento para o modelo relacional, visando auxiliar o usuário na execução da fase de projeto lógico de um banco de dados.	UNICAMP
2011 DA MELO et al.	Comparativo entre banco relacional e base textual: CDS/ISIS	Apresentar uma nova forma de armazenamento para dados bibliográficos de uma rede de bibliotecas	Foi possível, por meio de uma bateria de testes, detectar necessidades nos modelos, o modelo atual utilizado e a Base Textual CDS/ISIS, que se mostrou mais eficiente no tempo de resposta das consultas, tratando as mesmas em média duas vezes mais rápidas em comparação ao Banco Oracle.	Perspect. ciênc. Info
2011 ABREU Cristiane de Lima Caputo	O uso de sistema de gerenciamento de banco de dados para controle de contratos: estudo de caso em uma empresa de construção pesada de Belo Horizonte – MG	Analisar e otimizar o processo de controle de contratos de subempreiteiros e de locação de equipamentos de uma empresa de construção pesada de Belo Horizonte MG.	Foi realizado um levantamento do processo de controle de contratos visando o entendimento de todas as partes envolvidas que estavam fragmentadas sem uma conexão explícita, dificultando o andamento do processo aos novos colaboradores, bem como a recuperação da informação por parte do restante da empresa. Após este levantamento inicial, foi iniciada a criação do banco de dados baseado na lógica envolvida na parte de controle dos contratos.	UFMG

2014 JANUZZI, Celeste Aída Sirotheau Corrêa; falsarella,; Orandi Mina; Sugahara, Cibele Roberta.	Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais.	Discutir a relação entre os diversos termos e conceitos referentes a sistemas de informação apresentados nos estudos sobre o tema	Diferentes denominações sempre vão existir, portanto é muito importante para os estudos no tema que se compreenda e se assimile as características apresentadas pelos grupos de sistemas de informação, pois facilita o acompanhamento e discernimento em relação à variedade disponibilizada para as organizações.	Perspectivas em Ciência da Informação
2017 Nunes	Um modelo de dados voltado ao treinamento e formação policial	Propor um modelo de dados capaz de fornecer subsídios para o desenvolvimento de um banco de dados para informatizar as principais atividades de treinamento e capacitação da Academia Nacional da Polícia Rodoviária Federal - ANPRF.	Foi realizada a proposta de um Modelo de Entidade Relacionamento capaz de abordar os aspectos relevantes de um evento de treinamento ou capacitação.	UFSC
2019 Moura et al	Consultas SQL utilizando linguagem natural para um contexto acadêmico	Propôs a criação de um sistema de consultas em uma base de dados representando um contexto acadêmico utilizando linguagem controlada	Enquete e testes sobre armazenamento de palavras em dicionários	UFCE
2021 Franck et al	Diagrama Entidade - Relacionamento: uma ferramenta para modelagem de dados conceituais em Engenharia de Software	Abordar as principais informações sobre o modelo entidade - relacionamento como ferramenta para modelagem de dados conceituais.	O Modelo Entidade - Relacionamento, e principalmente o diagrama, é uma importante ferramenta durante o desenvolvimento de sistemas, principalmente aqueles mais complexos e difíceis de visualizar sem uma análise mais aprofundada	Research, Society and Development,

Tabela 1- Caracterização dos artigos

Fonte: Autoria própria, 2023.

Categoria 1 - Sistema de armazenamento

O estudo realizado por DA Melo et al. (2011) fez uma comparação entre banco relacional e base textual: CDS/ISIS. Nesse aspecto, os estudantes mostraram um modelo de banco de dados e ferramentas que possibilitam a migração dos dados da Base Textual CDS/ISIS para o Banco Relacional Oracle. E por meio de um trabalho criterioso, eles conseguiram migrar dos dados por aplicativos que possibilitaram a manipulação da base atual e, depois inseriram as informações no modelo novo. A seguir validaram o projeto, quando então foram geradas consultas comparativas nos dois modelos e aplicados, através de um software específico, testes de stress, com diversos parâmetros, a fim de comparar a performance de consultas entre os modelos.

Segundo o estudo de Frank *et al*. (2021), ou seja, o banco de dados pode ter várias outras entidades, tais como chaves e tabelas intermediárias, que conseguem dar nexo no contexto de bases de dados relacionais. Todavia, outros modelos virão para um sistema completo, porque isso poderia implicar em um modelo muito grande e difícil de interpretar, que os autores entendem, que, dependendo da extensão do que é desenvolvido,

pode-se criar modelos apenas para uma parte do sistema, um módulo, ou mesmo uma funcionalidade.

Categoria 2 - Sistema de gerenciamento

O estudo de Abreu (2011) analisou e otimizou o processo de controle de contratos de subempreiteiros e de locação de equipamentos de uma empresa de construção criando um banco de dados, essa atitude mostra a relevância do gerenciamento das informações, especialmente na celeridade dos processos e na recuperação de dados, ou seja, destacou que, para um modelo de dados está voltado ao treinamento e formação específica, devem ser discutidos alguns aspectos relevantes a respeito da solução proposta, sua aplicabilidade, deficiências e necessidades de melhoria, com o objetivo de aprimorar a adequação do modelo à realidade proposta. Isso mostra que o gerenciamento é um fator extremamente relevante.

Date (2004) enfatiza o SGDB como um software genérico, ou seja, ele serve para manipular os dados, com uma visão lógica (projeto de BD), tem linguagem própria, e que são programas que definem e constroem os bancos de dados.

Elmasri e Navathe (2011) deixaram claro em sua teoria que o modelo conceitual não dita como o SGDB será implementado, nem na sua apresentação física e nem logica. Mas que vencida esta etapa, do modelo Entidade-relacionamento abre-se a visão do sistema do banco de dados, sendo que o modelo lógico se caracteriza por relacional, hierárquico e de rede.

Como é o caso do estudo de DA Melo *et al.* (2013) que falam que as técnicas de armazenamento, indexação e aprimoramento de consultas nos Sistemas de Banco de dados Relacionais (SGBDRs) aperfeiçoaram os processos ampliando e dando mais complexidade a esses sistemas.

Já Franck *et al*. (2021) falam da flexibilidade e dinamismo que o modelo de banco de dados relacional possui, pois envolve diversos aspectos, e pode trabalhar em separado as informações lançadas, mesmo sendo possível ser aplicado de forma unificada. Os autores explicam que julgam desnecessário padronizar um modelo para várias entidades, mas sim, decompor a modelagem em várias partes menores para modelagem de dados conceituais.

Matrícula	Nome	Data de Nascimento	Curso
84636	Luiz	17/02/1999	Direito
48625	João	06/05/1998	Veterinária
18765	Ricardo	27/01/2001	Engenharia

Tabela 2 - Tipo de tabela do modelo relacional

Fonte: Dados da própria pesquisa (2023).

De acordo com o Quadro 01 as informações estão cadastradas para serem utilizadas e serem trabalhadas de acordo com a interdependência que possuem entre si, já que as informações estão armazenadas num domínio específico. Esta tabulação permite inserção e recuperação sem complexidades, o que se tornou evidente na explicação de Werlich (2018).

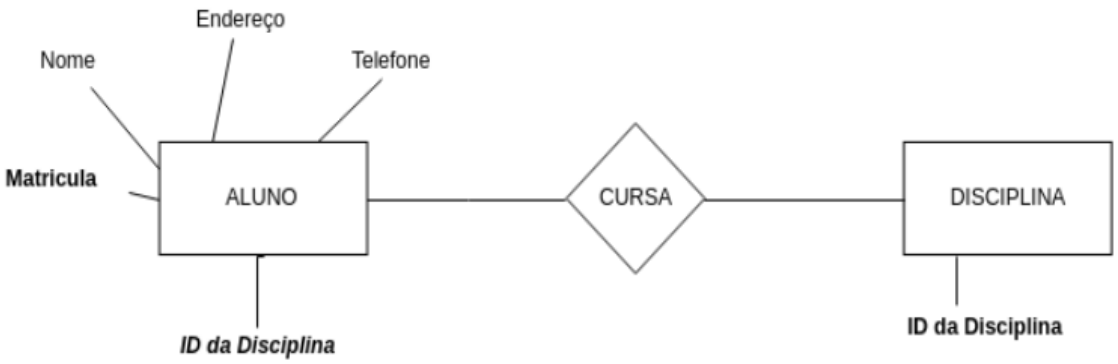


Figura 1 - Entidade aluno e disciplina

Fonte: Moura (2019, p.20).

Na Figura 1 do modelo ER, segundo o exemplo de Moura (2019), a entidade ALUNO pode ser caracterizada pelo nome, endereço, telefone, curso e matrícula como chave primária, sendo que cada entidade possui atributos intrínsecos, sem repetição na tabulação.

Estes aspectos denotam a importância do banco de dados relacional, já que o seu desenvolvimento nas mais diversas empresas e instituições servem para monitoramento das informações com precisão, destacando-se principalmente no gerenciamento financeiro. Tais resultados encontrados abalizaram este estudo e deram ênfase na grande importância no uso de banco de dados relacional, mesmo que tenha desvantagens como o alto custo, e a demora em sua implantação, porém traz vantagens que compensam como a eficiência e a transparência com segurança das informações.

Todos estes estudos foram pertinentes à temática, e exibiram a o banco de dados relacional através diante de muitas percepções, tais como a utilidade, versatilidade, segurança e durabilidade das informações já armazenadas, ou migradas para outro tipo de armazenamento.

3. CONCLUSÃO

Esta pesquisa analisou o funcionamento do banco de dados relacional com as características que possui e explicou suas vantagens quando aplicadas, bem como explicou o que é um banco de dados, modelo entidade-relacionamento (E-R), modelo relacional para compreender o padrão SQL. Vale ressaltar que houve algumas dificuldades em encontrar acervos que abordassem a temática, mas que o conteúdo aqui, revela o quanto é importante o modelo relacional, destacado principalmente na sua larga utilização no mercado em todas as áreas por apresentar flexibilidade, organização, e garantia de confiabilidade na segurança das informações.

É importante frisar que diante dos resultados e discussões discorridos, foi concluído que o modelo de banco de dados relacional superou os modelos anteriores, pois, ainda, hoje está em evidência no mercado, porque as relações estabelecidas interagem dentro das tabelas diversificadas nas matrizes com linhas e colunas por meio da atomicidade, consistência, isolamento e durabilidade. E o outro fator é que o modelo estudado possibilitou a evolução chegando a existir outros padrões de sistemas mais recentes.

Portanto, a contribuição que esta investigação traz para estudos futuros, é que seja realizada uma avaliação do banco de dados modelo relacional pesquisado num estudo em que permita a comparação da sua utilização em empresas de ramos diferentes, visto que poderá ser melhor interpretado a sua eficácia.

Referências

DA MELO, Daniel Augusto; PALHARES, Márcia Maria; PALHARES, Mônica Geralda. **Comparativo entre banco relacional e base textual**: CDS/ISIS; Perspect. ciênc. inf. 18 (3) Set 2013. Disponível em: https://doi.org/10.1590/S1413-99362013000300005. Acesso em: 16 nov. 2022.

DATE, Christopher J. **Introdução a sistemas de bancos de dados**. Elsevier Brasil, 2004.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6. ed. São Paulo: Addison Wesley, 2011.

FERREIRA, Fabio. Banco de dados - **Modelagem de dados**. GitBook, 2019. Disponível em: https://fabiojaniolima.gitbooks.io/banco-de-dados-modelagem-de-dados/content/. Acesso em: 16 nov. 2022.

FRANCK, Kewry Mariobo; PEREIRA, Robson Fernandes; FILHO, Jerônimo Vieira Dantas. Diagrama Ratio-Entity: uma ferramenta para modelagem conceitual de dados em Engenharia de Software. ***Research, Society and Development***, v. 10, n. 8, e49510817776, 2021 (CCBY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v10i8.17776.

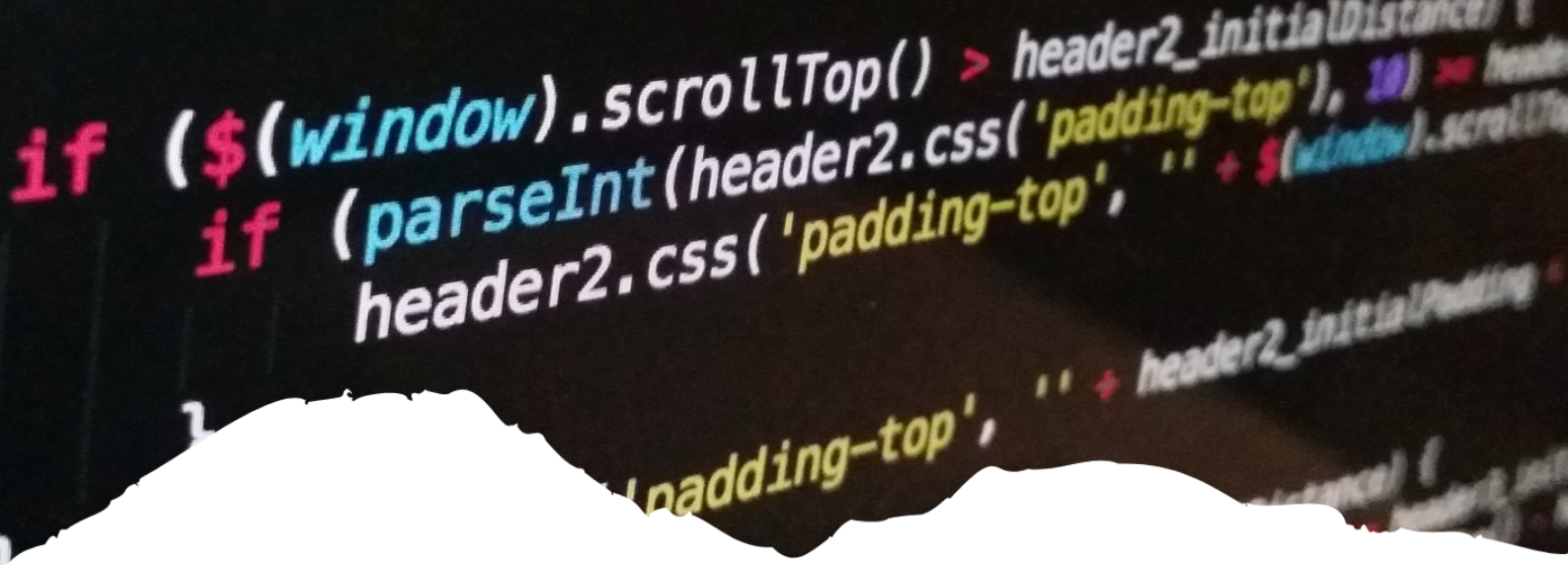
JANUZZI, Celeste Aída Sirotheau Corrêa; FALSARELLA, ; Orandi Mina; SUGAHARA, Cibele Roberta. Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais . **Perspectivas em Ciência da Informação**, v.19, n.4, p.94-117, out./dez. 2014.

MACÁRIO, Carla; BALDO, Stefano**. O Modelo Relacional**. [S. l.: s. n.], 2005. Disponível em: https://www.ic.unicamp.br/~geovane/mo410-091/Ch03-RM-Resumo.pdf. Acesso em: 4 nov. 2022.

MOURA, Erik Almeida. **Consultas SQL utilizando linguagem natural para um contexto acadêmico**. Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas, Curso de Ciência da Computação, Russas, 2019.

NUNES, Ronnie Carlos Tavares. **Um modelo de dados voltado ao treinamento e formação policial.** TCC de conclusão de curso da Universidade federal de Santa Catarina pós-graduação em tecnologias da informação e comunicação aplicadas à segurança pública e direitos humanos. Araranguá, 2017. Disponível em: https://repositorio.ufsc.br/ Acesso em 06 de mar de 2023.

WERLICH, Claudia. **Modelagem de Dados**. [S. l.: s. n.], 2018. 213 p. ISBN 9788552211549.



22

UMA ANÁLISE DO MODELO DE BANCO DE DADOS RELACIONAL

AN ANALYSIS OF THE RELATIONAL DATABASE MODEL

Pedro Rafael Costa Feitosa

Resumo

O modelo relacional é amplamente reconhecido como o modelo mais utilizado no campo de banco de dados atualmente. Sua introdução em 1970 causou uma revolução na indústria e, apesar das tendências recentes em direção à orientação a objetos, o modelo relacional ainda mantém sua posição dominante no mercado. Este trabalho tem como objetivo explorar em detalhes o modelo relacional, destacando suas principais características e vantagens. Além disso, serão apresentados comandos em linguagem SQL para a implementação dessas características específicas.

Palavras-chave: banco de dados, modelo relacional, Tabelas, Consulta SQL.

Abstract

The relational model is widely recognized as the most widely used model in the database field today. Its introduction in the 1970s caused a revolution in the industry, and despite recent trends towards object orientation, the relational model still maintains its dominant market position. This work aims to explore in detail the relational model, highlighting its main characteristics and advantages. In addition, commands in SQL language will be presented for the implementation of these specific characteristics.

Key-words: database, relational model, Tables, SQL Query.

1. INTRODUÇÃO

O modelo de banco de dados relacional é uma abordagem amplamente adotada para a organização e gerenciamento de dados. Ele foi introduzido pela primeira vez por Edgar F. Codd em 1970 e revolucionou a maneira como os dados são armazenados e manipulados. No modelo relacional, os dados são estruturados em tabelas, onde cada tabela representa uma entidade e cada linha corresponde a um registro. As relações entre as tabelas são estabelecidas através de chaves primárias e chaves estrangeiras, permitindo que os dados sejam relacionados e consultados de forma eficiente.

Uma das principais vantagens do modelo relacional é a sua flexibilidade. Ele permite que os dados sejam organizados de maneira lógica e estruturada, facilitando a compreensão e a manipulação dos mesmos. Além disso, o modelo relacional é independente da implementação física, o que significa que as aplicações podem interagir com os dados de maneira consistente, independentemente de como eles estão armazenados em disco. Isso oferece uma camada de abstração que simplifica o desenvolvimento e a manutenção de sistemas de banco de dados.

Outro aspecto importante do modelo relacional é a capacidade de garantir a integridade dos dados. Através do uso de restrições e regras, é possível manter a consistência dos dados armazenados no banco de dados. Restrições como chaves primárias e chaves estrangeiras garantem que os dados sejam únicos e corretamente relacionados, evitando inconsistências e duplicações. Além disso, o modelo relacional suporta a normalização, um processo que permite a eliminação de redundâncias e a organização eficiente dos dados, contribuindo para a integridade e a eficiência do sistema de banco de dados.

O modelo relacional também oferece recursos avançados de consulta e manipulação de dados. Através da linguagem SQL (Structured Query Language), os usuários podem realizar consultas complexas que envolvem múltiplas tabelas e condições de seleção. A linguagem SQL também permite a definição de visões, que são representações personalizadas dos dados que simplificam o acesso e a análise das informações.

O modelo de banco de dados relacional é uma abordagem poderosa e amplamente utilizada para organizar e gerenciar dados. Com sua estrutura baseada em tabelas, relacionamentos, chaves e linguagem SQL, ele recursos avançados de consulta.

2. MODELO RELACIONAL

Em 1970, Edgar F. Codd ofereceu-nos uma colaboração revolucionária ao formular o modelo de dados relacional. A abordagem relacional representa uma forma de descrever um banco de dados por meio conceitos matemáticos simples: a Teoria dos Conjuntos. Voltada principalmente a melhorar a visão dos dados pelos usuários, essa abordagem faz com que os usuários vejam o banco de dados como um conjunto de tabelas bidimensionais, originada em linhas e colunas (MACHADO, 2020)

De acordo com Takai (2005), a estrutura fundamental do modelo relacional é a relação (tabela). Uma relação é constituída por um ou mais atributos (campos) que traduzem o tipo de dados a armazenar. Cada instância do esquema (linha) é chamada de tupla (registro). O modelo relacional não tem caminhos pré-definidos para se fazer acesso aos dados como nos modelos que o precederam. O modelo relacional implementa estruturas de dados organizados em relações. Porém, para trabalhar com essas tabelas, algumas restrições precisaram ser impostas para evitar aspectos indesejáveis, como: Repetição de informação, incapacidade de representar parte da informação e perda de informação. Essas restrições são: integridade referencial, chaves e integridade de junções de relações. Abaixo a figura 1.0 mostra exemplo de modelo relacional Cliente- Conta Corrente.

Cod_Cliente	Nome	Rua	Cidade
1	Pedro	A	São Paulo
2	Maria	B	Jundiai

Num_CC	Saldo
20121	1200
21582	1320
21352	652

Cod_Cliente	Num_CC
1	20121
2	21582
2	21352

Figura – 1.0 Tabelas do modelo relacional Cliente - Conta Corrente

Fonte: Takai (2005)

2.1 Linguagem SQL (Structured Query Language)

O SQL (Structured Query Language) é uma linguagem declarativa para banco de dados relacional, sendo que muitas das suas caracteristicas originais foram inspiradas na ál-

gebra. Tal linguagem foi desenvolvida no início dos anos 1970, nos laboratórios da IBM, em um projeto chamado System R, que tinha por objetivo demonstrar a viabilidade da implementação do modelo relacional proposto de dados. Atualmente, a linguagem SQL é um grande padrão adotado pela maioria dos bancos de dados; tendo em vista sua simplicidade e facilidade de uso.

2.1.1 DDL – Definição de dados

As principais instruções do DDL são CREATE, ALTER e DROP, que permitem criar, modificar e excluir objetos de banco de dados, respectivamente. É importante destacar que o DDL é uma das partes fundamentais da administração de um banco de dados, pois é por meio dele que se garante a integridade, segurança e eficiência do sistema. Abaixo na tabela 1.0 mostra um exemplo desses comandos. Na tabela 1.0 mostra exemplos de DDL (FLAVIA, 2009).

COMANDO	DESCRIÇÃO	EXEMPLO
CREATE	Cria uma nova tabela no banco de dados	PilotosF1(código int (11), nome char (20), pais char (20), motor char (20));
ALTER	Modifica a estrutura de uma tabela existente	ALTER TABLE PilotoF1 ADD código_Ranking (11);
DROP	Exclui uma tabela do banco de dados	DROP TABLE PilotoF1;

Tabela – 1.0Adaptada- DDL (Definição de dados**)**

Fonte: Cardoso (2013)

2.1.2 DQL – Consulta de dados

De acordo com Flavia (2009), O DQL (Data Query Language) é uma linguagem utilizada para consultar dados em um banco de dados. É por meio do DQL que são feitas as consultas nas tabelas para recuperar informações específicas. A principal instrução do DQL é o SELECT, que é utilizado para recuperar dados de uma ou mais tabelas, com a possibilidade de filtrar, agrupar e ordenar os resultados. O SELECT também permite fazer operações matemáticas, concatenar strings, entre outras funcionalidades. Na tabela 1.1 mostra exemplos de DQL.

COMANDO	DESCRIÇÃO	EXEMPLO
SELECT	Recupera dados de uma ou mais tabelas	SELECT * FROM PilotoF1

Tabela – 1.1Adaptada- DQL (Consulta de dados**)**

Fonte: Cardoso (2013)

2.1.3 DML – Manipulação de dados

Uma das principais partes da linguagem SQL é a DML, que inclui os comandos que permitem a manipulação dos dados. Quando dizemos manipulação, estamos falando sobre inserção (INSERT), atualização (UPDATE) de dados e exclusão (DELETE) de dados em uma tabela. Na tabela 1.2 mostra exemplos de DML (Flavia, 2009)

COMANDO	DESCRIÇÃO	EXEMPLO
INSERT	Insere novos registros em uma tabela	INSERT INTO PilotoF1(nome, pais, motor) VALUES (Lucas, brasil, motorF1);
UPDATE	Atualiza registros existente em uma tabela	UPDATE PilotoF1 motor = “motorF2” WERE id = 1
DELETE	Exclui registros de uma tabela	DELETE FROM PilotoF1 WERE id = 1

Tabela – 1.2 Adaptada- DML (Manipulação de dados**)**

Fonte: Cardoso (2013)

2.1.4 DCL – Controle de dados

DCL (Data Control Language) é uma linguagem utilizada para controlar o acesso e permissões de usuários em um banco de dados. É por meio do DCL que são definidos os privilégios e restrições de acesso a tabelas e outros objetos do banco. As principais instruções do DCL são GRANT e REVOKE, que permitem conceder e revogar permissões de acesso a usuários ou grupos de usuários. É importante destacar que o DCL é uma parte fundamental da administração de um banco de dados, pois é por meio dele que se controla quem pode acessar e modificar os dados armazenados. Na tabela 1.3 mostra exemplos de DDL (Flavia, 2009)

COMANDO	DESCRIÇÃO	EXEMPLO
GRAANT SELECT	Concede permissao para um realizer consultas em uma tabela	GRANT SELECT ON tabela1 TO usuarios1
REVOKE SELECT	Revoga a permissao de realizar consultas em uma tabela	REVOKE SELECT ON tabela1 FROM usuarios1

Tabela – 1.3 Adaptada- DCL (Controle de dados**)**

Fonte: Cardoso (2013)

2.2 Restrições de Integridade

Segundo Date (2003), uma restrição de integridade (RI) é uma condição especificada sobre um esquema de banco de dados e limita os dados que podem ser armazenados em uma instância do banco de dados. Se uma instância do banco de dados satisfaz todas as restrições de integridade especificadas em seu esquema, então ela é uma instância válida. Um SGBD impõe restrições de integridade, no sentido de que ele permite o armazenamento apenas de instância válidas no banco de dados.

2.3 Restrições de Chave

Uma restrição de chave é uma declaração que estabelece que um subconjunto mínimo de campos em uma relação é um identificador único para uma tupla. Esse subconjunto de campos, que identifica exclusivamente uma tupla de acordo com a restrição de chave, é conhecido como chave candidata da relação (DATE, 2003)

2.4 Restrições Gerais

Segundo Ramakrishnan (2011), as restrições de domínio, de chave primária e de chave estrangeira são consideradas parte fundamental do modelo de dados relacional e recebem atenção especial na maioria dos sistemas comerciais. Às vezes, entretanto, é necessário especificar restrições mais gerais.

2.5 Relacionamentos e Conjuntos de Relacionamento

Um relacionamento é uma associação entre duas ou mais entidades. Por exemplo. podemos ter o relacionamento em que Attishoo trabalha no departamento de farmácia. Como com as entidades, podemos desejar reunir um conjunto de relacionamentos semelhantes em um conjunto de relacionamentos. Um conjunto de relacionamentos pode ser considerado um conjunto de tuplas. Ramakrishnan (2011)

Figura – 2.0 Um conjunto de relacionamento Ternário

Fonte: Ramakrishnan (2011)

No caso do exemplo ilustrado na Figura 2.0 do relacionamento “Trabalha_em”, será utilizado o seguinte comando SQL para realizar o mapeamento.

CREATE TABLE Trabalha_Em (cpf CHAR (11), Id-depto INTERGER, desde, DATE,

PRIMARY KEY (cpf, id-depto),

FOREIGN KEY (cpf) REFERENCES Funcionarios,

FOREIGN KEY (id-depto REFERENCES Departamento)

2.5.1 Conjunto Relacionamento com Restrições de Chave

Considere agora um outro conjunto de relacionamentos chamado Gerencia entre os conjuntos de entidades Funcionários e Departamentos, tal que cada departamento tenha no máximo um gerente, embora um mesmo funcionário possa gerenciar mais do que um departamento. A restrição de que cada departamento tem no máximo um gerente é um exemplo de uma restrição de chave, e isso implica que cada entidade Departamentos apareça em no máximo um relacionamento gerencia em qualquer instância permitida de Gerencia. Essa restrição é indicada no diagrama ER da Figura 2.1 utilizando se uma seta de Departamentos a Gerencia. Intuitivamente, a seta afirma que dada entidade de Departamentos, podemos determinar univocamente o relacionamento gerencia no qual ela aparece (RAMAKRISHNAN, 2011).

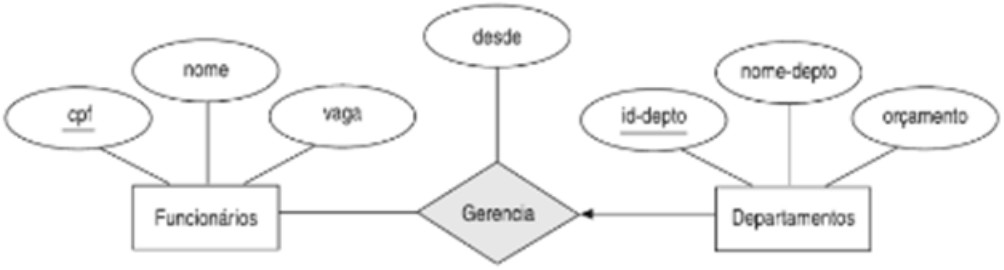


Figura – 2.1 Registro de chave em Gerência

Fonte: Ramakrishnan (2011)

Na ilustrado da Figura 2.1 do relacionamento “Gerencia”, será utilizado o seguinte comando SQL para realizar o mapeamento.

```
CREATE TABLE Depto (id-depto INTERGER, nome-depto CHAR (30), orçamento REAL,
  cpf CHAR (11), desde DATE,
PRIMARY KEY (id-depto),
  FOREIGN KEY (cpf) REFERENCES Funcionarios,
```

2.5.2 Conjunto Relacionamento com Restrição de Participação

A restrição de chave em Gerencia nos informa que um departamento tem no máximo um gerente. Uma dúvida natural é questionar se todo departamento tem um gerente. Consideremos que é exigido que todo departamento tenha um gerente. Esse requisito é um exemplo de restrição de participação: a participação do conjunto de entidades departamentos no conjunto de relacionamentos gerencia é considerada total. Uma participação que não é total é dita parcial. Como um exemplo. a participação do conjunto de entidades Funcionários em Gerencia é parcial, uma vez que nem todo funcionário gerencia um departamento (RAMAKRISHNAN, 2011)

2.6 Normalização de Dados

O processo em questão é fundamentado no conceito de formas normais. Uma forma normal consiste em uma regra que deve ser seguida por uma tabela para ser considerada “bem projetada”. Existem várias formas normais, ou seja, diversas regras cada vez mais rigorosas para verificar tabelas relacionais. Neste contexto, serão consideradas quatro formas normais específicas: primeira forma normal (1FN), segunda forma normal (2FN), terceira forma normal (3FN) e quarta forma normal (4FN) (HEUSER, 2009)

2.6.1 Forma Normal 1(1FN)

Segundo Carlos (2009), O processo inicial da normalização consiste em transformar um esquema de tabela não-normalizada em um esquema relacional que esteja na Primeira Forma Normal (1FN). Uma tabela está na 1FN quando não possui tabelas aninhadas. Portanto, alcançar a 1FN envolve a eliminação de quaisquer tabelas aninhadas que possam existir. Esse processo é essencial para garantir que a estrutura da tabela seja simplificada

e atenda aos requisitos da 1FN.

2.6.2 Forma Normal 2(2FN)

A Segunda Forma Normal (2FN) é aplicada a uma tabela que atende a todos os requisitos da Primeira Forma Normal (1FN) e onde os registros não chaves dependem completamente da chave primária, sem depender apenas de uma parte dela. A 2FN trata especificamente dessas irregularidades e tem como objetivo evitar a redundância nos dados armazenados no banco de dados. Ao garantir que as dependências funcionais estejam adequadamente estabelecidas, a 2FN contribui para uma estrutura mais eficiente e coerente da tabela (HEUSER, 2009). A Segunda Forma Normal (2FN) é essencial para eliminar redundâncias e estabelecer dependências funcionais adequadas na estrutura da tabela, resultando em um banco de dados mais eficiente e consistente.

2.6.3 Forma Normal 3(3FN)

Na terceira forma normal Heuser (2009) fala, durante a normalização para a Terceira Forma Normal (3FN), busca-se eliminar outro tipo de redundância. Uma tabela encontra-se na 3FN quando, além de satisfazer os critérios da Segunda Forma Normal (2FN), todas as colunas não chave dependem diretamente da chave primária, ou seja, não existem dependências funcionais transitivas ou indiretas. Uma dependência funcional transitiva ou indireta ocorre quando uma coluna não chave depende funcionalmente de outra coluna, ou combinação de colunas, que não fazem parte da chave primária. Ao eliminar tais dependências, a 3FN contribui para um modelo de dados mais organizado, evitando redundâncias desnecessárias.

2.6.4 Forma Normal 4(4FN)

A Quarta Forma Normal (4FN) é alcançada por uma entidade quando ela já está na Terceira Forma Normal (3FN) e não possui dependências multivaloradas entre seus atributos. Isso significa que não há campos que se repetem em relação à chave primária, evitando redundância nas tuplas da entidade. Para atingir a 4FN, é necessário fragmentar essa relação, a fim de eliminar essas dependências funcionais específicas. Dessa forma, garantimos um modelo de dados mais eficiente, livre de redundâncias desnecessárias (HEUSER, 2009).

2.7 Vantagens do Modelo de Banco de Dados Relacional

O modelo de banco de dados relacional oferece vantagens significativas em termos de flexibilidade e organização dos dados. Conforme mencionado por Ramakrishnan e Gehrke (2011), o modelo relacional permite a criação de tabelas que representam entidades e seus relacionamentos, fornecendo uma estrutura clara e intuitiva para armazenar e recuperar informações. Essa estrutura tabular facilita a identificação de padrões e relações entre os dados, permitindo consultas e análises eficientes. Além disso, o modelo relacional oferece a flexibilidade de adicionar, modificar ou excluir dados sem afetar a integridade das informações existentes, tornando-o adequado para ambientes em constante evolução.

Outras vantagens do modelo de banco de dados relacional é a capacidade de garantir a integridade e a consistência dos dados. De acordo com Machado e Abreu (2018), o modelo relacional permite a definição de restrições e regras de integridade, como chaves primárias, chaves estrangeiras e restrições de integridade referencial. Essas restrições garantem que os dados sejam consistentes e estejam livres de inconsistências ou duplicações. Além disso, o modelo relacional suporta operações de transação, permitindo que um conjunto de operações seja tratado como uma unidade indivisível. Isso garante que as alterações nos dados sejam realizadas de forma correta e consistente, mesmo em cenários de concorrência e falhas.

Referências

CARDOSO. G.C; Virginia. M. C. **Linguagem SQL Fundamentos e Praticas**. ed. São Paulo: Saraiva, 2013

DATE.C.J. **Introdução a Sistemas de Banco de dados**. ed. Elsevier, 2003

FLAVIA. J. **Guia Profissional Microsoft SQL Server 2008**. ed. São Paulo: Digerati Books, 2009.

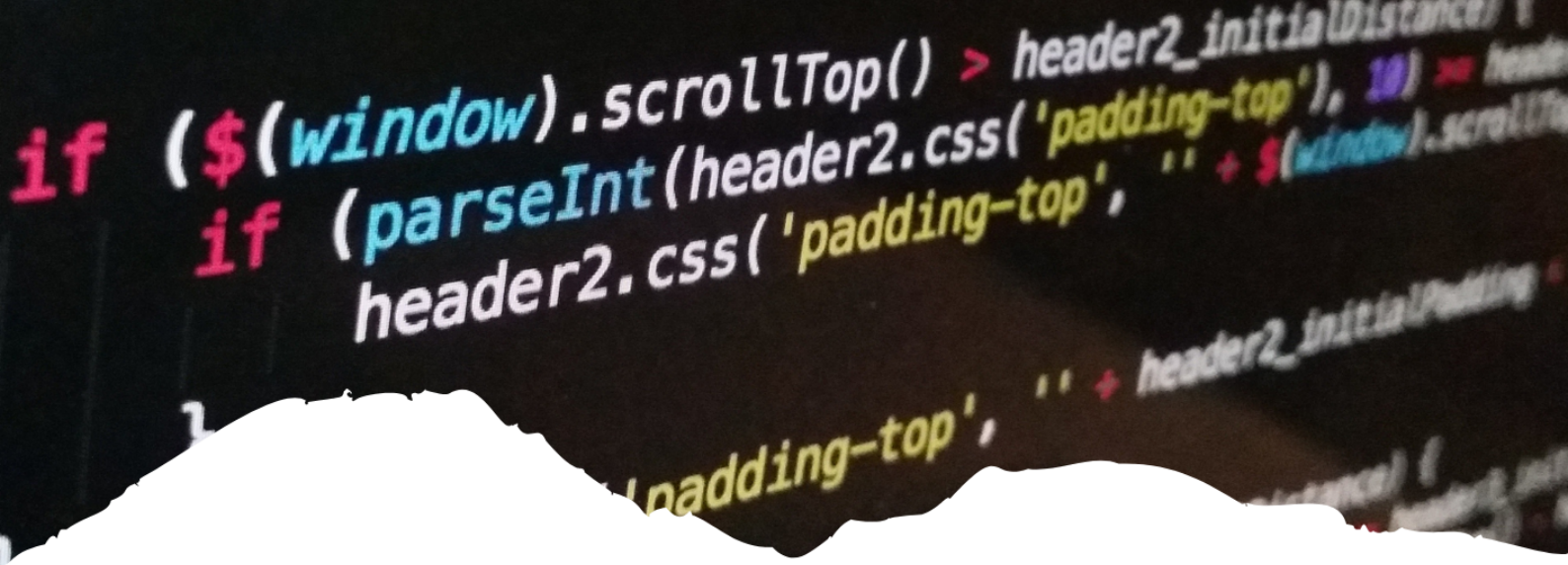
HEUSER.C.A. **Projeto de Banco de Dados**. ed.- Dados Eletrônicos. - Porto Alegre: Bookman, 2009

MACHADO. F. N. R; Abreu. M. P**. Projeto de Banco de Dados: Uma Visão Pratica**. ed. São Paulo: Erica, 2018

MACHADO. F. N. R. **Banco de Dados Projeto e Implementação**. 4. ed. São Paulo: Erica, 2020

RAMAKRISHNAN. R; GEHRKE. J. **Sistemas de Gerenciamento de Banco de Dados**. 3. ed. – Dados eletrônicos. – Porto Alegre: AMGH, 2011

TAKAI. O. K; Italiano. I. C; Ferreira. J. E**. Introdução à Banco de Dados**. DCC-IME-USP, 2005



23

SISTEMA DE IDENTIFICAÇÃO E AUTENTICAÇÃO: BIOMÉTRICA FACIAL

IDENTIFICATION AND AUTHENTICATION SYSTEM: FACIAL BIOMETRICS

Jhonathan Carvalho dos Santos

Resumo

A biometria refere-se ao método automatizado de identificar um indivíduo com base em sua identidade, traços físicos ou comportamentais distintivos. A palavra biometria vem da palavra grega que significa “medida biológica” que é uma ciência responsável por estudar as características físicas ou comportamentais individuais de cada pessoa, a premissa básica são que as pessoas têm características estruturais que as tornam únicas, essas características podem incluir a impressões digitais, características faciais, padrões de íris, impressões de voz e até traços comportamentais, como velocidade de digitação ou estilo de caminhada. O método biométrico tornou-se cada vez mais popular nos últimos anos devido à sua capacidade de reconhecer os indivíduos com precisão e segurança. Pelo supracitado o tema do artigo é sistema de identificação e autenticação biométrica facial, dessa forma os objetivos da pesquisa é analisar a importância do sistema de identificação e autenticação biométrica facial, conceituar biométrica facial, compreender a importância da biométrica facial e identificar como é utilizada a biométrica facial. Para isso a metodologia adotada foi a pesquisa bibliográfica nas principais bases digitais Scielo e Google Acadêmico nos meses de março a maio de 2023.

Palavras-chave: Autenticação, Biométrica Facial, Identificação.

Abstract

Biometrics refers to the automated method of identifying an individual based on their identity, distinctive physical or behavioral traits. The word biometrics comes from the Greek word that means “biological measurement” which is a science responsible for studying the individual physical or behavioral characteristics of each person, the basic premise is that people have structural characteristics that make them unique, these characteristics can include the fingerprints, facial features, iris patterns, voice prints and even behavioral traits like typing speed or walking style. The biometric method has become increasingly popular in recent years due to its ability to accurately and securely recognize individuals. Based on the above, the theme of the article is a facial biometric identification and authentication system, so the research objectives are to analyze the importance of a facial biometric identification and authentication system, conceptualize facial biometrics, understand the importance of facial biometrics and identify how the facial biometrics. For this, the methodology adopted was the bibliographical research in the main digital databases Scielo and Google Scholar from March to May 2023.

Keywords: Authentication, Facial Biometrics, Identification.

1. INTRODUÇÃO

A busca pela precisão da autenticidade de acessos escalou de uma maneira significativa no ramo tecnológico, o que incentivou a criação de métodos de verificação que vão além de senhas que faziam com que o usuário fosse obrigado a decorar uma sequência de números e letras para possuir o mínimo de segurança.

A biometria refere-se ao método automatizado de identificar um indivíduo com base em sua identidade, traços físicos ou comportamentais distintivos. Essas características podem incluir a impressões digitais, características faciais, padrões de íris, impressões de voz e até traços comportamentais, como velocidade de digitação ou estilo de caminhada.

O método biométrico tornou-se cada vez mais popular nos últimos anos devido à sua capacidade de reconhecer os indivíduos com precisão e segurança. Diante disso essa pesquisa será de grande importância aos estudantes de ciência da computação e a todos que se interessem pelo tema.

Por esse motivo o problema de pesquisa foi, quais são os benefícios do sistema de identificação e autenticação biométrica facial para os usuários? Pelo supracitado os objetivos da pesquisa é analisar a importância do sistema de identificação e autenticação biométrica facial, conceituar biométrica facial, compreender a importância da biométrica facial e identificar como é utilizada a biométrica facial.

2. DESENVOLVIMENTO

2.1 Biometria

A biometria, antes de tudo, refere-se a uma ciência responsável por analisar características biológicas, ela é responsável pelo estudo da medição e estatística dos seres vivos. A palavra biometria vem da palavra grega que significa “medida biológica” que é uma ciência responsável por estudar as características físicas ou comportamentais individuais de cada pessoa, a premissa básica são que as pessoas têm características estruturais que as tornam únicas.

Seu principal fundador e estudioso foi o brilhante Francis Galton, além de descobrir como descrever, diferenciar e quantificar o comportamento humano, criou a famosa teoria da genética, inventando assim o sistema de coleta de impressões digitais. A biometria existe em várias partes do corpo humano e no comportamento humano, por exemplo: rosto, voz, palma e dedos, olhos, retina e íris, geometria da mão etc., mesmo gêmeos idênticos têm características que diferem entre si (FERREIRA, 2017).

Ela é definida por Ramos (2012) como:

> A biometria fisiológica é baseada em medições e dados provenientes da parte do corpo humano enquanto que a biometria comportamental é baseada em medições de características de forma indireta e de dados relacionados a uma ação tomada por uma pessoa. Um dos métodos adotados na biometria comportamental é a métrica, a qual subdivide um comportamento em começo, meio e fim. (RAMOS, 2012).

A biometria está ganhando popularidade e é amplamente utilizada nos negócios e na

vida cotidiana, especialmente no campo da segurança. Este crescente campo da tecnologia torna-se parte integrante do nosso dia a dia, pois cada pessoa é única e tem características próprias distintas, para garantir a legalidade do logotipo. Nessa lógica dos sistemas modernos, a biometria substitui senhas já desatualizadas, digitais ou criptografados. O próprio corpo passa a ser o código para entrar em determinada sala, acessar determinadas informações e até registrar horários de chegada e saída, menos suscetível a fraudes ou erros (FERREIRA, 2017).

2.1.1 Verificação e identificação

Na autenticação, o usuário afirma alguma identidade, cabe ao sistema determinar se esta afirmação é verdadeira analisando a biometria do usuário pessoal. Nesse caso, as amostras coletadas são comparadas apenas com o modelo correspondente quem o usuário afirma ser. Se as amostras e modelos coletados tiverem altamente semelhante, o sistema considera a afirmação como verdadeira, de outra forma, ele é rejeitado e o usuário é considerado um impostor. Os sistemas de autenticação são geralmente adequados para cenários onde o objetivo é restringir o acesso das pessoas a determinados serviços não autorizado (JAIN; ROSS; NANDAKUMAR, 2011).

Segundo Jain, Ross e Nandakumar (2011), a função de reconhecimento pode ser dividida em duas categorias, reconhecimento positivo e reconhecimento negativo. em reconhecimento positivo, o sistema tenta responder à pergunta “Você é alguém que o sistema conhece?”, e identificar um indivíduo com base em um conjunto de identidades conhecidas. Já a identificação negativa tenta responder à pergunta “Você é quem diz ser?”, considerando que o usuário nega sua identidade. A finalidade do Sistema de Identificação Negativa é para evitar que uma pessoa use várias identidades.

Ao se tratar de reconhecimento positivo ou negativo, as amostras coletadas dos usuários são comparadas com o modelo de todas as pessoas no banco de dados, o sistema retorna com a identidade da pessoa cujo modelo de saída é mais semelhante à amostra ou resposta que indica que a pessoa que está sendo perfilada não está registrada no banco de dados.

2.1.2 Detecção facial

Muitos dos algoritmos de reconhecimento facial precisam de treinamento extensivo antes que possam alcançar um resultado satisfatório. Esses algoritmos devem ser treinados em uma série de imagens de várias faces diferentes, bem como em uma série de imagens de objetos não faciais.

Segundo Pereira (2007), a maioria das ferramentas de software de reconhecimento facial que estão sendo desenvolvidas são baseadas em certas características e pontos estratégicos da face, como a distância entre os olhos, a profundidade dos olhos, o tamanho do nariz, a mandíbula, a distância entre os olhos e as sobrancelhas, e outros pontos podem ser usados, dependendo do revelador. A identificação e captura adequada desses pontos pode ser feita em uma imagem com apenas duas dimensões, mapeando o ponto a ser analisado e construindo um método para enquadrá-lo em três dimensões geométricas para maior precisão. Depois que a foto é tirada, cada ponto é convertido em dados digitais que são comparados com outros dados contidos no banco de dados.

O problema de reconhecimento facial pode então ser abordado com um padrão de

reconhecimento de duas classes, onde uma classe corresponde a rostos e a outra classe a tudo o que não é um rosto. A dificuldade de reconhecer rostos em imagens se deve ao fato de que, em princípio, não se sabe de antemão em que área da imagem os rostos podem estar e em que escalas eles serão encontrados, e também porque alguns objetos ou uma combinação deles se assemelham a rostos quando digitalizados em baixa resolução (BRAGA, 2013).

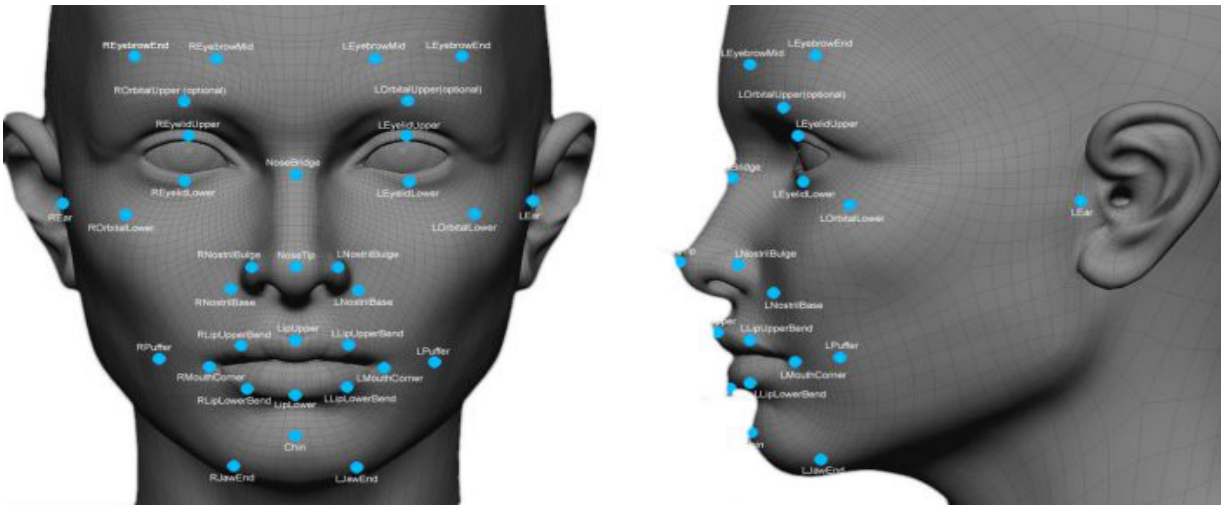


Figura 01: Reconhecimento facial

Fonte: Tecnobog (2019).

A detecção de rosto e a extração de características faciais podem ser realizadas simultaneamente, dependendo do tipo de algoritmo usado.

Segundo Pereira (2007), várias formas de reconhecimento desses padrões podem ser consideradas, como reconhecimento em imagens não frontais de rostos, reconhecimento em ambientes externos afetados pela luz, reconhecimento de rostos masculinos, que é mais propício à identificação com mais traços proeminentes, enquanto os traços femininos são em sua maioria suaves e difíceis de identificar.

Para possibilitar o reconhecimento facial, é necessário o processamento de imagens fixas, que é uma série de procedimentos preparatórios que envolvem técnicas de processamento de imagens. Um dos cuidados a ter é trabalhar nas partes externas dos rostos da imagem. Outras considerações são: correção de iluminação; processamento digital para melhorar a imagem; forma de aquisição da imagem; extração de objetos do fundo; parametrização da imagem, definindo a área do objeto a ser analisada; e reconhecimento do objeto por meio de ferramentas específicas.

Portanto, os principais métodos utilizados para adaptar uma imagem ao reconhecimento de padrões são: conversão da imagem colorida para tons de cinza, binarização (adaptar a imagem para distinguir tons e ser capaz de separar o fundo do rosto), detecção de contorno e segmentação da imagem em regiões para facilitar a análise do perfil (CASTILLO, 2012).

Os Histogramas de imagens digitais são técnicas utilizadas no processamento de imagens no domínio espacial. Os histogramas podem ser usados para obter dados estatísticos ou para aprimorar imagens, indicando qualitativamente os níveis de brilho e contraste de uma imagem (CORDEIRO, 2015).

Portanto, a equalização de histograma visa a obtenção de um histograma homogêneo da imagem, com alto contraste, o que ajuda a identificar elementos na imagem inicial. Nessa direção, “a equalização do histograma envolve o ajuste dos níveis de cinza de uma

imagem para que os níveis de cinza da imagem de entrada sejam mapeados em um histograma uniforme" (CORDEIRO, 2015).

Duas métricas são importantes ao avaliar a qualidade do algoritmo: o número de objetos que foram identificados incorretamente como um rosto (falsos positivos) e o número de rostos que não foram identificados (falsos negativos), idealmente, o algoritmo teria ambos os valores zero (BRAGA, 2013).

2.1.3 Viola Jones

A detecção de facial é um aspecto importante para a biometria, vigilância por vídeo e interação humano-computador. o algoritmo de detecção de face Viola-Jones que atende ao desempenho da implementação de FPGA mais rápida conhecida. O design da GPU oferece custos de desenvolvimento muito menores, mas a implementação do FPGA consome menos energia (VIKRAM, 2017).

O algoritmo de Viola-Jones utiliza características semelhantes a Haar, ou seja, um produto escalar entre a imagem e alguns modelos semelhantes a Haar. Mais precisamente, deixe I e P denotar uma imagem e um padrão, ambos o mesmo tamanho N × N (WANG, 2014).

Para compensar o efeito de diferentes condições de iluminação, todas as imagens devem ser médias e variância normalizada de antemão. Aquelas imagens com variância menor que um, com pouca informação de interesse em primeiro lugar, são deixados fora de consideração.

2.1.4 Arquitetura de um sistema biométrico

As tecnologias biométricas baseiam-se na comparação dos dados biométricos obtidos na fase de registo e os dados biométricos fornecidos pelo utilizador para utilizar um determinado serviço (na fase de detecção), ou seja, um sistema biométrico é basicamente um sistema de reconhecimento facial que identifica uma pessoa. com base em dados de referência derivados de uma característica física ou comportamental específica do indivíduo (SIMÃO, 2020).

Na fase de registro, o recurso biométrico estudado (por exemplo, impressão digital, imagem da íris) é armazenado usando um sensor e, em seguida, dados digitais (matriz de pixels, sinal digital etc.). Criada em muitos casos, apenas as características essenciais são extraídas dos dados para construir o modelo. As principais vantagens desse procedimento são a redução do volume de dados e maior anonimato (SIMÃO, 2020).

No entanto, apesar dos grandes esforços e progressos do comitê ISO-SC37 na solução desses problemas, atualmente ainda há uma tendência de armazenar dados brutos para garantir a interoperabilidade dos sistemas biométricos. A fase de registo permite a ligação entre utilizadores. Portanto, a etapa de cadastro possibilita a associação entre o usuário e suas características biométricas. Durante esta etapa, um modelo de referência é obtido a partir de uma ou mais amostras do recurso biométrico em questão.

2.1.5 Íris

A íris é o anel colorido do olho localizado entre a pupila e a esclera (a parte branca do olho). É um órgão interno, protegido, mas visível à distância. A estrutura visível da íris é

formada durante o desenvolvimento fetal e se estabiliza durante os dois primeiros anos de vida sem sofrer alterações ao longo dos anos (SBI, 2020).

A estrutura complexa da íris, caracterizada por uma combinação de características especiais como coroa, glândula, filamentos, sardas, sulcos radiais e listras, é única para cada indivíduo e é muito útil como meio de identificação. Assim, como as impressões digitais, até mesmo as íris de gêmeos idênticos são diferentes, assim como as íris de ambos os olhos do mesmo indivíduo (SBI, 2020).

Normalmente, as medições biométricas devem ser processadas para colocá-las no espaço métrico apropriado. Eles são imagens de íris convertidas em vetores no espaço de Hamming, chamado código de íris.

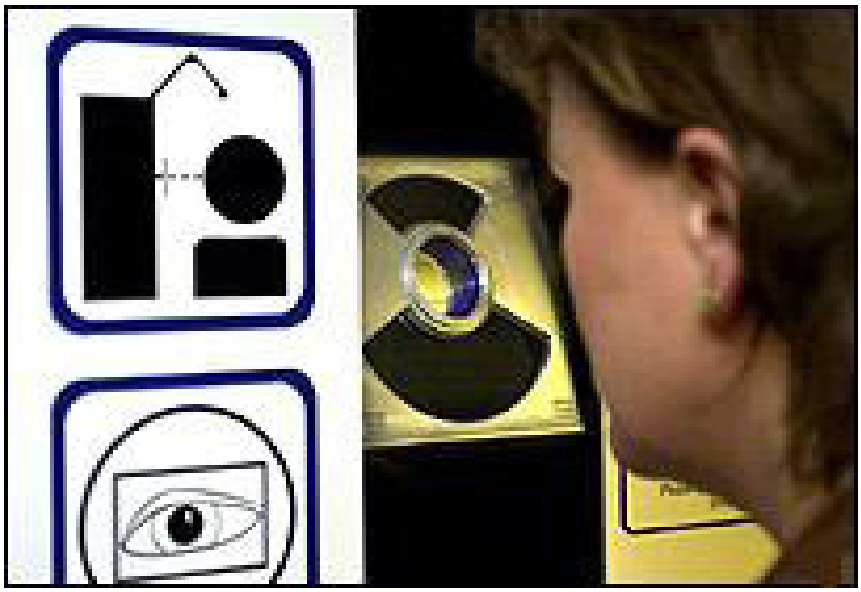


Figura 02: Ortogonalidade do olho

Fonte: GTA (2018)

A medida canônica do erro de íris é a distância binária de Hammingt. O algoritmo proposto por Daugman normalmente produz um código de íris de comprimento 208 bits. A priori OSIRIS pode fornecer códigos de tamanhos diferentes dependendo da escolha dos parâmetros (filtros e pontuações) e com limitações, principalmente relacionadas à propagação de Hamming para usuários legítimos e fraudadores.

Para se obter o código íris, inicialmente, isola-se a íris na imagem do olho. A imagem da Iris é, então, decomposta usando wavelets 2D de Gabor para diferentes orientações e a informação de fase decomposta é quantizada a fim de se obter o código Iris binário

2.2 Metodologia

O estudo irá abordar o sistema de identificação e autenticação biométrica facial. É um trabalho de caráter teórico, incluindo uma revisão de literatura e com pretensão de ser uma simplificada sistematização sensata de pensamentos consequentes de fontes sagradas, a cerca de um assunto específico, foi será realizada uma consulta a livros, dissertações e por artigos científicos selecionados através de busca nos seguintes bases de dados Scielo e Google Acadêmico. O período dos artigos pesquisados foram os trabalhos publicados nos últimos “10” anos, para isso as palavras-chave utilizadas foram: “sistema de identificação”, “autenticação” e “biometria facial”. Quanto à solução do problema, aqui está um es-

tudo qualitativo, principalmente descritivo, destinado a explicar por que as coisas ocorrem.

2.3 Resultados e Discussão

A utilização do reconhecimento facial em qualquer das suas tarefas concebíveis é uma atividade complexa, cuja execução depende de vários passos executados numa ordem específica que definem o processo necessário para a utilização e construção de um sistema de reconhecimento facial que procede do uso da imagem facial junto com os algoritmos necessários que serão enviados.

De acordo com o livro *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (GATES PRESS, 2011), a biometria facial, é um ramo da inteligência artificial e aplicações de visão computacional, são tecnologias complexas que incluem, desde o reconhecimento automático até o reconhecimento individual baseado em dados faciais característicos. Nem a detecção de expressão nem o reconhecimento facial precisam ser perfeitos para serem eficazes. São tecnologias básicas, mas difíceis de projetar para alcançar níveis mais altos de segurança. Por exemplo, o autor dedica parte do livro a explicar como o reconhecimento facial pode desempenhar um papel na prevenção de ataques terroristas e no acesso a sistemas críticos (COSTA, 2019).

Como um dos recursos que os humanos mais usam para identificar outra pessoa, ele conecta os diferentes pontos de um rosto que, juntos, formam um padrão de reconhecimento viável. Segundo Moraes (2010), as aplicações que utilizam esse recurso vão desde o exame de faces humanas estáticas em ambientes controlados até imagens em tempo real com fundos complexos. As abordagens mais populares em problemas de reconhecimento facial são “baseadas na localização e análise de atributos faciais como olhos, nariz e boca, ou sua análise global, representada como uma combinação ponderada de uma série de faces canônicas”. (MORAEAS, 2010, p. 27).

Vale ressaltar que o reconhecimento facial é baseado no treinamento para localizar rostos em imagens, durante o processo de treinamento recebe várias fotos de rostos para aprender a detectá-los. Depois de receber a imagem, ele aprende a distinguir entre objetos e rostos e combinar algoritmos de análise para obter o reconhecimento facial (KLOSOWSKI, 2020).

Para reconhecimento facial, a classificação indica qual pessoa pertence ao rosto de teste. “O objetivo é encontrar na base de dados a face que mais se assemelha à imagem de teste. Para cada face de teste, existe uma face que mais se assemelha a ela na base de dados” (SANTOS, 2017, p. 49).

No Brasil, a tecnologia de reconhecimento facial usando inteligência artificial para detectar faces está em uso desde 2011 e 47 (quarenta e sete) implementações no setor público foram relatadas até 2019. O RF é utilizado principalmente em quatro áreas: transporte, segurança pública, educação e controle de fronteiras (INSTITUTO IGARAPÉ, 2021).

Existem algoritmos de classificação como: K-Nearest Neighbor (K-NN), Support Vector Machine (SVM). O algoritmo K-NN segundo Diniz et al. (2013, p. 45) baseia-se na busca dos vizinhos mais próximos do padrão de teste. As buscas na vizinhança são feitas usando uma métrica de distância. Existem diferentes métricas para calcular a distância entre dois pontos, as mais comuns na literatura da área são: distância euclidiana, distância de Mahalanobis, distância de Manhattan, distância de Minkowski etc.

3. CONSIDERAÇÕES FINAIS

Foi possível concluir através da pesquisa que a biometria é o estudo estatístico das características físicas ou comportamentais humanas, que também são conhecidas como recursos biométricos, ela tornou-se uma ferramenta cada vez mais importante para identificar indivíduos na sociedade, seja para prevenir fraudes, aumentar a privacidade, controlar acesso a áreas com restritas informações e até mesmo ser possível que identifique criminosos em ambientes públicos como portos e o aeroporto.

A cada dia, a biometria, principalmente a facial está se tornando um recurso valioso para identificação de pessoas por ser uma tecnologia acessível, segura e confiável. Diversas entidades de segurança pública e privada em todo o mundo estão empenhadas em utilizar a biometria na segurança para controle de acesso e identificação dos usuários do sistema. Logo, a vantagem principal dessa técnica é que com ela os indivíduos não precisam possuir itens ou se lembrar de algo pessoal para ter acesso as suas informações e ser autenticado.

Referências

BRAGA, Luiz Filipe Zenicola et al. **Sistemas de Reconhecimento Facial**. 2013. Tese de Doutorado. UNIVERSIDADE DE SÃO PAULO.

CASTILHO, J. M. **Estudo e implementação de técnicas de processamento de imagens aplicadas em reconhecimento de face**. Trabalho de Conclusão de Curso - Bacharel em Engenharia da Computação – Universidade Federal do Pará, 2012.

CORDEIRO, F. R. **Desenvolvimento de um Mecanismo Semi-Supervisionado para Segmentação de Tumores em Imagens de Mamografia Digital**. Tese, Universidade Federal de Pernambuco, Centro de Informática, 2015.

COSTA, Vambaster José da. **Reconhecimento de Padrões Faciais: Uma Síntese.** Monografia, (Graduação) Universidade Tecnológica Federal do Paraná, Paraná. 2019

DINIZ, F. A. et al. **Redface: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces**. Revista Brasileira de Computação Aplicada, v. 5, n. 1, p. 42-54, 2013.

FERREIRA, Thiago Marcos. **O uso da biometria no controle das horas trabalhadas pelos policiais civis de Santa Catarina e seus reflexos jurídicos**. Araranguá, 01 de maio de 2017.

GATES, K. **Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.** Critical Cultural Communication. NYU Press, 2011.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. 2021.

JAIN, A. K.; ROSS, A. A.; NANDAKUMAR, K. **Introduction to biometrics**. [S.l.]: Springer Science & Business Media, 2011.

KLOSOWSKI, ***Thorin. Facial Recognition Is Everywhere. Here's what we can do about it. Wirecutter***, 15 de julho de 2020.

MORAES, Jairo. **Controle de acesso baseado em biometria facial.** Universidade Federal do Espírito Santo, 2010.

PEREIRA, A. **Ambientes Virtuais de Aprendizagem: em diferentes contextos**. Rio de Janeiro: Ciência Moderna Ltda, 2007.

RAMOS, Maurício Peres. **Controle de acesso biométrico.** Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina. Florianópolis, 2012.

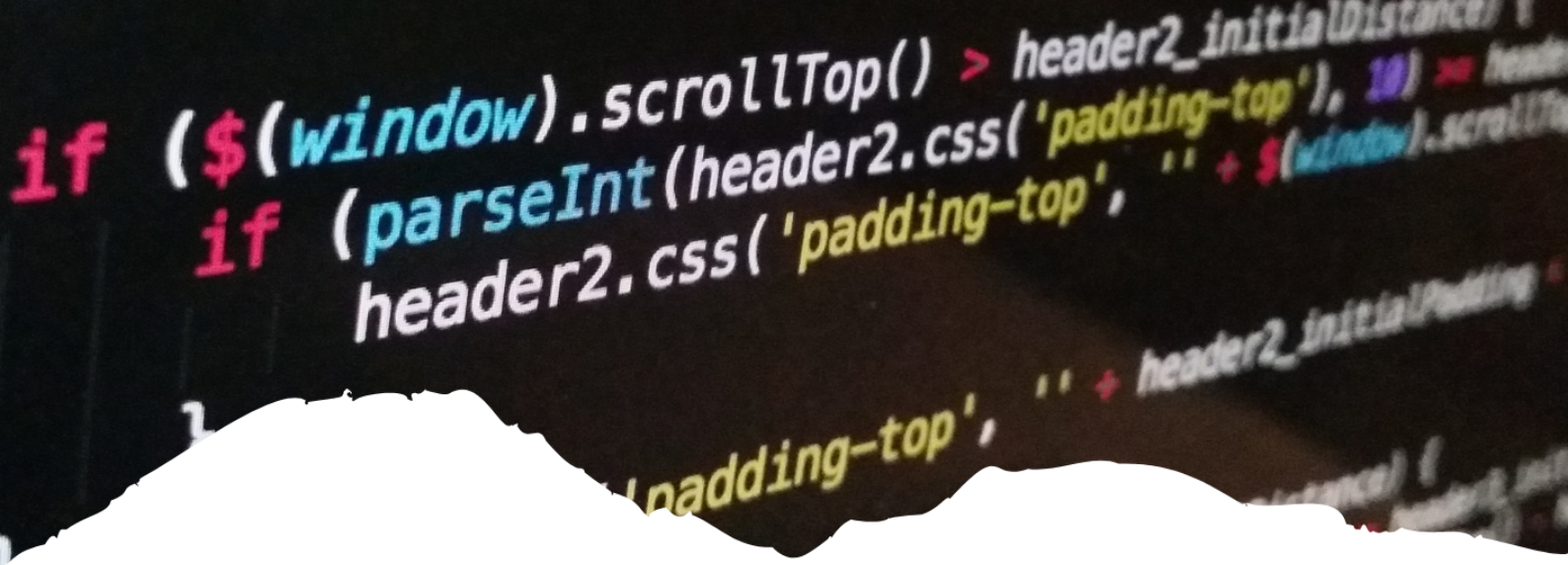
SANTOS, P. S., STEMMER, M. R., CASAGRANDE, J. H. B., **Rastreamento De Múltiplos Objetos Em Cenas De Videovigilância Baseado No Algoritmo De Extração Vibe E Filtro De Kalman.** SBAI, Porto Alegre, 04 de out. de 2017.

SBI, Sociedade Brasileira de Imunologia. **Impressões digitais.** Nelson Vez, 2020.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; **Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas**. InternetLab/IDEC, São Paulo, 2020.

VIKRAM, K.; PADMAVATHI, S. **Facial partsdetectionusing Viola Jones algorithm**. In: 2017 4th international-conferenceonadvancedcomputingand communication systems (ICACCS). IEEE, 2017. p. 1-4.

WANG, Yi-Qing. **Ananalysisofthe Viola-Jones face detectionalgorithm**. ImageProcessingOnLine, v. 4, p. 128-148, 2014.



24

UTILIZAÇÃO DOS SERVIÇOS EM NUVEM NO AMBIENTE EMPRESARIAL, E COMO ELES PODEM AJUDAR NA ACELERAÇÃO E OTIMIZAÇÃO DOS PROCESSOS

USE OF CLOUD SERVICES IN THE BUSINESS ENVIRONMENT, AND HOW THEY CAN HELP ACCELERATE AND OPTIMIZE PROCESSES

Rafael Alves Martins

Resumo

A computação em nuvem, que abrange cada elemento de um computador, como inicialização de software e uso de armazenamento de banco de dados na nuvem, agora é um serviço indispensável para melhorar a eficiência e a produtividade dos negócios. Os serviços de computação em nuvem incluem servidores, armazenamento, redes, software, bancos de dados, aplicativos e muito mais. Ao contrário do local, onde era necessário preparar um servidor físico no momento da implantação, a computação em nuvem tem a grande vantagem de poder implantar rapidamente e reduzir o investimento inicial. Um mecanismo chamado virtualização é indispensável para realizar a computação em nuvem. A virtualização é uma tecnologia que integra várias peças de hardware com software de virtualização. Por exemplo, se você virtualizar um servidor, a quantidade de processamento da CPU e a capacidade de memória podem ser distribuídas para cada servidor virtual, permitindo o processamento simultâneo de dois ou mais sistemas.

Palavras-chave: Computação em Nuvem, Modelos de Implantação de Nuvem, Sistemas, Tecnologia.

Abstract

Cloud computing, covering every element of a computer, such as starting software and using cloud database storage, is now an indispensable service for improving business efficiency and productivity. Cloud computing services include servers, storage, networks, software, databases, applications, and more. Unlike on-premises, where it was necessary to prepare a physical server at the time of deployment, cloud computing has the great advantage of being able to deploy quickly and reduce the initial investment. A mechanism called virtualization is indispensable to perform cloud computing. Virtualization is a technology that integrates various pieces of hardware with virtualization software. For example, if you virtualize a server, the amount of CPU processing and memory capacity can be distributed to each virtual server, allowing simultaneous processing of two or more systems.

Keywords: Cloud computing, Cloud Deployment Models, Systems, Technology.

1. INTRODUÇÃO

Com o desenvolvimento da tecnologia de TI, algumas pessoas podem ouvir a palavra serviço em nuvem com mais frequência. Os serviços em nuvem são muito convenientes para uso privado e comercial, sendo uma tecnologia que pode resolver tarefas demoradas em um curto período de tempo.

Hoje em dia, em nosso dia a dia e em nossas atividades corporativas, nunca esquecemos a palavra nuvem. Estamos agora em uma era em que muitos serviços estão disponíveis na nuvem através da rede. E muitos serviços são prestados de acordo com a finalidade, como para consumidores e empresas.

A computação em nuvem é o uso de recursos do computador pela Internet. Os recursos de computador incluem aplicativos disponíveis na Internet, plataformas como ambientes de desenvolvimento e infraestrutura de TI como servidores em nuvem e máquinas virtuais. Considerando o cenário global em relação a utilização dos serviços em nuvem no ambiente empresarial, qual a importância da computação em nuvem para a revolução no empreendedorismo e de que modo a computação em nuvem traz impactos para o setor industrial?

A utilização dos serviços em nuvem no ambiente empresarial e seus benefícios para a otimização do setor industrial através da sua utilização e ferramentas, as quais são utilizadas para agilidade dos processos internos da empresa, visto que os serviços em nuvem possuem muitos benefícios em relação aos outros tipos de armazenamentos, pois o usuário consegue ter acesso a dados e aplicações que estão sendo executados na nuvem estando em qualquer lugar do mundo através da internet.

Os serviços fornecidos na forma de computação em nuvem, cujo quais são especialmente chamados de serviços em nuvem. Que permitem com que as empresas conduzam de forma eficiente os processos de gestão empresarial, trazendo assim um melhor desempenho para a mesma, pois oferecem alternativas de trabalho e agilizam processos, economizando tempo.

A crescente digitalização dos processos industriais tem levado a um aumento da quantidade de dados produzidos por empresas de diversos setores industriais. Os recursos dos provedores de nuvem estão disponíveis como um pool do qual os usuários podem extrair. Estes últimos não precisam saber exatamente onde estão localizados os servidores que prestam os serviços que utilizam. O objetivo geral da pesquisa irá ser descrever o método de descrever sobre a integração de recursos da computação em nuvem e seus benefícios para o setor empresarial; tendo como objetivo específico demonstrar a Demostrar os tipos de serviços disponíveis de computação em nuvem; Detalhar etapas de implementação em nuvem, caracterizar o processamento dos dados na nuvem, combinado com uso de diferentes recursos.

2. COMPUTAÇÃO EM NUVEM

O termo computação em nuvem está associado a um novo paradigma na área de computação. Basicamente, esse novo paradigma tende a deslocar a localização de toda a infraestrutura computacional para a rede. Com isso, os custos de software e principalmente de hardware podem ser consideravelmente reduzidos (VAQUERO et al., 2009).

Embora este assunto esteja sendo amplamente discutido nos dias de hoje, ainda não há uma definição completa do termo. Na literatura, podemos encontrar uma infinidade de definições que em algumas vezes podem ser semelhantes, e em outras podem apresentar conceitos diferentes. Por exemplo, alguns autores defendem que a escalabilidade e o uso otimizado dos recursos são características chave da computação em nuvem, enquanto outros discordam, afirmando que esses elementos não são características, e sim requerimentos de uma infraestrutura que suporta esse novo paradigma da computação (VAQUERO et al., 2009).

3. COMPUTAÇÃO EM NUVEM DENTRO DA SOCIEDADE MODERNA

Com o avanço da sociedade humana moderna, serviços básicos e essenciais são quase todos entregues de uma forma completamente transparente. Serviços de utilidade pública como água, eletricidade, telefone e gás tornaram-se fundamentais para nossa vida diária e são explorados por meio do modelo de pagamento baseado no uso (VECCHIOLA et al., 2010). As infraestruturas existentes permitem entregar tais serviços em qualquer lugar e a qualquer hora, de forma que possamos simplesmente acender a luz, abrir a torneira ou usar o fogão. O uso desses serviços é, então, cobrado de acordo com as diferentes políticas de tarifação para o usuário final. Recentemente, a mesma ideia de utilidade tem sido aplicada no contexto da informática e uma mudança consistente neste sentido tem sido feita com a disseminação de Computação em Nuvem (SOUSA, 2010).

Computação em nuvem é uma tendência recente de tecnologia cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso. Tendências anteriores à computação em nuvem foram limitadas a uma determinada classe de usuários ou focadas em tornar disponível uma demanda específica de recursos de TI, principalmente de informática (BUYYA et al., 2010).

O conceito de disponibilizar serviços de software e hardware por uma rede global não é novo. Já podemos encontrar raízes desse conceito na década de 60, quando Joseph Carl Robnett Licklider, um dos responsáveis pelo desenvolvimento da ARPANET (Advanced Research Projects Agency Network), já havia introduzido a idéia de uma rede de computadores intergaláctica (MOHAMED, 2020).

Computação em nuvem pretende ser global e prover serviços para as massas que vão desde o usuário final que hospeda seus documentos pessoais na Internet até empresas que terceirizam toda infraestrutura de TI para outras empresas (SOUSA, 2010).

Ainda que possua características atrativas para as empresas de menor porte, a computação em nuvem conquistou também o mercado das grandes empresas, oferecendo soluções robustas e customizadas, por meio de serviços com grande capacidade de processamento e ambientes seguros. Em 2017, das empresas listadas na “Fortune Global 50”, apenas duas não anunciaram o uso desse tipo de tecnologia (ALBERTO EDUARDO, 2021).

A adoção de novos modelos de computação é uma decisão que envolve diversas áreas da empresa, com análise de vários fatores. Exige uma gestão eficaz e que, nos casos de empresas menores, permite menos erros. Dentre as opções existentes no mercado, o conceito de “nuvem” assume uma posição de vanguarda quando se fala em computação atualmente, devido às suas características inovadoras, com foco em compartilhamento de recursos e redução de custos. Por isso, é importante conectar as empresas de menor porte a esse novo conceito, apresentando suas características e corroborando a importância de investimento em TI de ponta, que atualmente se resume no modelo de computação em nuvem (FREITAS, 2021).

4. A CRESCENTE DIGITALIZAÇÃO DOS PROCESSOS INDUSTRIAIS

A crescente digitalização dos processos industriais tem levado a um aumento da quantidade de dados produzidos por empresas de diversos setores industriais. Isso se deve à integração da Internet das Coisas, dispositivos inteligentes e robótica nas instalações de fabricação industrial. Gerenciar manualmente esses grandes conjuntos de dados é praticamente impossível, e manter data centers no local para cuidar da análise de dados tem seu próprio risco e não é economicamente viável para pequenas empresas (MARCOS VINICIUS, 2021).

Além da área de entretenimento, negócios e demais funções cotidianas, grandes avanços vêm sendo conquistados quanto ao uso da tecnologia de nuvem na indústria. A natureza flexível e escalável da nuvem oferece uma solução mais abrangente para gerenciar os conjuntos de dados cada vez maiores produzidos nas instalações de fabricação (SPOSITO, 2021).

Devido à indústria 4.0, a tecnologia de nuvem na indústria vem trazendo benefícios, sendo aplicada para trazer melhorias para muitos processos. Quando bem adotada, a tecnologia de nuvem permite que indústrias imprimam mais funcionalidades no seu dia a dia, ajudando a adequação ao conceito 4.0, ao passo que também fornece infraestrutura para simplificar processos, agilizar a comunicação e gerar dados em tempo real (GERIBELLO, 2021).

Diante da rápida transformação digital presenciada no atual cenário, empresas são obrigadas a integrar tecnologias, como digitalização e automação de processos, Internet das coisas (IoT) e inteligência artificial em todas as suas operações. As aplicações das ferramentas como Big Data, Internet das Coisas (IoT) e Computação em Nuvem na Nova Indústria, se caracterizam por máquinas e equipamentos dotados de sensores que fazem interligação direta entre si via rede, gerando assim uma grande base dados inteligente, proporcionando múltiplas possibilidades de visões de mercado, fomentando a inovação nos modelos de negócio e processos produtivos, facilitando assim as tomadas de decisões devido à alta gestão de conhecimento (DOS SANTOS, 2021).

Neste cenário, a tecnologia de nuvem na indústria é o grande catalizador para essas tecnologias: “Ela funciona como uma plataforma de inovação, conectando diferentes tecnologias, facilitando o seu acesso e as transformando em valor para o negócio”, salienta o arquiteto de software de International Business Machines (IBM) Cloud (DOS SANTOS, 2021).

A atividade industrial, naturalmente, produz e consome muitos dados. Com a implementação do conceito 4.0, então, a tendência é de que cada vez mais os processos industriais necessitem e gerem mais informações. Armazenar, processar, distribuir corretamente e assegurar essa quantidade de dados não é tarefa fácil de ser feita sem o auxílio da tecnologia. (GEISSBAUER R.; VEDSO, 2016).

A computação em nuvem permite que as indústrias imprimam muito mais funcionalidades no seu dia a dia. Por exemplo, na fabricação de uma peça, as máquinas precisam de informações de comando, como quantidade, modelo, material utilizado etc. Ao mesmo tempo, elas produzem informações do seu desempenho, quantidade de peças produzidas, entre outras. Para um funcionário fazer a gestão deste processo com computação em nuvem, ele apenas precisa ter acesso ao software que recebe as informações do provedor (PEREIRA; DE OLIVEIRA, 2018).

Na indústria, a computação em nuvem também se destaca por permitir a descentralização da informação. Cada profissional que atua em uma fábrica pode ter as informações necessárias para executar seu trabalho, mesmo que estas sejam provenientes de outra

planta, de forma rápida e organizada. Além disso, por meio de acessos restritos, é possível segmentar quem tem acesso à o que (RODRIGUES; BIONDI, 2017).

Basicamente, portanto, a computação em nuvem, ou cloud, auxilia as indústrias a se adequarem ao conceito 4.0 ao passo que fornece infraestrutura para simplificar processos, agilizar a comunicação e fornecer dados em tempo real. O que se deve prestar mais atenção na aplicação do Cloud à indústria são os requisitos de segurança da informação e garantia de sua transmissão. A tecnologia implementa os recursos fundamentais para a indústria 4.0. (MONTEAGUDO, 2017).

Ao migrar os serviços para a nuvem, as empresas podem substituir os gastos de capital por "custos variáveis". Em vez de investir pesadamente em hardware e software de servidores desnecessários. Quando usada corretamente, a computação em nuvem é a abordagem mais econômica para implantar, gerenciar e atualizar a infraestrutura de TI (DOS SANTOS, 2021).

A computação em nuvem permite infraestrutura de TIC flexível e de baixo custo para empreendedores, PMEs e países em desenvolvimento com poucos recursos. Como resultado, a computação em nuvem tornou-se a base que suporta o crescimento de vários setores, não apenas o setor de informação e telecomunicações, e as organizações que puderem utilizar isso de forma eficaz terão o trunfo para vencer a competição internacional cada vez mais acirrada. Além disso, a computação em nuvem oferece serviços por meio de data centers distribuídos em diversas regiões, o que ajuda a reduzir o risco de desastres e ataques cibernéticos (GUEDES; CARLOS RODRIGO, 2018).

5. MODELOS DE IMPLANTAÇÃO DE NUVEM

Usuários do armazenamento em "nuvem" O serviço de computação em nuvem pode ser classificado quanto à restrição de acesso aos usuários, nas seguintes categorias. Existem quatro categorias distintas de nuvem, as públicas, privadas, Comunitárias e híbridas (SIMIONI, 2018).

5.1 Nuvem pública

A nuvem pública é aquela em que os serviços e a infraestrutura são fornecidos por terceiros. As ferramentas, recursos e espaços são compartilhados e gerenciados por provedores de serviços que os entregam aos clientes através de uma conexão segura via internet. No modelo de implantação de nuvem pública, a infraestrutura de nuvens é disponibilizada para o público em geral, sendo acessado por qualquer usuário que conheça a localização do serviço. Neste modelo de implantação não podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes, e menos ainda, utilizar técnicas para autenticação e autorização (SIMIONI, 2018).

Os administradores de TI criam redes de nuvem pública com várias máquinas virtuais (VMs) fragmentadas de um grande conjunto de data centers de terceiros. Ao virtualizar recursos de computação, processamento e armazenamento, provedores terceirizados podem oferecer aos usuários finais uma variedade de serviços em nuvem, desde opções simples de armazenamento até aplicativos de software e ferramentas de desenvolvimento. Todos eles podem ser acessados através de uma conexão com a internet. Os usuários finais de muitas empresas podem usar seus serviços por meio de aplicativos móveis e outros portais da web (THOMÉ; HENTGES, 2013).

As soluções de nuvem pública são uma das infraestruturas de TI mais usadas para computação e armazenamento atualmente. Os exemplos mais usados são Google Workspace, Amazon Web Services (AWS), Dropbox, serviços da Microsoft, como Microsoft 365 e Azure, e serviços de streaming, como Netflix. Em todos os casos, a nuvem pública usa senhas como linha de frente de segurança para compartilhar os mesmos recursos em uma conexão com a Internet (MEIRELLES, 2015).

O Google Workspace oferece vários aplicativos, desde processamento de documentos até armazenamento virtual e salas de conferência. Esses aplicativos geralmente são usados ao mesmo tempo por um ou vários usuários em uma organização ou empresa. As soluções de nuvem pública podem acessar, editar e compartilhar todos os tipos de dados, permitindo tipos de produtividade impossíveis ou inacessíveis com TI rigorosa no local. Os funcionários de hoje podem trabalhar e acessar dados em praticamente qualquer lugar do mundo, redefinindo quantas empresas operam e trabalham juntas (MEIRELLES, 2015)

As opções de armazenamento em nuvem pública também oferecem aprimoramentos de segurança e backup. Em caso de falha ou corrupção do servidor, os dados carregados na nuvem permanecem intactos. As nuvens públicas também são adequadas para cargas de trabalho flexíveis e variáveis. Com o conhecido “clique em um botão”, os usuários têm acesso a recursos sob demanda, oferecendo às empresas uma maneira mais eficiente de reduzir o desperdício de espaço de TI (SIMIONI, 2018).

5.2 Nuvem privada

No modelo de implantação de nuvem privada, a infraestrutura de nuvem é utilizada exclusivamente para uma organização, sendo esta nuvem local ou remota e administrada pela própria empresa ou por terceiros. Neste modelo de implantação são empregados políticas de acesso aos serviços. As técnicas utilizadas para prover tais características podem ser em nível de gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização. O gerenciamento e operação da nuvem são realizados por uma organização e o acesso às informações pode ser restrito por políticas de segurança (MARCOS ANTÔNIO, 2018)

Existem duas vantagens principais das nuvens privadas. Uma é que oferece melhores configurações de segurança do que a nuvem pública. A outra é que é possível construir um ambiente de nuvem especializado para um negócio específico, e é adequado para negócios de empresas, como empresas que não podem fazer negócios sem usar um sistema especial em vez de uma configuração altamente versátil como nuvem pública. é que um ambiente de infraestrutura combinada pode ser configurado (NEILSON CARLOS, 2012).

Como a nuvem privada é criada de acordo com as próprias especificações do usuário, o custo inicial e o custo de manutenção são maiores do que a nuvem pública e, em alguns casos, o preço é quase o mesmo do local. Especialmente o tipo local exigirá um cálculo cuidadoso de recursos no momento da introdução, especialmente no momento da aquisição de hardware. Além disso, como o tipo de hospedagem é quase baseado em contratos de longo prazo, é difícil aumentar ou diminuir recursos com facilidade (SOTO, 2011).

5.3 Nuvem comunitária

Neste caso, a infraestrutura da nuvem é administrada por um conjunto de organizações e cujo gerenciamento pode estar sujeito a regras estabelecidas pela comunidade

proprietária. Este tipo de modelo de implantação pode existir localmente ou remotamente e geralmente é administrado por alguma empresa da comunidade ou por terceiros (LOPES, 2018).

Uma nuvem comunitária é uma nuvem privada que se comporta como uma nuvem pública. São esforços colaborativos que permitem que diferentes organizações privilegiadas compartilhem e trabalhem no mesmo aplicativo. Em geral, as empresas que pertencem ao mesmo setor, mas compartilham preocupações comuns de segurança e conformidade, usam a nuvem da comunidade. Por exemplo, agências de saúde e governamentais geralmente implementam nuvens comunitárias em suas operações (PEDRO HENRIQUE, 2016).

Por haver instituições diferentes relacionadas ao gerenciamento de uma nuvem comunitária, ´é possível que existam políticas diferentes de gerenciamento entre as instituições e a unificação dessas políticas pode se mostrar complexa. As instituições podem ter normas diferentes a respeito da aquisição de equipamentos, procedimentos distintos para a utilização desses equipamentos, horários de funcionamento diferentes, políticas de segurança diferentes, entre outras peculiaridades que qualquer uma das instituições mantenedoras da nuvem comunitária pode ter. Essas diferenças criam necessidades particulares a cada instituição que devem ser atendidas pelo sistema que provê o serviço de computação em nuvem, mantendo as características importantes ao serviço (PEDRO HENRIQUE, 2016).

5.4 Nuvem híbrida

Trata-se de um grupo de nuvens, embora estas nuvens mantenham sua identidade diferenciada entre o grupo, podem ser do tipo privada, pública ou comunitária. As nuvens pertencentes as estas categorias podem estar associadas entre si por protocolos ou padrões técnicos. Tratando-se de Pessoas Físicas no âmbito de sua utilização, a nuvem capacita os usuários a armazenar grandes quantidades de conteúdo de diversas fontes e formatos. Com o avanço tecnológico esse tipo de armazenamento já invadiu os sistemas androides, IOS e Windows Phone, além de consoles, através de aplicativos, correios eletrônicos e plataformas digitais que permitem esse tipo de armazenamento (BORCARD, 2018).

A principal vantagem da nuvem híbrida é a capacidade de resposta. A necessidade de rápida adaptação e mudança de direção é um princípio fundamental dos negócios digitais. As organizações podem combinar recursos públicos, privados e locais conforme necessário para obter a capacidade de resposta necessária para ser competitivo (GOMES, 2017).

Nem todas as organizações são adequadas para a nuvem pública. É por isso que muitas empresas em potencial estão optando por uma combinação híbrida de serviços em nuvem. As nuvens híbridas oferecem os benefícios das nuvens públicas e privadas, aproveitando a arquitetura existente do data center (GOMES, 2017).

A arquitetura de nuvem híbrida tem como características principais os data centers locais, recursos de nuvem pública e privada e cargas de trabalho são claramente separados, mas vinculados por gerenciamento de dados comum. Pode executar aplicativos essenciais aos negócios ou conectar-se a sistemas existentes executados em arquiteturas tradicionais que contêm dados confidenciais que não são adequados para a nuvem pública (BORCARD, 2018)

A infraestrutura de nuvem híbrida é possibilitada pela malha de dados. A malha de

dados usa uma abordagem definida por software para fornecer um conjunto comum de serviços de dados em todas as combinações de recursos de TI (BORCARD, 2018).

Como as grandes corporações tendem a ser mais conservadoras, optam por nuvens híbridas, desta forma não descaracterizam tanto seus processos e suas políticas internas, já pequenas empresas por serem mais flexíveis e de fácil adaptação, tendem a arriscar mais e experimentar essas tecnologias antes. É extremamente importante que as empresas entendam do tema afim de perceberem de forma clara seus benefícios e consigam tomar suas decisões com maior segurança (GOMES, 2017).

6. CONSIDERAÇÕES FINAIS

Os serviços em nuvem são distribuições de recursos de armazenamento, bancos de dados, redes, software, análises pela Internet. A implementação de tal solução permite que as empresas tirem proveito de aplicativos e ferramentas relacionadas à produtividade, sem qualquer instalação e a necessidade de poder de computação. Tudo o que você precisa para usar o serviço é um dispositivo, fixo ou móvel, e um acesso à Internet.

Usar um serviço em nuvem significa aproveitar os recursos, poder computacional e aplicativos oferecidos pelo provedor. Com a disseminação cada vez mais massiva de dispositivos móveis e a necessidade de ter os dados da empresa à mão, oferece uma ampla gama de soluções que você pode adotar, este tipo de serviço não se distingue pelo tamanho ou tipo de empresa, pois pode ser adaptado a qualquer orçamento.

A computação em nuvem é um fator importante que impulsiona a Indústria 4.0 e a transformação digital. As tecnologias de nuvem atuais vão além do fornecimento de velocidade, escalabilidade, armazenamento e custo-benefício para fornecer a base para tecnologias de ponta, como Inteligência Artificial, aprendizado de máquina e Internet das Coisas, permitindo que as empresas inovem. Os dados subjacentes às tecnologias da Indústria 4.0 residem na nuvem, e os Sistemas Ciber-Físicos, os pilares da Indústria 4.0, se comunicam e coordenam por meio da nuvem.

As empresas precisam implementar soluções de última geração que garantam a capacidade de trabalhar em qualquer lugar, de forma contínua e segura. Os serviços em nuvem podem garantir tudo isso.

Referências

ADRIANO PEREIRA, EUGÊNIO DE OLIVEIRA, **Indústria 4.0: Conceitos E Perspectivas Para O Brasil,** Disponível em: file:///C:/Users/MAQUINA%2001/Downloads/4938-10951162-1-PB.pdf, Acessado em: 2018.

BRUNA THOMÉ, EDUARDO HENTGES, **Computação Em Nuvem: Análise Comparativa De Ferramentas Open Source Para Iaas,** Disponível em: http://hiperfcloud.setrem.com.br/wpcontent/uploads/2017/03/THOME_ERRC_2013.pdf Acessado em: 2013.

BUYYA ET AL, RAJKUMAR BUYYA, RAJIV RANJAN E RODRIGO N. CALHEIROS, **Modelagem e simulação de ambientes de computação em nuvem escaláveis e o kit de ferramentas CloudSim: desafios e oportunidades.** Disponível em: https://ieeexplore.ieee.org/abstract/document/5192685/ Acessado em: 2009.

CARLOS LEONARDO FREITAS VIVEIROS FRANCO, ALBERTO EDUARDO BESSER FREITAG, MARCELLE CANDIDO CORDEIRO E MARCELO JASMIM MEIRIÑO, **Vantagens Da Computação Em Nuvem Para Empresas De Menor Porte.** Disponível em: http://www.sadsj.org/index.php/revista/article/view/439 Acessado em: 2021.

CLEITON RODRIGUES, FRANZ BIONDI, MILENA MONTEAGUDO. **Estudos De Caso Da Indústria 4.0 Aplicados Em Uma Empresa Automobilística,** Disponível https://www.researchgate.net/profile/Cleiton-Mendes/publication/ em: Acessado em: 2017.

DIEGO RAFAEL GUEDES, CARLOS RODRIGO, **A Importância Da Tecnologia Sem Fio Na Indústria 4.0,** Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/487/314 Acessado em: 2018.

EA MOHAMED, AMR MOHAMED ALI, EL-ADL MOHAMED, SOUMAYA YACOUT E YASSER SHABAN, **Sistema De Diagnóstico De Falhas Não Supervisionadas Baseado Em Computação Em Nuvem No Contexto Da Indústria.** Disponível em: https://www.scielo.br/j/gp/a/k4cWwbpXG3gtph9BPNGCZfr/abstract/?lang=pt Acessado em: 2020.

FERNANDO MEIRELLES, **Computação Em Nuvem: Análise Bibliométrica Da Produção Científica Sobre Os Fatores Que Influenciam As Empresas No Seu Uso,** Disponível em: https://www.academia.edu/download/46097037/MEIRELLES_Computacao_em_nuvem_analise_bibliometrica_da_producao_cientifica.pdf Acessado em: 2015

FLÁVIO R. C. SOUSA, LEONARDO O. MOREIRA E JAVAM C. MACHADO, **Computação Em Nuvem: Conceitos, Tecnologias, Aplicações E Desafios.**Disponívelem:https://www.researchgate.net/profile/JavamMachado/publication/237644729_Computacao_em_Nuvem_Conceitos_Tecnologias_Aplicacoes_e_Desafios/links/56044f4308aea25fce3121f3/Computacao-em-Nuvem-Conceitos-Tecnologias-Aplicacoes-e-Desafios.pdf Acessado em: 2010.

GEISSBAUER R.; VEDSO, J.; SCHRAUF, S. **Indústria 4.0: Digitalização Como Vantagem Competitiva No Brasil. Pricewaterhousecoopers,** Disponível em: https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/pwc-industry-4-survey-16.pdf Acessado em: 2016

JULIO ALBA SOTO, OPENNEBULA**: Implantação De Uma Nuvem Privada E Orquestração Das Máquinas Virtuais No Paradigma Da Computação Em Nuvem,** Disponível: http://www.2015w.cgeti.ufc.br/monografias/JULIO_ALBA_SOTO.pdf Acessado em: 2011.

MARCOS AMPARO VINICIUS, RENATO SABINO GERIBELLO, SILAS BASTIANELLI PINTO, JESSICA SPOSITO PAULETTI INOUE E MAYARA DOS SANTOS AMARANTE, **Indústria 4.0: Impactos Da Tecnologia Da Informação Na Nova Indústria** Disponível em: https://revistas.brazcubas.br/index.php/pesquisa/article/view/651 Acessado em: 2021.

MYLENA LOPES DE SOUSA, MARCOS ANTÔNIO PEREIRA COELHO, LUCAS BORCARD CANCELA, LUCIANO DIAS DE SOUSA E ADRIANO SIMIONI ALVIM : **As Plataformas De Armazenamento Big Data E Computação Em Nuvem: Vantagens E Utilizações Práticas** Disponível em: http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/15045 Acessado em: 2018

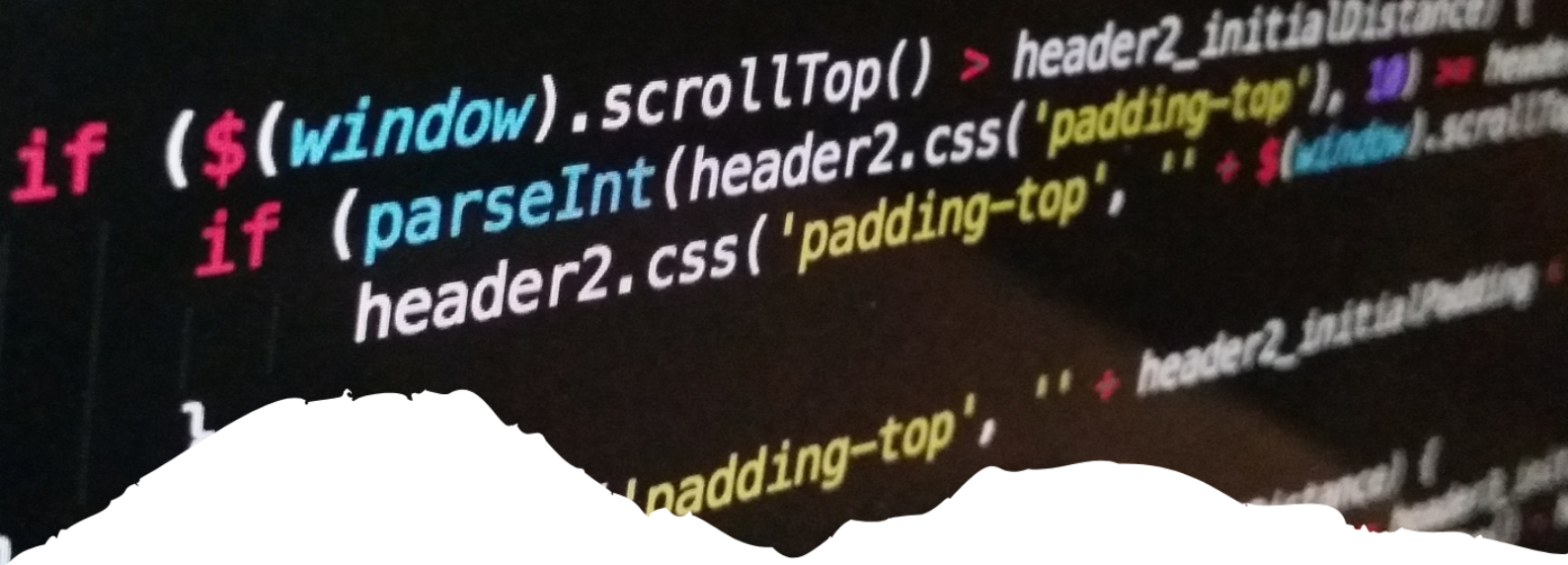
NEILSON CARLOS, **Um Estudo Sobre A Adoção Da Computação Em Nuvem No Brasil,** Disponível em: https://www.academia.edu/download/35753333/Dissertacao_Neilson_Ramalho.pdf, Acessado em: 2012.

PEDRO HENRIQUE CRUZ CAMINHA, **Implementação De Autenticação Federada Em Uma Nuvem Comunitária Geodistribuída,** Disponível em: https://www.gta.ufrj.br/ftp/gta/TechReports/Cruz16/Cruz16.pdf Acessado em: 2016.

RAPHAEL DE AQUINO GOMES, **Implantação Eficiente De Múltiplas Coreografias De Serviços Em Nuvens Híbridas,** Disponível em: https://repositorio.bc.ufg.br/tede/handle/tede/7351, Acesso em: 2017

VAQUERO, L. M.; CACERES, J.; LINDER, **M. A Break in the Cloud: Towars a Cloud Definition.** ACM SIGCOMM Computer Communication Reviwer, 39(1): 50-55, janeiro 2009.

VECCHIOLA ET AL, CHRISTIAN VECCHIOLA, SURAJ PANDEY E RAJKUMAR BUYYA, **Computação Em Nuvem De Alto Desempenho: Uma Visão Das Aplicações Científicas.** Disponível em: https://ieeexplore.ieee.org/abstract/document/5381983/ Acessado em: 2010.



25

O CRESCIMENTO E ENLACE DE EQUIPAMENTOS DE REDE SEM FIO

THE GROWTH AND LINKING OF WIRELESS NETWORK EQUIPMENT

Yasmim De Jesus Lopes Louzeiro

Resumo

As redes sem fio são atualmente ótimas opções para solucionar problemas ligados à conectividade, principalmente com relação à Internet. Frente ao exposto, o objetivo do presente material, consiste em consistir em descrever o funcionamento das redes sem fio com o aumento dos dispositivos móveis que utilizam a rede sem fio. De forma específica, pretende-se, conceituar a interferência de fontes terceiras; relatar a importância a redução da força do sinal; conhecer a propagação multivias e os erros de bits. Para tanto, realizou-se uma revisão bibliográfica, de natureza qualitativa, baseando-se nas principais bases de dados, utilizando-se descritores previamente delimitados, considerou-se o período de publicação dos últimos 20 anos. Com base nos estudos encontrados, compreendeu-se as redes sem fio possuem vantagens e desvantagens, no tocante a vantagens, tem-se a facilidade de instalação; mobilidade, e redução de custos, por outro lado, entende-se que existe a disponibilidade de Menor Banda de Transmissão, pois as redes sem fio em geral provêm enlaces com menor banda passante, ainda se enfatiza, as taxas de erros, pois as redes sem fio apresentam uma taxa de erro de bit (BER - Bit Error Rate) superior às redes com fio. No caso de um enlace de fibra óptica, o BER típico varia entre 10-8 e 10-9, em um enlace sem fio, essa taxa cai na faixa de 10-4 a 10-6.

Palavras-chave: Redes, Computadores, Conectividade, Dispositivos móveis.

Abstract

Wireless networks are currently great options to solve problems related to connectivity, especially with respect to the Internet. Given the above, the objective of this material is to describe how wireless networks work with the increase in mobile devices that use wireless networks. Specifically, it is intended to conceptualize the interference from third party sources; to report the importance of reducing the signal strength; to know about multivia propagation and bit errors. To this end, a bibliographic review was carried out, of a qualitative nature, based on the main databases, using previously delimited descriptors, considering the publication period of the last 20 years. Based on the studies found, it was understood that wireless networks have advantages and disadvantages, regarding the advantages, there are the ease of installation, mobility, and cost reduction, on the other hand, it is understood that there is the availability of lower bandwidth, because wireless networks in general provide links with lower bandwidth, it is also emphasized, the error rates, because wireless networks have a bit error rate (BER - Bit Error Rate) higher than wired networks. In the case of a fiber optic link, the typical BER ranges from 10-8 to 10-9, in a wireless link this rate falls in the range 10-4 to 10-6.

Keywords: Networks, Computers, Connectivity, Mobile Devices.

1. INTRODUÇÃO

Atualmente com o avanço tecnológico, cresceu a necessidade de possuir aparelhos sem fios, tendo em vista que o mais utilizado é o telefone celular. Em todo o mundo, 5,1 bilhões de pessoas usam algum tipo de telefone celular. Esse número equivale a 67% da população mundial. O uso de aparelhos sem fio para a internet ficou evidente, e os serviços móveis que elas disponibilizam vieram para marcar pra sempre na história da vida da humanidade, na atualidade é impossível viver em um ambiente que se precise estar em constante comunicação não possuir um dispositivo portátil para se comunicar.

Analisa-se que do ponto de vista de redes, que existem muitos desafios que podem surgir, em particular nas camadas de enlaces e a sua relação com as redes maiores nas quais se conectam. A natureza sem fio dos enlaces de comunicação nas redes e pela mobilidade que esses enlaces sem fio possuem merece uma importante compreensão.

Mediante o exposto, questiona-se: considerando o crescimento da utilização de aparelhos que utilizam a rede sem fio, como este crescimento vem impactando as redes sem fio e a utilização da mesma?

Considera-se comum o uso de aparelhos sem fio, dessa forma, o presente trabalho tem como intuito através das estratégias abordadas na literatura de capacitar e orientar analistas de redes.

O profissional de redes atua em vários campos de redes, através das suas competências aprimoradas durante sua graduação, com isso, o mesmo vem se destacando e é de fundamental importância e analisar redes, desse modo, possível uma rápida identificação do fato.

Durante o evento de enlace sem fio, um usuário se conecta a uma estação-base ou a um outro usuário sem fio por meio de um enlace de comunicação sem fio. Tecnologias de enlace sem fio diferentes têm taxas de transmissão diferentes e podem transmitir a distância deferentes. O analista de redes precisa deduzir e entender é redução da força do sinal, descobrir quais as interferências que podem ocorrer de outras fontes, entender o empaqueto da propagação multivias e a taxa de erros de bits.

Desse modo, considera-se que a temática desta pesquisa é relevante tanto do ponto de vista acadêmico, quanto social, pois irá auxiliar no adequado funcionamento das redes sem fio; é de suma importância em um mundo onde a comunicação a base de todo o contexto social e dentro desse contexto as redes sem fio são as mais utilizadas por sua mobilidade.

Para tanto, o objetivo geral do presente material, consiste em descrever o funcionamento das redes sem fio com o aumento dos dispositivos móveis que utilizam a rede sem fio. Para tanto, delimitou-se os seguintes objetivos específicos: Conceituar a interferência de fontes terceiras; relatar a importância a redução da força do sinal; conhecer a propagação multivias e os erros de bits.

2. DESENVOLVIMENTO

No mundo da telefonia pode-se dizer que os dez últimos anos foram a década da telefonia celular. Segundo a União Internacional das Telecomunicações, o Brasil era o sexto maior mercado do mundo em telefonia celular no ano de 2010, com 202,94 milhões de

aparelhos em uso. Em 2012, 247 milhões de linhas de telefones celulares ativas já existiam no Brasil, e em 2022, atingiu a marca de 256,4 milhões de linhas ativas (ROSSATO; SPANHOL; DE CAMARGO, 2020).

Atualmente, os usuários de redes sem fio exigem a mesma acessibilidade, segurança, qualidade de serviço e alta disponibilidade que os usuários da rede cabeada. O uso de redes sem fio tornou-se essencial tanto em ambientes domésticos como nos ambientes corporativos onde é preciso ter mobilidade e ao mesmo tempo acessibilidade de recursos da rede como informações de arquivos e e-mail, utilização de comunicações unificadas, acesso a sistemas de bancos de dados e aplicações. (KUROSE; ROSS, 2006).

De acordo com Medeiros et al., (2019), as redes sem fio são "soluções normalmente aplicadas, onde uma infraestrutura de cabeamento convencional não pode ser utilizada". As redes sem fio atendem com a mesma eficiência ou, até mesmo, com uma melhor relação custo/benefício em comparação à implementação de cabeamentos convencionais.

Nas redes sem fio (wireless networks) os pacotes são transmitidos, "através do ar", em canais de frequência de rádio (frequências na faixa de KHz até GHz) ou infravermelho (frequências da ordem de THz) (RUFINO, 2007).

Meios de transmissão diferem com relação à banda passante, potencial para conexão, a escolha do meio de transmissão adequada às aplicações é extremamente importante pelo fato de que ele influencia diretamente no custo das interfaces com a rede. Qualquer meio físico capaz de transportar informações eletromagnéticas é passível de ser usada em redes de computadores. Os mais comumente utilizados são o par traçado, cabo coaxial e a fibra ótica. Sob circunstâncias especiais, radiofusão, infravermelho, enlaces de satélite e micro-ondas também são escolhas possíveis (MENDES, 2020).

Compreende-se que desde o início da civilização, o homem sempre esteve em busca de comunicar-se de maneira rápida e eficiente, utilizando-se de inúmeros recursos e tecnologias. Na história da comunicação sem fio, o primeiro dado oficial data de 1895, quando um pesquisador italiano, Guglielmo Marconi, utilizando fundamentos de James Maxwell e de Heinrich Hertz, realizou a primeira transmissão sem fio da história com o envio de um sinal; assim, ele demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código morse (afinal de contas, os pontos e traços são binários). Os modelos sistemas digitais sem fios têm um desempenho melhor, mas a ideia básica é a mesma. Em uma primeira aproximação, redes sem fios podem ser divididas em três categorias principais: interconexão de sistemas, LANs sem fios e WANs sem fios (TANENBAUM, 2003).

A partir desse momento, as pesquisas e o desenvolvimento de equipamentos de tecnologia wireless não pararam de avançar; representando ganhos não apenas para o setor de telecomunicação, mas também contribuindo extensivamente nas aplicações em redes de computadores.

As redes sem fio precisam de equipamentos para realizar a distribuição das informações pela rede. Alguns equipamentos utilizados para criar uma rede sem fio são: antenas, cabos, conectores, pontos de acesso, *wireless bridge*, entre outros.

Os componentes utilizados em uma rede sem fio são basicamente os mesmos que os utilizados em uma rede cabeada, com a diferença física de não possuírem cabos e serem específicos para as redes sem fio. São eles: NIC (*Network Interface Card* - Cartão de Interface de Rede), Antenas, *APs* (Pontos de Acesso) e *Wireless Bridges*.

Assim como em redes cabeadas, as redes sem fio também são alvo de invasões e investidas de hackers. Por isso não se pode deixar de lado a questão da segurança das in-

formações em ambientes com tecnologia de redes sem fio. A segurança em redes sem fio está se tornando um assunto de extrema importância. O fato de não haver fios ou cabos ligando os computadores e o sinal de radiofrequência estar presente no ar, abre novas oportunidades para ações hostis de hackers.

De acordo com Neto; Morais e Oliveira (2019), alguns mecanismos podem ajudar a proteger uma rede sem fio, geralmente os próprios equipamentos oferecem essa alternativa de segurança. Os meios mais conhecidos de se proteger uma rede sem fio são: endereço MAC, protocolo WEP, protocolo WPA e o RADIUS (Remote Access Dial-In User Service).

Ainda se enfatiza nesse ínterim, a questão dos erros. Em uma transmissão de dados, não basta enviar os dados para a outra ponta. É preciso verificar a sua integridade na recepção, se não ocorreram erros devido às interferências que podem surgir no meio de transmissão (SOUSA, 2009).

Devido à ocorrência de erros no meio de transmissão, foi preciso desenvolver um sistema que garantisse a integridade dos dados para o receptor, ou seja, que os dados recebidos fossem exatamente iguais aos transmitidos. A forma encontrada foi utilizar algoritmos que leem os dados a serem transmitidos e fazem um cálculo que gera um resultado colocado no final do bloco de dados transmitido. Ao receber o bloco de dados, o receptor recalcula com o recebido. Se o resultado for o mesmo, indica que não ocorreram alterações ao longo da transmissão. Caso isso não ocorra e haja divergência no resultado, é devido a alterações ao longo da transmissão, e o receptor solicita uma retransmissão do bloco (SOUSA, 2009).

A supervisão de erros no enlace é baseada em cálculos pré-determinados, usando os conteúdos dos campos de endereço, comando e dados e as informações referentes à esta supervisão são enviadas neste campo. Uma comparação destes campos enviados e recebidos permite a constatação de quadros transmitidos com ou sem erros (BREITENBACH; POSSAMAI, 2020).

É um campo composto de 2 octetos, com o objetivo de possibilitar a detecção de erros que o meio físico possa introduzir na transmissão dos quadros. Utiliza-se um algoritmo matemático para detecção de erros.

A camada de enlace de dados está localizada entre a camada de rede e a camada física no modelo da Internet. Ela recebe os serviços da camada física e provê serviços para a camada de rede (FOROUZAN, 2006).

A camada de enlace de dados é responsável por transportar pacotes de um nó (computador ou roteador) a outro através da rede. Diferentemente da camada de rede que desempenha um papel global na arquitetura, a camada de enlace tem um nível de responsabilidade apenas local. Todos os processos envolvendo dois nós é de responsabilidade da camada de enlace. Noutras palavras, visto que LANs e WANs são delimitadas por nós de rede, podemos dizer que a responsabilidade da camada de enlace é encaminhar pacotes através de uma LAN ou WAN (FOROUZAN, 2006).

A integridade dos pacotes deve ser preservada durante a viagem através de uma LAN ou WAN (entre dois nós). A camada de enlace deve prover mecanismos que assegurem integridade aos pacotes das camadas superiores do modelo. Se um pacote for corrompido durante uma transmissão, a camada de enlace deve ser capaz de corrigi-lo ou pedir retransmissão desse pacote. A camada de enlace deve também assegurar que o próximo nó da rede não está sendo inundado com os dados provenientes do nó anterior, isto é, essa camada tem que prover controle do fluxo de dados (FOROUZAN, 2006).

Independentemente do contexto, uma comunicação bem-sucedida só pode acontecer se todas as partes interessadas estiverem falando a mesma língua. No mundo das redes, essa língua é chamada de *especificação*, e se for objeto de um acordo por um número suficiente de partes interessadas ou se receber um selo de aprovação por um órgão da indústria, essa especificação poderia subir de status e tornar-se um *padrão* (ENGST; FLEISHMAN, 2005).

De qualquer maneira, isso é teoria, mas toda indústria tem um grande número desses chamados padrões que falham ao funcionar conjuntamente e são um fator de concorrência entre os fabricantes. Mas, o mundo das redes sem fio evoluiu, de maneira notável, saindo quase completamente desse lamaçal de padrões concorrentes. Quando falamos de redes sem fio, estamos nos referindo a uma família de padrões que funcionam conjuntamente: equipamentos que suportam um dos padrões sempre são compatíveis com outros dispositivos que suportam o mesmo padrão. Melhor ainda, a retrocompatibilidade tem sido a regra a não a exceção (ENGST; FLEISHMAN, 2005).

Existe um conjunto de tecnologia de LAN sem fio que usam uma modificada de CSMA/CD. Os produtos, que são fabricados por várias empresas, então disponíveis sob uma variedade de nomes comerciais. Por exemplo, a Apple Computer Corporation vende um dispositivo de *Aiport*; a Lucent Corporation vende WaveLan; a Solectek vende AirLAN; e a Proxim Corporation vende RangeLAN. Dispositivos mais antigos usam frequências de 900MHz para permitir que os dados sejam enviados a 2Mbps; o padrão 802.11b da IEEE, também conhecido como Wi-Fi, define LANs sem fio que operam a 11Mbps usando uma frequência com alcance de 2,4GHz. Um padrão conhecido como *bluetooth* especifica uma tecnologia de LAN sem fio designada para curtas distâncias (COMER, 2007).

Em vez de transmitir sinais através de um cabo, o hardware de LAN sem fio usa antenas para transmitir sinais de RF através do ar, que outros computadores recebem.

Segundo Barros (2020), a função das antenas é realizar a transição de meios confinados, tais como cabo coaxial ou guia de onda, para o espaço e vice-versa. Trata-se de um dos equipamentos mais decisivos para um desempenho satisfatório em redes *Wi-Fi*. Ao contrário do que muitas pessoas acreditam as antenas não amplificam os sinais, elas apenas convergem (direcionam) a energia. Segundo o autor supracitado: “As antenas trabalham igualmente para transmitir ou receber os sinais (reciprocidade). Por exemplo, ao medir os padrões de radiação de uma antena em uma determinada faixa de teste, a antena pode transmitir ou receber as ondas de rádio” (BARROS, 2020, p. 13).

Como outras tecnologias de LAN, as LANs sem fio usam compartilhamento. Isto é, todos os computadores que participam em uma determinada LAN sem fio são configurados para usar uma mesma frequência de rádio. Deste modo, eles devem se alternar no envio de pacotes.

A Internet não impõe especificações para LANs e WANs. Ao contrário, ela aceita qualquer padrão de rede local (LAN) como rota de comunicação dos pacotes provenientes da camada de rede. O fato básico é que coexistem muitos protocolos de controle das LANs. Em 1985, a Computer Society do IEEE iniciou um projeto, denominado Projeto 802 (802 *Project*), para estabelecer padrões e permitir a interconectividade entre equipamentos de diversos fabricantes (FOROUZAN, 2006).

2.1 Metodologia

Os procedimentos da pesquisa são de caráter bibliográficos, trata-se portando de

uma Revisão de Literatura, de natureza qualitativa, no qual, realizou-se uma consulta a livros, dissertações e por artigos científicos, para tanto, utilizou-se as seguintes bases de dados: “biblioteca Faculdade Pitágoras”; “Biblioteca digital brasileira de teses e dissertações do Instituto Brasileiro de Informação em Ciência e Tecnologia – IBICT” e “Scielo”. Considerou-se o período de publicação dos últimos 20 anos. As palavras-chave utilizadas na busca forma: “Redes de Computadores”, “Tecnologias de Rede”, “Comunicação de dados” e “Comunicação entre Computadores”.

2.2 Resultados e Discussão

Compreende-se que no início das redes locais, não existiam padrão. Prevaleciam o caos e a instabilidade. Os padrões proprietários de fornecedores eram a regra, os clientes se tronavam clientes para toda a vida a as empresas inchavam. Os padrões específicos de cada empresa impediam que os clientes usassem produtos “de fora” por medo de incompatibilidade. Em fevereiro de 1980, o IEEE assumiu a responsabilidade de estabelecer padrões para redes locais, inicialmente para as camadas físicas e de enlace de dados, usando o modelo de referências OSI como base. O IEEE (*Institute of Electrical and Electronics Engineers*) é uma sociedade profissional fundada em 1963. Os membros do IEEE são engenheiros, cientistas e estudantes. Dentre suas atividades consta coordenar padrões para computadores e comunicações. Muitos padrões internacionais da ISSO (*International Organization for Standardization*) e da IEC (*International Electrotechnical Commission*) são baseados em padrão de rede do IEEE (GALLO; HANCOCK, 2003).

O IEEE desenvolveu seus padrões para redes locais sob os auspícios da IEEE Computer Society. Como o projeto do IEEE para desenvolver padrões de redes locais recebeu o número 802, referenciando o mês de fevereiro de 1980, o trabalho desse comitê ficou coletivamente como Projeto 802. Por isso, os padrões resultantes desse projeto são denominados IEEE 802.*x* (GALLO; HANCOCK, 2003).

O IEEE iniciou o desenvolvimento de seus padrões para redes locais com um modelo de arquitetura, definido no IEEE 802.1. Esse modelo de arquitetura corresponde às duas camadas mais baixas do modelo OSI. A diferença entre os modelos IEEE e OSI é que o IEEE divide a camada de enlace de dados OSI em duas partes: a *subcamada de controle lógico de ligações* (LLC – *logical link control*) e a *subcamada de controle de acesso a meios* (MAC – *media access control*). Vale observar que MAC não tem nada a ver com os computadores Macintosh. A subcamada LLC, definida no IEEE 802.2, é a camada superior da camada de enlace de dados. Ela engloba diversas funções, incluindo enquadramento, controle de fluxo e controle de erros. A subcamada MAC é a metade mais baixa da camada de enlace de dados. Ela fornece protocolos de gerenciamento de acesso a meios para acessar meios compartilhados (GALLO; HANCOCK, 2003).

Em vez de transmitir sinais através de um cabo, o *hardware* de LAN sem fio usa antenas para transmitir sinais de RF através do ar, que outros computadores recebem. Como outras tecnologias de LAN, as LANs sem fio usam compartilhamentos. Isto é, todos os computadores que participam em uma determinada LAN sem fio são configurados para usar uma mesma frequência de rádio. Deste modo, eles devem se alternar no envio de pacotes (COMER, 2007).

Uma diferença entre o modo como LANs com e sem fio administram compartilhamento surge por causa da forma com que as transmissões sem fio se propagam. Embora a energia eletromagnética se irradie em todas as direções, os transmissores de LAN sem fio usam poucas energias, o que significa que uma transmissão tem energia suficiente

somente para viajar uma distância pequena. Além disso, obstruções metálicas podem bloquear o sinal. Assim, as unidades sem fio localizadas em pontos bem distantes ou atrás de obstruções não receberão as transmissões do outro (COMER, 2007).

Enlaces sem fio: um hospedeiro se conecta a uma estação-base ou a um outro hospedeiro sem fio por meio de um enlace de comunicação sem fio**.** Tecnologias de enlace sem fio diferente têm taxas de transmissão diferentes e podem transmitir a distâncias diferentes (COMER, 2007);

Pontua-se que os enlaces em redes sem fio podem ser realizados em duas topologias distintas, ponto-a-ponto ou ponto-multiponto. Estas duas topologias têm uma imposição: em ambos os casos se faz necessário a visada direta entre as antenas, ou seja, duas antenas devem se "enxergar" sem nenhum obstáculo interposto entre elas, tais como árvores, paredes ou montanhas (KUROSE; ROSS, 2013).

Conclui-se que, considerando uma rede simples cabeada, por exemplo, uma rede residência com hospedeiros interconectados por um computador Ethernet cabeado. Se substituíssemos a Ethernet cabeada por uma rede 802.11 sem fio, uma placa NIC sem fio substituiria as placas da Ethernet cabeada nos hospedeiros e um ponto de acesso substituiria o comutador Ethernet, mas, na camada de rede ou acima dela, praticamente nenhuma mudança seria necessária. Isso sugere que concentremos nossa atenção na camada de enlace ao procurarmos diferenças importantes entre redes com fio e sem fio. Realmente, podemos encontrar várias diferenças importantes entre um enlace com fio e um enlace sem fio: (KUROSE; ROSS, 2013).

Redução da força do sinal. Radiações eletromagnéticas são atenuadas quando atravessam algum tipo de matéria (por exemplo, um sinal de rádios ao atravessar uma parede). O sinal se dispersará mesmo ao ar livre, resultando na redução de sua força (às vezes denominada atenuação de percurso) à medida que aumenta a distância entre emissor e receptor.

Interferência de outras fontes. Várias fontes de rádio transmitindo na mesma banda de frequência sofrerão interferência umas das outras. Por exemplo, telefones sem fio de 2,4 GHz e LANs sem fio802.11b transmitem na mesma banda de frequência. Assim, o usuário de uma LAN sem fio 802.11b que estiver se comunicando por telefone sem fio de 2,4 GHz pode esperar que nem a rede nem p telefone funcionem particularmente bem. Além da interferência de fontes transmissoras, o ruído eletromagnético presente no ambiente (por exemplo, um motor ou um equipamento de microondas próximo) pode resultar em interferência.

Propagação multivias. Propagação multivias (ou multicaminhos) ocorre quando porções da onda eletromagnética se refletem em objetos e no solo e tomam caminhos de comprimento diferentes entre um emissor e um receptor. Isso resulta no embaralhamento do sinal recebido no destinatário. Objetos que se movimentam entre o emissor e o receptor podem fazer com que a propagação multivias mude ao longo do tempo.

A discussão anterior sugere que erros de bits serão mais comuns em enlaces sem fio do que em enlaces com fio. Por essa razão, talvez não seja nenhuma surpresa que protocolos de enlace sem fio empreguem não somente poderosos códigos de detecção de erros por CRC, mas também protocolos ARQ de nível de enlace que retransmitem quadros corrompidos (KUROSE; ROSS, 2013).

Taxas de erros de bits mais altas e que variam ao longo do tempo não são as únicas diferenças entre um enlace com fio e um sem fio. Lembre-se de que, no caso de enlaces *broadcast* cabeados, todos os nós recebem as transmissões de todos os outros nós. No

caso de enlace sem fio, a situação não é tão simples (KUROSE; ROSS, 2013).

Sempre que se estabelece um fluxo de dados de um ponto a outro, tal fluxo está sujeito a sofrer modificações imprevisíveis provocadas pela interferência. A interferência pode modificar a forma do sinal original. Em um erro simples, ou seja, aquele onde apenas um *bit* é modificado por vez, ocorre a troca de 0 por um 1 ou vice-versa. Por exemplo, durante uma transmissão de dados, um ruído em rajada impulsiva num intervalo de tempo de 0,01s pode modificar todos os 12 *bits* de informações de uma transmissão a 1200 bps. A expressão "erros isolados" é aplicada sempre que apenas um *bit* da unidade de informação (tal como *byte*, caractere, sequência de dados ou pacote) é modificado.

Os erros isolados são muito frequentes numa transmissão serial de dados. Para compreender porque, imagina-se que a fonte envie dados a uma taxa de 1 Mbps. Isto significa que o tempo de duração de cada *bit* é 1/1.000.000 = 1 µs. Para que um único *bit* seja corrompido, um ruído deve se manifestar em apenas 1 µs, o que é muito raro, pois ruído se manifestam normalmente durante um intervalo de tempo muito maior (CORREIA, 2007).

Contudo, a transmissão serial não é a única fonte de incidência dos erros isolados. Numa comunicação paralela, um único *bit* da sequência de dados também pode ser modificado. Por exemplo, imagina-se uma linha paralela para transmissão de dados a 8 fios sendo utilizada para enviar 8 *bits* ao mesmo tempo e que um dos fios está sujeito a uma interferência maior. Nesse caso, é possível que 1 *bit* seja corrompido em cada *byte* transmitido. Imagine-se ainda, que essa transmissão paralela ocorre dentro de um computador, entre CPU e memória, e que estejamos transmitindo 8 Mbytes de dados. Percebe-se como isso pode ser grave. O termo rajada de erros (*burst error*) deve ser utilizado sempre que 2 ou mais *bits* da sequência de dados forem corrompidos (FOROUZAN, 2006).

As rajadas de erros são mais frequentes numa transmissão serial. Normalmente, o tempo de duração de um ruído é muito maior que o tempo de um *bit*. Sendo assim, quando um ruído afetar uma certa sequência de dados, um conjunto de *bits* da sequência podem ser corrompidos ao mesmo tempo. A quantidade de *bits* afetados na sequência depende da taxa de transmissão de dados e do intervalo de duração do ruído. Por exemplo, se estivermos transmitindo dados a 1 Kbps, um ruído de 1/100s pode afetar 10 *bits* ao mesmo tempo. Se estivermos transmitindo a 1 Mbps, o mesmo ruído pode afetar 10.000 *bits* (CORREIA, 2007).

Embora o objetivo da verificação de erros leve à correção dos mesmos, na maioria das vezes, primeiramente devemos detectá-los. É muito mais simples detectar um erro do que corrigi-lo, mas é o primeiro passo no processo de correção de erros (FOROUZAN, 2006).

Um mecanismo eficiente de detecção de erros seria enviar os dados duplicados. O dispositivo receptor seria então capaz de comparar *bit* a *bit* entre as duas versões de dados enviados e apontar possível erros. Quaisquer discrepâncias indicariam a ocorrência de erros. Este sistema seria totalmente preciso (a probabilidade de ocorrência de erros exatamente nos mesmos *bits* de ambos os conjuntos de dados é infinitesimalmente pequena), mas também seria insuportavelmente lento. Não somente o tempo de transmissão seria duplicado, mas também os esforços para comparar *bit* a *bit* as duas unidades de dados (FOROUZAN, 2006).

A ideia de incluir informação extra numa transmissão para facilitar a detecção de erros foi uma excelente solução para o problema. Entretanto, em vez de repetir todo o fluxo de dados, foi adotado a inclusão de uma certa quantidade de *bits* adicionais no final de cada sequência de dados. Esta técnica é denominada redundância porque os *bits* extra são informação redundantes, isto é, eles são descartados tão logo a verificação da transmissão tenha sido realizada. As detecções de erros utilizam o conceito de redundância,

que é a técnica de adicionais *bits* extras no final da unidade de informação para facilitar a detecção de erros no destino (FOROUZAN, 2006).

3. CONCLUSÃO

Compreendeu-se por meio da presente pesquisa, que as redes sem fio vêm se mostrando ótimas soluções de conectividade em localidades carentes de infraestrutura física de cabeamentos. Além de não ser necessária a utilização de cabos ou fios, a tecnologia proporciona mobilidade dentro de ambientes corporativos com o objetivo de obter maiores rendimentos na produtividade.

Por meio do aporte teórico, observou-se que as redes sem fio possuem vantagens e desvantagens, no tocante a vantagens, tem-se a facilidade de instalação; mobilidade, e redução de custos, por outro entende-se que existe a disponibilidade de Menor Banda de Transmissão, pois as redes sem fio em geral provêm enlaces com menor banda passante, ainda se enfatiza, as taxas de erros, pois as redes sem fio apresentam uma taxa de erro de bit (BER - Bit Error Rate) superior às redes com fio. No caso de um enlace de fibra óptica, o BER típico varia entre 10-8 e 10-9, em um enlace sem fio, essa taxa cai na faixa de 10-4 a 10-6.

A partir desses dados pode-se concluir que, existem razões para usar redes sem fio, elas são versáteis em muitas situações, desde aproveite-se seus métodos e ações para garantir a privacidade e a qualidade das informações transmitidas. Sugere-se para trabalhos futuros experimentos práticos em redes sem fio, para melhor compreender sua funcionalidade, bem como, os pós e contras.

Referências

BARROS, Tales. **Antenas de Microfita Fractais Quadrangulares para Aplicação em Comunicações Sem Fio**. 2020. Dissertação de Mestrado.

BREITENBACH, Alter; POSSAMAI, Vinicius. O Método Brute Force Para Invasão De Redes Sem Fio. **SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO**, v. 2, n. 1, 2020.

COMER, Douglas E. Comer. **Redes de computadores e internet**. 4 ed. Porto Alegre: Bookman, 2007.

CORREIA, Luiz Henrique Andrade. Tópicos em Tecnologias de Comunicação Sem Fio. Curso de Pós-Graduação “Lato Sensu” (especialização) a distância: **Tecnologia de Redes de Computadores.** Editora UFLA/FAEPE, 2007

ENGST, Adam Engst; FLEISHMAN, Glenn Fleishman. **Kit do iniciante em redes sem fio:** o guia prático sobre redes Wi-Fi para Windows e Macintosh. 2 ed. São Paulo: Pearson Makron Books, 2005.

FOROUZAN, Behrouz A. Forouzan. **Comunicação de dados e redes de computadores**. 3 ed. Porto Alegre: Bookman, 2006.

GALLO, Michael A. Gallo; HANCOCK, William M. Hancock. **Comunicação entre computadores e tecnologias de rede**. São Paulo: Pioneira Thomson Learning, 2003.

KUROSE, James F. Kurose; ROSS, Keith W. Ross. **Redes de Computadores e a Internet:** Uma abordagem top-down. 3 ed. São Paulo: Pearson Addison Wesley, 2006.

KUROSE, James F. Kurose; ROSS, Keith W. Ross. **Redes de Computadores e a Internet:** Uma abordagem top-down. 6 ed. São Paulo: Pearson Education do Brasil, 2013.

MEDEIROS, Dianne SV et al. Análise de dados em redes sem fio de grande porte: Processamento em fluxo em tempo real, tendências e desafios. **Sociedade Brasileira de Computação**, 2019.

MENDES, Douglas Rocha. **Redes de computadores: teoria e prática**. Novatec Editora, 2020.

NETO, Celso Cardoso; MORAES, Jorge Luiz Abreu; OLIVEIRA, Cleber Romulo de. NOVAS TECNOLOGIAS REDES SEM FIOS WIRELESS. **REVISTA DE TRABALHOS ACADÊMICOS-CAMPUS NITERÓI**, v. 1, n. 18, 2019.

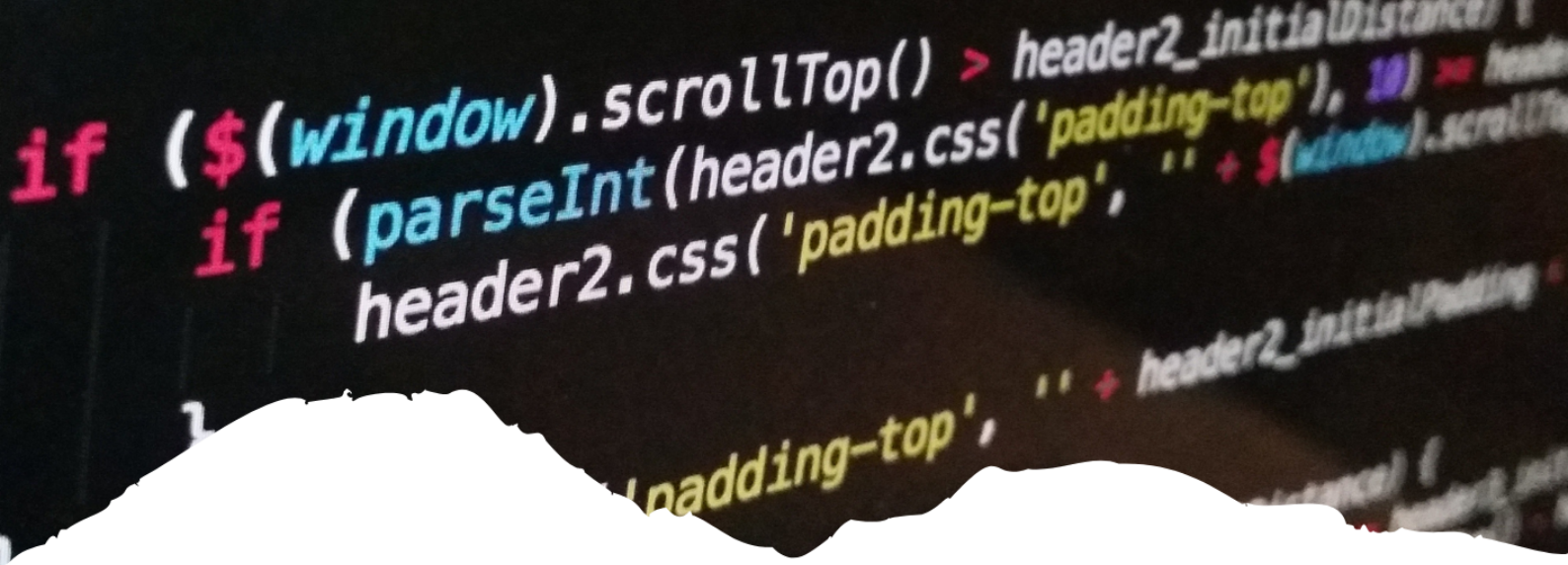
ROSSATO, Jonas; SPANHOL, Fabio Alexandre; DE CAMARGO, Edson Tavares. Implantaçao e avaliaçao de uma rede sem-fio de longo alcance e baixa potência para cidades inteligentes. In: **Anais do IV Workshop de Computaçao Urbana**. SBC, 2020. p. 192-205.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes wi-fi e bluetooth. Novatec Editora, 2019.

RUFINO, Nelson Murilo de Oliveira Rufino. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 2 ed. São Paulo: Novatec Editora, 2007.

SOUSA, Lindeberg Barros de Sousa. **Redes de Computadores:** guia total. 2 ed. São Paulo: Érica, 2009.

TANENBAUM, Andrew S. Tanenbaum. **Redes de Computadores**. 4 ed. Rio de Janeiro: Elsevier, 2003.



26

ANÁLISE DA TECNOLOGIA DA INFORMAÇÃO APLICADA AO E-COMMERCE: RELEVÂNCIA DA TI PARA O COMÉRCIO VIRTUAL

ANALYSIS OF INFORMATION TECHNOLOGY APPLIED TO E-COMMERCE: RELEVANCE OF IT FOR VIRTUAL COMMERCE

Luís Gustavo Dias Ramos

Resumo

O presente estudo aborda a análise da tecnologia da informação (TI) aplicada ao comércio eletrônico (E-commerce), bem como sua relevância para o sucesso das vendas online. A pesquisa apresenta uma revisão bibliográfica sobre o tema, sendo destacado os principais softwares para criação, manutenção e segurança dos sites de vendas. O objetivo principal foi identificar o funcionamento da TI no E-commerce. Tendo como questão norteadora os impactos da indisponibilidade da TI para o desenvolvimento do E-commerce. A pesquisa apresenta conceitos, origens do TI, além da representação de dados em forma de gráficos que podem ser utilizados como base para aprimoramento da experiência do consumidor, aumentando a eficiência operacional e, consequentemente impulsionando as vendas no ambiente virtual. Os resultados demonstram a importância da adoção de mecanismos de segurança e de gerenciamento de software para a garantia e otimização dos serviços de TI, para que sejam oferecidos serviços e programas de atendimento ao consumidor com o mínimo de impactos negativos para o desenvolvimento do e-commerce.

Palavras-chave: Tecnologia da Informação, E-commerce, Software.

Abstract

This study addresses the analysis of information technology (IT) applied to electronic commerce (E-commerce), as well as its relevance to the success of online sales. The research presents a bibliographic review on the subject, highlighting the main software for creation, maintenance and security of sales sites. The main objective was to identify the functioning of IT in E-commerce. Having as a guiding question the impacts of IT unavailability for the development of E-commerce. The research presents concepts, IT origins, in addition to the representation of data in the form of graphics that can be used as a basis for improving the consumer experience, increasing operational efficiency and, consequently, boosting sales in the virtual environment. The results demonstrate the importance of adopting security mechanisms and software management for the guarantee and optimization of IT services, so that services and customer service programs are offered with the minimum of negative impacts for the development of e-commerce.

Key-words: Information Technology, E-commerce, Software.

1. INTRODUÇÃO

O mercado atual, passou ao longo do tempo por várias transformações, e seguindo o gancho dos avanços tecnológicos percebe-se que o comércio tradicional evoluiu. Um exemplo claro é comércio eletrônico ou E-commerce termo mais utilizado atualmente que consiste principalmente na venda de produtos e serviços através de sites e inúmeros aplicativos que visam facilitar o cotidiano do consumidor. Ao analisar tal tendência a pesquisa visou analisar a Tecnologia da Informação (TI) tendo por base sua importância para empresas, bem como profissionais autônomos que trabalham com transações realizadas por meios digitais, principalmente na criação e desenvolvimento de sites e aplicativos para o comércio eletrônico. Compreendeu-se com a pesquisa que os negócios estão tornando-se cada vez mais dependentes da Gestão de TI, pois nos últimos anos, são notáveis os crescimentos e a relevância que a Tecnologia da Informação (TI) tem realizado no mercado digital. Com a transformação do E-commerce, hoje em dia, fazer compras nunca foi tão fácil, é só visitar qualquer site ou aplicativo, mediante a uma simples pesquisa no motor de busca da internet e tudo de forma prática, rápida e segura.

Contudo alguns detalhes tornam-se primordiais para o bom desempenho dos negócios no mercado digital, como por exemplo, a criação e desenvolvimento de sites que instiguem ao consumidor a realizar compras seguras e com maior facilidade, além de um software completo com informação sobre os perfis dos diversos usuários que utilizam tal plataforma de compra. Nesse sentido, a Tecnologia da Informação como atividade que abrange todas as atividades desenvolvidas na sociedade pelos recursos da informática tem papel fundamental no uso de ferramentas de vendas como o E-commerce.

A pesquisa teve como objetivo geral a identificação do funcionamento da TI no E-commerce. Pontua-se ainda os objetivos específicos como: Análise da ascensão do mercado eletrônico no Brasil; Ilustração do passo a passo para desenvolvimento de sites e aplicativos para o E-commerce; Exposição de mecanismos de gerenciamento de software para segurança e Serviços de TI; e apresentação dados sobre os principais meios e plataformas de criação de sites utilizadas atualmente.

O problema norteador problema norteador baseou-se no seguinte questionamento: Quais os impactos da indisponibilidade dos Serviços de TI para o desenvolvimento do E-commerce na atualidade?

A metodologia utilizada foi o levantamento bibliográfico com análise de livros, revistas, artigos científicos específicos sobre o tema. A partir da pesquisa foi possível perceber um crescimento dos consumidores online em 87%, sendo que 75% utilizam as redes sociais para buscas e 74% costumam utilizar o Instagram, o Facebook e outras redes sociais para realizarem suas compras.

2. CONCEITO DE TECNOLOGIA DA INFORMAÇÃO – TI

Historicamente, o conhecimento era um privilégio das classes que estavam no poder e daqueles ligados ao alto escalão religioso. O acesso aos livros, e consequente ao conhecimento, tão importante para o sucesso e manutenção de um negócio lucrativo era garantido somente as pessoas alfabetizadas. Nunes e Santana (2018, p. 10) ressaltam que: Embora o conhecimento sempre tenha se mostrado necessário para construção de ferramentas, elaboração de produtos, e solução de problemas, com o advento da ciência e da tecnologia

(principalmente no século XX), a sua importância tornou-se uma ferramenta significativa. Com a evolução das telecomunicações a era computacional passou a ser uma tendência e uma ferramenta imprescindível para o mercado, automatizando determinadas tarefas em grandes empresas e meios governamentais. De acordo com Olifer (2008, p. 4) "[...] as redes de computadores trouxeram algo de novo para o mundo das comunicações, isto é, o armazenamento praticamente inexaurível de informações acumuladas pela civilização humana durante os vários milhares de anos de existência".

A partir do aprimoramento das grandes máquinas foi possível o advento da informação, ou seja, os computadores tornaram-se capazes de trocar dados de forma automática. Com a facilidade de obtermos e disponibilizar informações através destes dispositivos, temos a Tecnologia da Informação, chamada inicialmente por: computadores, sistemas de tratamento da informação, máquina de processamento de dados e, até mesmo, de cérebro eletrônico.

Assim, destaca-se como uma melhor definição sobre o conceito Tecnologia da Informação a trazida por Lemos II (2011, p. 51) que ressalta a mesma "como um conjunto de todas as atividades e soluções providas por recursos de computação".

> O termo TI é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como, o modo de como esses recursos estão organizados num sistema capaz de executar um conjunto de tarefas. A tecnologia da informação abrange todas as atividades desenvolvidas na sociedade pelos recursos da informática (LEMOS II, 2011, p. 52).

Entende-se, que a Tecnologia da Informação possui larga escala de transmissão, contribuindo de forma satisfatória para prestação de serviços tecnológicos. Seus principais recursos podem ser agrupados em três grandes esferas, sendo eles: recursos de Hardware; recursos de Software; recursos de Rede que serão analisados ao longo desta pesquisa.

2.1 E-commerce: origem no Brasil

A partir da evolução da tecnologia foram atribuídas ao nosso cotidiano, inúmeras vantagens com relação ao tempo, distância e rapidez em diversas transações. Com a internet, foi possível ainda a ascensão de pequenos empreendedores ganharem espaço no mercado através de vendas online. Dessa forma, nasceu o e-commerce. No Brasil o comércio eletrônico surgiu na década de 1990, com a venda de livros pela Internet.

Comércio eletrônico, ou e-commerce, ou ainda comércio virtual (ou comércio online), é um tipo de transação comercial feita especialmente através de um equipamento eletrônico, como um computador. Mas, atualmente, outros equipamentos conectados à internet também são usados para isso, como smartphones, tablets e outras mídias (CLARO, 2013, p. 14).

O Sebrae (2016) ressalta que o E-commerce ou comércio eletrônico como sendo parte integrante do e-business. Descrevendo aquele como atividade mercantil que, fará a conexão eletrônica entre a empresa e o cliente como estratégia de venda de produtos ou serviços. Já o e-business como uma estratégia de introdução da empresa na internet, melhorando as atividades de comunicações internas e externas, transmissão de dados, controles internos, treinamento de pessoal, entre outras possibilidades.

Segundo Lima e Viera (2021) em seu artigo intitulado, E-COMMERCE: A importância

de uma boa experiência online, “Nos dias de hoje, o uso da tecnologia é algo imprescindível, e com a chegada da indústria 4.0 toda essa tecnologia recebeu um grande impulso, e as ferramentas tecnológicas alavancaram o e-commerce por completo”.

2.2 Tecnologia da informação aplicada ao e-commerce

A Tecnologia da Informação revolucionou o mundo dos negócios nos últimos anos. O mundo tornou-se digital e o comércio tradicional com suas lojas físicas abriram espaço para o mercado digital. É possível perceber o aumento considerável no uso de plataformas digitais para vendas. Sabe-se que por alguns anos, alguns negócios conseguiram manter seus serviços com o mínimo ou sem nenhum apoio da Tecnologia da Informação (TI), porém atualmente, a TI tornou-se um aliado e um diferencial no mercado competitivo.

Nesse sentido, a TI hoje, para algumas empresas tornou-se um parceiro estratégico. Com TI aplicado ao mercado eletrônico vislumbra-se a possibilidade de economia de investimentos, já que não há necessidade de gastos com lojas físicas. Nunes e Santana (2018) entendem que a TI permite, através de software seja possível prever o comportamento do mercado e assim conhecer o melhor momento para realização de compras ou vendas de produtos.

Hoje, em todo o mundo, as empresas buscam continuamente novas formas de aperfeiçoar a produção, comercialização e distribuição de seus bens e serviços, de forma a garantir ganhos de produtividade e redução de custos para competir no mercado globalizado. Elas sabem que isso representa a sua sobrevivência (CLARO, 2013, p. 28).

Observa-se que o gerenciamento do TI aplicado ao e-commerce traz como benefício um amplo conhecimento sobre o consumidor, a partir de pesquisa sobre os compradores, identificação de suas necessidades, gostos, comportamentos de compra, dados socioeconômicos, perfis, entre outros, que contribuem para criação de estratégias de vendas.

De acordo com Akkari (2018, p. 7) “o objetivo central do gerenciamento de TI é gerar valor por meio do uso de tecnologia e para atingir tal objetivo, as estratégias e tecnologias de negócios devem estar alinhadas”. Com isso, é de extrema importância o alinhamento dos serviços de TI com as necessidades atuais e futuras dos negócios.

2.3 Gerenciamento de Software para criação e manutenção de sites de venda eletrônica

Os conteúdos de softwares estão cada vez mais sofisticados, constantemente, desenvolvedores criam novas ferramentas para facilitar o processo de construção dos projetos com diversas finalidades. Como exemplo, os Frameworks[1] e plataformas tem como objetivo simplificar e facilitar o desenvolvimento de diversas aplicações entregando ao usuário uma série de elementos e bibliotecas que visam permitir a codificação da linguagem mais fácil e compatível com seus padrões e particularidades, e assim conseguindo reduzir o tempo gasto. De acordo com Sommerville (2011, p.368): O desenvolvimento de software usando serviços baseia-se na ideia de compor e configurar serviços para criar novos serviços compostos. Estes podem ser integrados com uma interface de usuário implementada em um browser para criar uma aplicação Web ou podem ser usados como componentes

1 É um termo inglês que, em sua tradução direta, significa estrutura. De maneira geral, essa estrutura é feita para resolver um problema específico. Na programação, um framework é um conjunto de códigos genéricos capaz de unir trechos de um projeto de desenvolvimento.

em alguma outra composição de serviço.

Face ao exposto, atualmente, pequenos empreendedores estão adotando a abordagem de sistemas orientados para aplicativos de vendas online. Essa abordagem permite que os desenvolvedores de software criem aplicações mais flexíveis e escaláveis, ao mesmo tempo em que reduzem a complexidade e os custos de desenvolvimento.

Portando a criação e manutenção de aplicativos e sites para e-commerce envolve diversas etapas, desde o planejamento até sua implementação. O processo envolve etapas como:

- Planejamento: define os objetivos do site. Qual seu público-alvo, conteúdo e suas funcionalidades. Nessa etapa são definidos ainda, a arquitetura do site, ou seja, a estrutura das páginas e como elas estarão interligadas.
- Design: etapa fundamental, pois é momento de criação do visual do site, inclui a escolha de cores, tipografia, imagens, além de elementos visuais que irão compor o layout do site.
- Desenvolvimento Front-end: nesta etapa, o profissional colocar em prática a estrutura de um site ou interface. Isso inclui a codificação HTML, CSS e JavaScript, com utilização de frameworks. Estas três linguagens permitem essas funcionalidades: HTML (responsável pela estrutura da página), CSS (cores e estilos), e o JavaScript (que traz vitalidade para as páginas da web).
- Desenvolvimento Back-end: nesta etapa, o código irá controlar o funcionamento do site criado. Cria uma ponte a qual permite que os sites acionem ações e as busque no banco de dados com base no que o usuário demanda no front-end, alimentado com as informações necessárias, trabalhando em conjunto para entregar o produto final ao usuário. As linguagens utilizadas variam podendo ser PHP, Ruby, Java, C#, JavaScript, Python, entre outras.
- Segurança e autenticação: segurança é uma questão crucial para a criação de sites de vendas e-commerce, pois os sites processam informações confidenciais de seus clientes, como dados pessoais, informações de cartão de crédito e históricos de compras. Qualquer falha na segurança pode resultar em danos financeiros e à reputação da empresa.
- Testes e lançamento: nesta última etapa, o site começa a ser testado em diferentes navegadores e dispositivos (desktop ou mobile) para garantir que tudo funcione corretamente. Logo após os testes, o site pode ser lançado para o público.

3. METODOLOGIA

O estudo foi apresentado a partir de pesquisa estratégica com análise de arquivos relacionados as variáveis observadas e, os resultados foram apresentados de maneira descritiva e quantitativa. Além da utilização de uma abordagem qualitativa, através de análises de estudos de casos sobre o assunto.

Para seleção de amostra foram utilizadas buscas em diferentes lojas virtuais para compressão do funcionamento de diferentes setores, tamanhos e níveis de maturidade na utilização de TI. Para coleta dos resultados e discussões foram realizados a partir da revisão literária com identificação de práticas e teorias.

A análise teve como fonte dados secundários, quanto a evolução do E-commerce no

Brasil, bem como a importância da Tecnologia da Informação para análise de dados e segurança das transações comerciais. Também foram discutidos pontos quanto a criação de sites e ferramentas que fornecem uma estrutura básica para o desenvolvimento de software, eliminando a necessidade de escrever código repetitivo e permitindo que os desenvolvedores se concentrem nas áreas-chave do projeto.

Os elementos textuais foram colhidos a partir de Revisão Bibliográfica. O período dos artigos pesquisados foi filtrado a partir de publicações nos últimos 12 anos.

As palavras-chave utilizadas como busca para esta pesquisa foram: Tecnologia da Informação; E-commerce; Rede de Computadores; Segurança; Criação de Sites.

4. RESULTADOS E DISCUSSÃO

A partir da pesquisa em questão foi possível perceber a eficiência e comodidade que o e-commerce tem promovido para alavancar os negócios. De acordo com site Terra.com em recente pesquisa, realizada em 2023, através da Associação Brasileira de Comércio Eletrônico (ABComm) as vendas registradas no e-commerce brasileiro chegaram a R$ 169,6 bilhões em 2022, um aumento de 5% em comparação ao ano de 2021. As previsões apontam ainda, um crescimento estimado em R$ 185,7 bilhões em 2023.

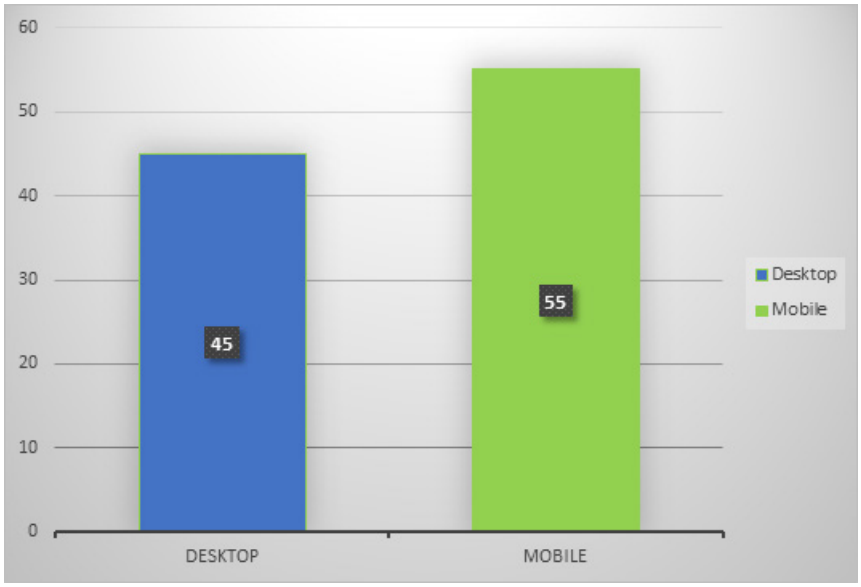


Grafico 1 – DISPOSITIVOS DE VENDAS ON-LINE

Fonte**:** ABCOMM (2022)

Segundo o gráfico 1 é possível identificar que o aumento nas vendas online também está relacionado ao crescimento de consumo via dispositivos mobile, representando 55% no total das vendas, enquanto dispositivos desktop apresentam 45%. Foi possível perceber que o cenário pandêmico da Covid-19, teve grande influência e aumentaram de forma considerável as vendas a partir de tecnologias digitais. Com os comércios fechados as compras pela internet passaram a ser uma opção segura para o consumo.

No que se refere a criação de sites para e-commerce, foi possível perceber que esta pode ser considerada uma parte fundamental do desenvolvimento web e tem um papel importante no sucesso de muitos negócios de comércio eletrônico. Nesse sentido, um site de e-commerce projetado de forma organizada e bem articulada, pode alavancar a marca, fornecer informações importantes aos clientes e aumentar as vendas.

A criação de sites promove aos negócios meios adequados para que informações sejam fornecidas de forma detalhada sobre seus produtos e serviços, permitindo que os clientes decidam qual a melhor opção de compra. É possível ainda, que os empreendedores gerenciem seus estoques e realizem transações comerciais de maneira mais eficiente.

Além disso, outra vantagem da criação de sites para e-commerce é a personalização. Os sites podem ser projetados para fornecer uma experiência personalizada para cada usuário, exibindo produtos e recomendações com base em seus interesses e histórico de navegação. Isso pode melhorar a experiência do usuário e aumentar o envolvimento do cliente.

Porém, a criação de sites para e-commerce também apresenta alguns desafios. Um deles é garantir que o site seja otimizado por mecanismos de busca SEO (Search Engine Optimization) que significa otimização para mecanismos de busca. Um outro desafio é garantir que o site seja seguro e confiável para as transações financeiras dos clientes. Nesse sentido, é de extrema importância que os sites de e-commerce sejam projetados com recursos de segurança robustos para proteger as informações pessoais e financeiras dos clientes. Para tanto, é necessário seguir algumas medidas de segurança como: o de forma organizada e bem articulada, pode alavancar a marca, fornecer informações importantes aos clientes e aumentar as vendas.

A criação de sites promove aos negócios meios adequados para que informações sejam fornecidas de forma detalhada sobre seus produtos e serviços, permitindo que os clientes decidam qual a melhor opção de compra. É possível ainda, que os empreendedores gerenciem seus estoques e realizem transações comerciais de maneira mais eficiente.

Além disso, outra vantagem da criação de sites para e-commerce é a personalização. Os sites podem ser projetados para fornecer uma experiência personalizada para cada usuário, exibindo produtos e recomendações com base em seus interesses e histórico de navegação. Isso pode melhorar a experiência do usuário e aumentar o envolvimento do cliente.

Porém, a criação de sites para e-commerce também apresenta alguns desafios. Um deles é garantir que o site seja otimizado por mecanismos de busca SEO (Search Engine Optimization) que significa otimização para mecanismos de busca. Um outro desafio é garantir que o site seja seguro e confiável para as transações financeiras dos clientes. Nesse sentido, é de extrema importância que os sites de e-commerce sejam projetados com recursos de segurança robustos para proteger as informações pessoais e financeiras dos clientes. Para tanto, é necessário seguir algumas medidas de segurança como mostra a tabela 1:

Certificado SSL	Secure Sockets Layser (SSL): É uma medida de segurança fundamental para qualquer site de vendas, Ele certifica que a troca de informações entre o navegador do usuário e o site estejam criptografadas e protegidas.
Autenticação de usuário	Tem como finalidade garantir que apenas usuários devidamente autorizados tenham acesso a informações confidenciais, como dados de cartão de crédito. Além da implementação de senhas fortes, autenticação de dois fatores e outras medidas de segurança.
Proteção contra-ataques de injeção de SQL	Os ataques de injeção SQL são ataques mais comuns em sites de comércio eletrônico, que podem ser evitados com a implantação de filtros de entrada de dados e com o uso de comandos SQL particularizados.

Monitoramento de atividades suspeitas	É de devida importância a monitoração constante das atividades no site, em busca de atividades suspeitas, tais como tentativas de login não sucedidas com frequência, transações financeiras incomuns ou atividade suspeita de usuários.
Atualizações regulares de segurança	É importante a manutenção e atualização do site com as mais modernas correções de segurança e patches para assegurar que qualquer tipo de vulnerabilidade seja corrigido o quanto antes.

Tabela 1 – Segurança

Fonte: Ramos (2023)

Percebe-se que a criação de sites para e-commerce é uma parte essencial do desenvolvimento web e oferece muitas vantagens para os negócios de comércio eletrônico. Contudo, os desenvolvedores devem estar cientes dos desafios envolvidos e trabalhar para projetar sites de e-commerce que sejam otimizados para SEO, fáceis e seguros de usar.

Por fim, destaca-se a busca em diferentes lojas virtuais para melhor visualização do funcionamento dos sites de compra e vendas online tendo como resultado que essa pode ser uma estratégia eficiente para compreender o funcionamento de diferentes setores, tamanhos e níveis de maturidade na utilização de TI.

Como por exemplo, ao pesquisar em lojas virtuais de diferentes segmentos, como moda, eletrônicos, livros, etc., é possível observar como cada uma delas lida com questões como segurança, velocidade de carregamento, experiência do usuário, integração com redes sociais, entre outros aspectos. Dentre a pesquisa observou-se as variáveis de venda por categorias como:

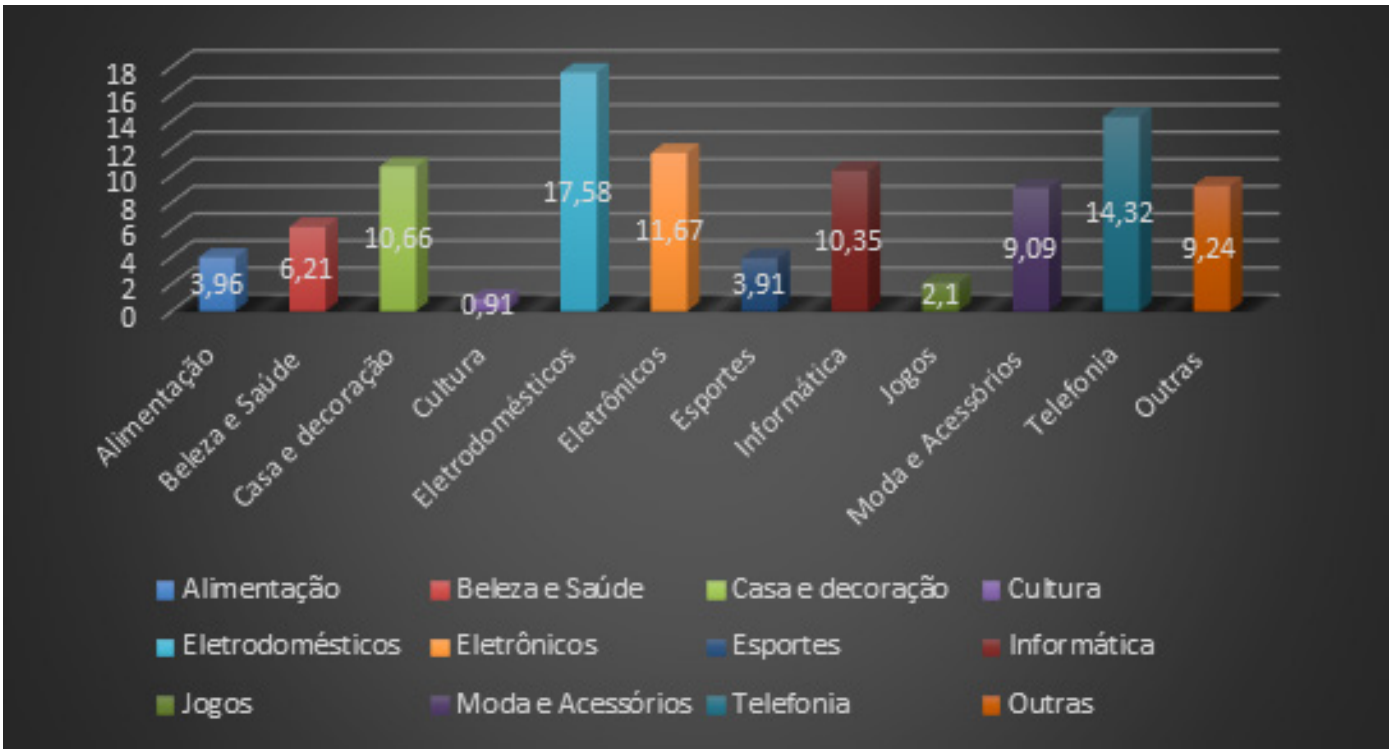


Gráfico 2 – Dados de vendas por categoria

Fonte**:** ABCOMM (2022)

O gráfico 2 apresenta dados sobre as principais categorias de vendas online. As categorias e sites como de venda de produtos eletrônicos em sua maioria cerca de 90% apresentam facilidade de acesso e segurança quanto a compra de produtos. Percebe-se que os sites foram criados com intuito de agilizar as vendas com conforto e facilidade.

Além disso, a pesquisa em lojas virtuais de diferentes tamanhos também pode fornecer informações valiosas sobre como empresas de diferentes portes lidam com a TI. Empresas maiores, com mais recursos financeiros e humanos, podem ter sites mais complexos e sofisticados, enquanto empresas menores podem optar por soluções mais simples e econômicas.

5. CONCLUSÃO

Face ao problema norteador, que discutiu sobre os impactos da indisponibilidade dos serviços de TI para o desenvolvimento do e-commerce na atualidade, é indiscutível que a tecnologia da informação (TI) é essencial para a garantia do sucesso do e-commerce, uma vez que a mesma é responsável por diversos aspectos que vão desde a criação de sites e aplicativos até a segurança dos dados e gerenciamento de software.

Com o estudo foi possível compreender ainda, a importância da adoção de mecanismos de segurança e de gerenciamento de software para garantir a disponibilidade de serviços de TI, diminuindo a possibilidades de impactos negativos para o desenvolvimento do e-commerce.

Com os resultados obtidos durante a pesquisa, ficou claro a eficiência de aplicativos de vendas online, tendo em vista que o consumidor está sempre em busca de respostas simples que visem ao atendimento de suas expectativas com rapidez e segurança durante as operações de compra e venda virtual. Além, do gerenciamento de software de padronização de dados como elementos essenciais para o sucesso dos negócios. Portanto, destaca-se novamente a importância da criação de sites com eficiência, presteza e segurança, pois a partir dessa ferramenta é possível que o consumidor sinta a presença online do vendedor, sendo garantido atendimento 24 horas por dia, e isso é conveniente para os clientes e aumenta as chances de venda.

Em resumo, a criação de um site para e-commerce é uma das maneiras mais eficazes de expandir uma presença online, além de aumentar o alcance do público, melhorando a experiência do cliente com a empresa.

Em resposta ao objetivo geral, conclui-se que a tecnologia da informação (TI) é utilizada no e-commerce em todas as etapas do processo de vendas online, desde a criação do site até a entrega do produto ao consumidor final. Sendo assim, ao analisar o funcionamento da TI no e-commerce, foi possível perceber insights valiosos sobre como melhorar a eficiência e eficácia das operações de vendas virtuais. Isso inclui a adoção de novas tecnologias, aprimoramento dos processos já existentes e a utilização de análise de dados para orientar as decisões do negócio.

Portanto, conclui-se que a TI é um elemento chave para o sucesso do e-commerce, e a sua indisponibilidade pode ter impactos significativos no desenvolvimento desse mercado. Sendo assim, é fundamental que as empresas que atuam nesse setor adotem medidas efetivas de segurança e gerenciamento de software, visando garantir a disponibilidade e qualidade dos serviços de TI, além de buscar se manter atualizadas em relação às novas tecnologias e plataformas disponíveis.

Referências

ABCOMM. **Forekast**. Disponível em: https://dados.abcomm.org/numeros-do-ecommerce-brasileiro. Acesso em: 05 de abr. 2023.

AKKARI, Alessandra Cristina Santos. **Gestão da Informação.** Londrina: Editora e Distribuidora Educacional S.A, 2018.

CLARO, Alberto. **Comércio eletrônico**. de O. Gonçalves; revisão técnica Kechi Hirama. — 9. ed. — São Paulo: Pearson São Paulo: Know How, 2013.

LEMOS II, Dalton Luiz. **Tecnologia da Informação** – 2 ed. Florianópolis: Publicações do IF – SC, 2011.

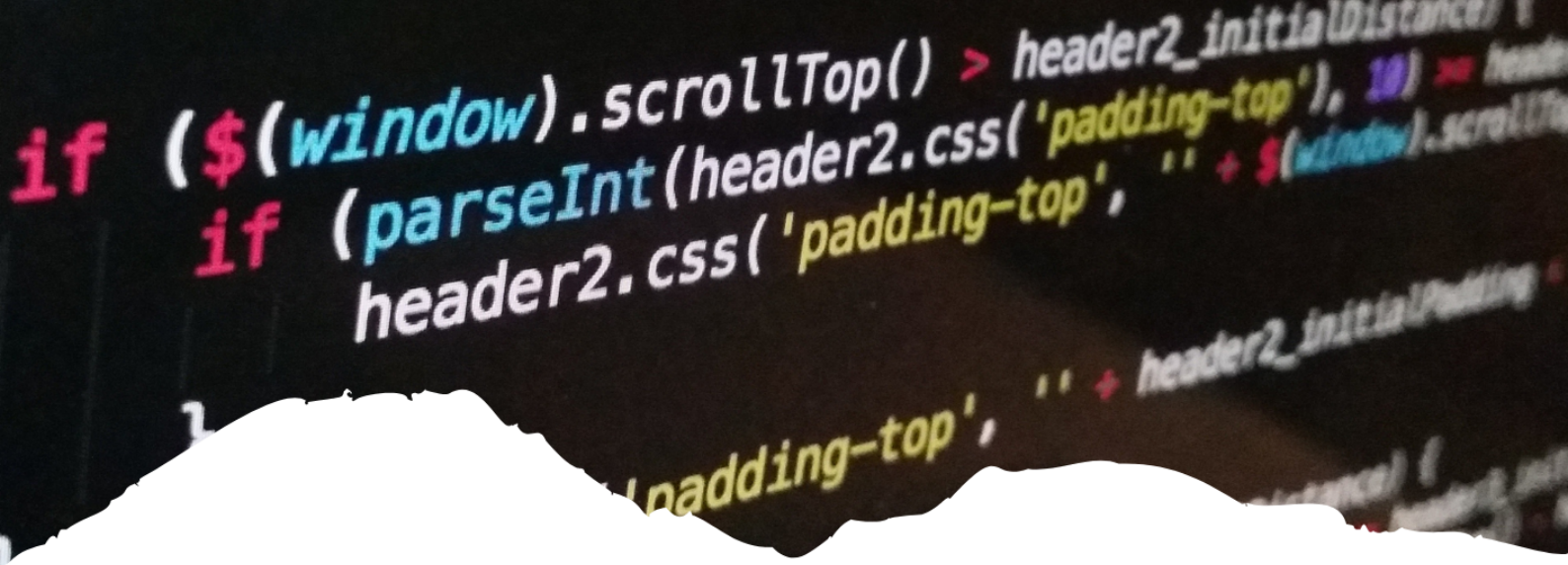
LIMA DE, Igor Ferreira e Vieira, Mateus de Almeida Fernandes. **E-COMMERCE: A importância de uma boa experiência online.** Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/20832/1/TCC%20Igor%20Ferreira%20de%20Lima%20e%20Matheus%20de%20Almeida%20Fernandes%20Vieira.pdf. Trabalho de Curso apresentado ao Centro Superior UNA de Catalão – UNACAT. Acesso em: 10 de abr. 2023.

NUNES, Sergio Eduardo. **Tecnologia da Informação na Gestão de Conhecimento**. Londrina: Editora e Distribuidora Educacional S.A, 2018.

OLIFER, Natalia. **Rede de Computadores**: princípios, tecnologias e janeiro: LTC, 2008. Prentice Hall, 2011.

SEBRAE. Uma breve definição sobre o comércio online, 2016. Disponível em: https://www.sebrae.com.br/sites/PortalSebrae/artigos/uma-breve-definicao-sobre-o-comercio-. Aceso em: 06 de abr. 2023.

Sommerville, Ian. **Engenharia de Software**; tradução Ivan Bosnic e Kalinka G.



27

A TRANSFORMAÇÃO DE SOFTWARES GERENCIAIS EM SISTEMAS DE APOIO À TOMADA DE DECISÕES

THE TRANSFORMATION OF MANAGEMENT SOFTWARE INTO DECISION SUPPORT SYSTEMS

Erivaldo Pires Santos

Resumo

O presente artigo apresenta um estudo sobre os *softwares*, destacando os sistemas computacionais estruturados e de base para tomada de decisões. Enfatizou as transformações dos *softwares*, e com base nas referências bibliográficas apresentou os principais conceitos e características que constituem um sistema. As empresas estão inseridas em um cenário empresarial de grande produtividade e de grande competitividade no mercado. Desde a criação da engenharia de *software* que intensificou a busca por aperfeiçoamento nos métodos de trabalho, o desenvolvimento de um *software* é um processo muito complexo que envolve vários fatores. Deste modo, a engenharia de *software* forneceu um amadurecimento no que diz respeito ao seu desenvolvimento, suas características e processos. O trabalho foi elaborado através de uma pesquisa qualitativa e descritiva, de natureza exploratória, utilizando-se de pesquisa bibliográfica onde foram feitos estudos a grandes autores de obras e artigos já publicados. Consiste em proporcionar às empresas ferramentas tecnológicas capazes de trazer um diferencial competitivo, transformar formas já ultrapassadas por meios mais eficientes e eficazes de levantamento de dados para elaboração relatórios específicos às necessidades e demandas das empresas quanto ao processo de tomada de decisão.

Palavras-chave: Software, Engenharia, Tecnologia, Decisão, Sistemas.

Abstract

This article presents a study on software, highlighting structured and basic computational systems for decision-making. Emphasized software transformations, and based on bibliographic references presented the main concepts and characteristics that constitute a system. Companies are inserted in a business scenario of high productivity and great competitiveness in the market. Since the creation of software engineering that intensified the search for improvement in working methods, software development is a very complex process that involves several factors. In this way, software engineering provided a maturation with regard to its development, its characteristics and processes. The work was elaborated through a qualitative and descriptive research, of an exploratory nature, using bibliographical research where studies were made of great authors of works and articles already published. It consists of providing companies with technological tools capable of bringing a competitive advantage, transforming outdated forms into more efficient and effective means of collecting data to prepare specific reports to the needs and demands of companies regarding the decision-making process.

Keywords: Software, Engineering, Technology, Decision, Systems.

1. INTRODUÇÃO

A maneira acelerada em que as mudanças tecnológicas foram surgindo exige cada vez mais das empresas a inovação para que haja um diferencial das concorrentes, criando um destaque no seu mercado de atuação. O mercado passou a ser movido pela tecnologia no desejo de conseguir a redução dos custos, os gestores direcionam seus esforços para otimizar os procedimentos já existentes ao processo produtivo e adiarem a necessidade de investir em uma melhor organização dos procedimentos administrativos dentro da instituição. Pondo neste novo cenário em que o centro das organizações está voltado à informação, tem-se a necessidade de adquiri-las de maneira rápida e eficaz trazendo bases para a tomada de decisão. Essa nova era tecnológica é uma realidade para todo mercado empresarial e assim tornando indispensável uma organização mais rápida para evitar perdas no espaço já conquistado no mercado.

Uma das tecnologias em evidência no mercado é o SAD – Sistema de Apoio à Decisão, sistema que auxilia no processo decisório com informações mais precisas de forma rápida. O SAD permite aos tomadores de decisões buscarem por informações em bancos de dados e locais distintos para que possam acessar a dados específicos e ter um melhor posicionamento nas decisões para a organização. Outra tecnologia de grande destaque é o *Business Intelligence* (BI) que significa Inteligência de Negócios, também chamado de Inteligência Empresarial por abranger todos os setores de uma empresa. O BI é um conjunto de técnicas e ferramentas que tem a possibilidade de oferecer suporte à tomada de decisão e monitora os resultados da empresa.

A tomada de decisão é um momento de extrema importância para a empresa, pois traz consigo riscos e oportunidades. Sendo assim, necessita-se que todas as informações e os dados necessários estejam disponíveis. Os *softwares* gerenciais servirão de auxílio para alcançar melhores resultados, a tomar decisões assertivas.

O presente artigo buscou atestar a importância da utilização de *software* gerenciais para auxiliar e acelerar os processos gerenciais da instituição, bem como aperfeiçoá-los e transformá-los em sistemas de apoio a tomada de decisões, apresentando o máximo de opções para que o empresário possa tomar decisões mais assertivas possíveis e corra menos riscos nos negócios.

2. DESENVOLVIMENTO

2.1 Metodologia

Este artigo foi desenvolvido através de uma pesquisa qualitativa e descritiva, com procedência bibliográfica. Baseando-se em fontes como sites, artigos e livros acerca do tema, trabalhos estes publicados nos últimos dez anos. Objetivou-se explanar a transformação de *softwares* gerenciais em sistemas mais modernos para auxiliarem nas tomadas de decisões de uma organização, enfatizando os estudos de Douglas Rocha Mendes, um dos autores de maior referência no mercado. Palavras-chave utilizadas nas buscas: Software, Engenharia, Tecnologia. Decisão.

2.2 Resultados e Discussão

A tomada de decisão é algo desafiador a gerentes e executivos, suas decisões devem ser consideradas em longo prazo, mas com resultados imediatos. Desta forma, surge a necessidade de tomar decisões de forma rápida e eficiente, com sistema de informações gerenciais que contribuem para a eficácia da gestão, levando em consideração ao ciclo de planejamento, organização, direção e controle. A tomada de decisões pode ser definida como a habilidade para processar informações mediante uma análise lógica e objetiva (confiar em si mesmo na hora de decidir, estar preparado para correr riscos razoáveis e para ser responsabilizado pelos resultados (BATISTA, 2006 p. 145).

Conforme Mowen e Hansen (2001) a tomada de decisão consiste na escolha entre alternativas com um final imediato, e limitado em curto prazo. Corresponde na definição do problema, identificação das alternativas, levantamento dos custos, comparação dos custos e selecionar a alternativa. Enquanto a tomada de decisão estratégica fornece garantias significativas decrescimento e sobrevivência em longo prazo.

Segundo Pressaman (2007, p. 13), "*software* é um conjunto de instruções para computadores que quando executadas tem a função de manipular dados adequadamente para se obter informação". Em outras palavras, o *software* pode ser definido como um conjunto de algoritmos que designa diversas instruções para serem executadas para alcançar determinado objetivo. O desenvolvimento de um *software* é uma das atividades mais valorizadas no mercado empresarial, ocorre quando se modificam os sistemas atuais de software para atender a novos requisitos, a mudanças de processos gerenciais ou regras de negócio. Diante disto, as mudanças são inevitáveis e o *software* deve se adaptar as mudanças para continuar útil. Com isso, é correto pensar que a engenharia de *software* define o *software* como um processo evolutivo, no qual é alterado constantemente durante seu ciclo de vida para que possa atender as demandas e necessidades dos clientes. Em consequência disso, a distinção entre manutenção e desenvolvimento é cada vez mais desnecessário, pois são processos contínuos (SOMMERVILLE, 2011).

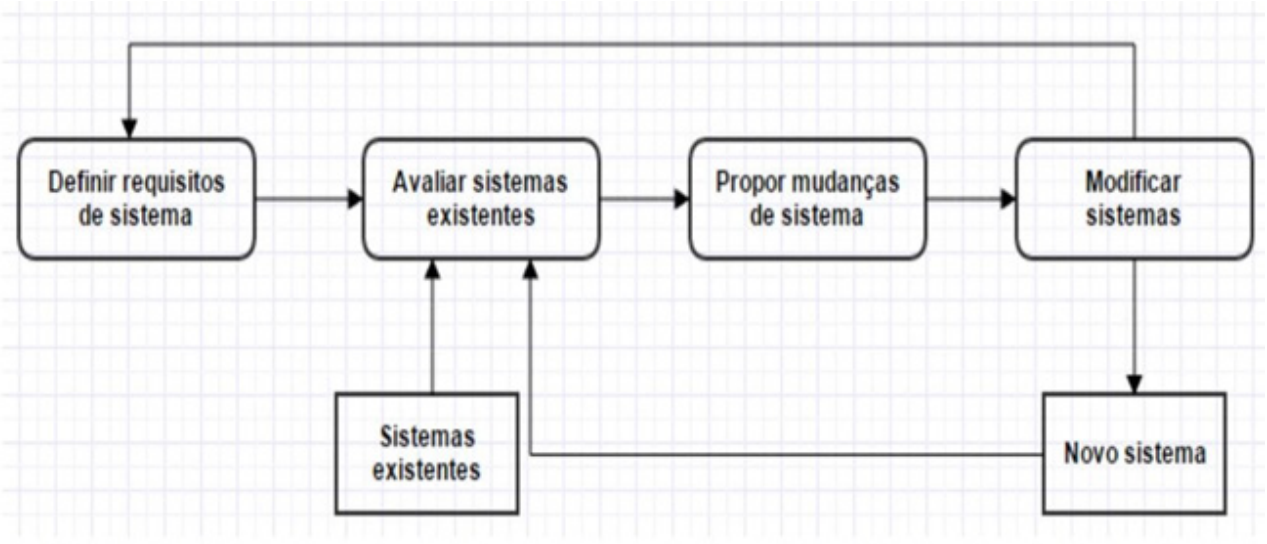


Figura 1: Evolução do sistema

Fonte: Sommerville (2011)

A figura 1 é uma representação de um processo de um sistema que passou por mudanças, as modificações necessárias para elevar o nível do sistema. Seguindo as etapas iniciamos com o Levantamento de Requisitos para saber quais as reais necessidades e exigências a serem seguidas pelo *software*, em seguida Avaliar Sistemas Existentes ana-

lisando assim se é possível há condições possíveis de mudanças. Após análises, são feitas as propostas de mudanças do sistema para assim fazer as devidas modificações, com as mudanças adequadas haverá os períodos de testes para assim dar continuidade na implementação do novo sistema. A evolução pode iniciar de requisitos já existentes que não foram implementados, de novos requisitos, de correções de *bugs* ou de novas melhorias de *software* que vieram da própria equipe de desenvolvimento. Esse processo de mudança e de evolução é periódico e continua por toda a vida do sistema.

Os sistemas de informações estão cada vez mais computadorizados, envolvendo vários elementos para o seu desenvolvimento, como Hardware, Software, Banco de Dados, Recursos Humanos, Redes e telecomunicações, Processamentos e Procedimentos. Os primeiros *softwares* surgiram na década de 50 (BOEHM, 2006). Neste período, o foco principal dos pesquisadores era voltado ao *hardware*. O *software* ainda era desconhecido, não possuía nenhuma técnica de engenharia e sua distribuição era bastante limitada. O *hardware* é geralmente encontrado nos grandes centros de pesquisas, e com isso, o *software* era pouco conhecido.

Somente a partir de meados dos anos 60, com o surgimento de microprocessadores, o *hardware* deixou de ser o foco dos pesquisadores, e passaram a investir em *software*. Assim, grandes organizações começaram a desenvolver grandes sistemas, criando o conceito de produto de *software*, passando a comercializá-lo (PRESSMAN, 2006). Para melhor entendimento, criou-se um quadro apontando as fases do sistema de informação acompanhado da evolução digital.

A transformação de *softwares* em sistemas de apoio à tomada de decisões é uma área de pesquisa muito importante atualmente, devido à crescente demanda por soluções que ajudem a lidar com grandes volumes de dados e a tomar decisões mais precisas e embasadas. Para que um sistema de informação seja útil e produza informações necessárias que possam ser utilizadas para controle de operações, analisar problemas, desenvolver novos projetos e tomar decisões, são necessárias três atividades importantes, que são: a entrada, o processamento e a saída.

A entrada é o processo responsável pela captação de dados brutos, dados que podem ser tanto internos quanto externos. Em seguida passa-se pelo processamento, que é a transformação dos dados brutos filtrado de uma forma mais significativa. E a saída que se refere a utilizar as informações processadas para desenvolver melhores resultados nos processos.

Existe diversos tipos de sistemas de informações empresariais, esses sistemas servem como base para a administração das empresas e a tomada de decisões. Os sistemas de informações têm por objetivos a excelência profissional, o desenvolvimento de novos produtos, auxiliar na tomada de decisões, aproximar o consumidor melhorando o atendimento e promover vantagem competitiva.

Neste artigo, foi proposto um processo para a transformação de um *software* existente em um sistema de apoio à tomada de decisões. Foram realizados testes em um *software* de gestão de estoques de uma empresa de varejo, com o objetivo de avaliar a eficácia da transformação proposta.

Os resultados mostraram que a transformação do *software* em um sistema de apoio à tomada de decisões permitiu uma melhor visualização e análise dos dados de estoque, tornando mais fácil a tomada de decisões sobre compras, estoques mínimos e máximos, entre outros aspectos. Além disso, a implementação de ferramentas de análise de dados e algoritmos de aprendizado de máquina permitiu a identificação de tendências e padrões nos dados de estoque, o que pode levar a decisões mais precisas e efetivas.

No entanto, foram identificados alguns desafios durante o processo de transformação, como a necessidade de integração de algumas ferramentas de análise de dados. Estes desafios podem ser superados com um planejamento cuidadoso e uma equipe experiente na área de transformação de *softwares* em sistemas de apoio à tomada de decisões.

Alguns outros pontos que poderiam ser discutidos em um artigo sobre a transformação de *softwares* em sistemas de apoio à tomada de decisões incluem:

- As diferentes técnicas de análise de dados e aprendizado de máquina que podem ser utilizadas para melhorar a capacidade do sistema de apoio à tomada de decisões. Por exemplo, técnicas de mineração de dados podem ser utilizadas para encontrar padrões em grandes conjuntos de dados, enquanto algoritmos de aprendizado de máquina podem ser utilizados para prever tendências futuras ou identificar anomalias.
- Os desafios associados à coleta, armazenamento e processamento de grandes volumes de dados, e as soluções que podem ser implementadas para lidar com esses desafios. Isso pode incluir discussões sobre tecnologias de banco de dados, nuvem computacional, segurança de dados e privacidade.
- A importância de uma abordagem iterativa e colaborativa para a transformação do *software* em um sistema de apoio à tomada de decisões, envolvendo diferentes *stakeholders* da empresa. Isso pode incluir os usuários finais do sistema, que podem fornecer *feedback* valioso sobre a usabilidade e a eficácia do sistema, bem como a equipe de desenvolvimento, que pode trabalhar para implementar as melhorias solicitadas pelos usuários.
- Exemplos de outros tipos de sistemas de apoio à tomada de decisões, como sistemas de inteligência de negócios, sistemas especialistas e sistemas de suporte a decisões baseados em modelos. A comparação entre esses diferentes tipos de sistemas pode ajudar a esclarecer as vantagens e desvantagens de cada abordagem.
- A importância de avaliar continuamente a eficácia do sistema de apoio à tomada de decisões e realizar ajustes e melhorias conforme necessário. Isso pode incluir a monitorização contínua dos dados de entrada e saída do sistema, a realização de testes de usabilidade com usuários finais e a implementação de atualizações de *software* para corrigir quaisquer problemas identificados.

PERÍODO	SITUAÇÃO
Antes de 1940	• Computadores não eram populares; • Técnicas de arquivamento e recuperação de informações emgrandes arquivos; • Presença do arquivador e uso excessivo de papéis; • Grande esforço para manter os dados atualizados.
1940 – 1952	• Computadores lentos e pouco duráveis; • Mão-de-obra muito grande para funcionamento; • Manutenção constante de válvulas e quilômetros de fios; • Grande espaço físico ocupado pelos computadores.
1952 – 1965	• Origem dos transmissores e microprocessadores; • Diminuição de cabos, fios e tamanho da máquina; • Início da comercialização de computadores para grandes empresas mundiais.
1965 – 1981	• Surgimento dos microcomputadores; • Linguagens de programação em alto nível; • Transmissão de dados através de redes.
1981 – Atualmente	• Altíssima velocidade; • Grande transferência de dados; • Programas de interatividade entre usuários; • Surgimento da Internet.

Quadro 1: Quadro das fases de evolução dos Sistemas de Informação.

Fonte: Construção do autor, 2023.

Percebe-se que a partir da evolução histórica, a evolução da informática foi sendo base para o sistema de informação. Dessa maneira, as empresas são beneficiadas podendo fazer uso de inovações tecnológicas cada vez maiores e mais eficazes para apoio a tomada de decisões através dos *softwares*. Através do *software* gerencial, é possível estabelecer um foco de mercado específico que atinja o público alvo de uma maneira mais abrangente buscando destaque entre os concorrentes.

A engenharia de *software* é uma área abrangente que engloba vários aspectos técnicos, gerenciais e de codificações, que vai desde a fase de levantamento de requisitos de um sistema até a fase de manutenção do mesmo. Com isso o software é tratado como um produto, sendo utilizado por seus usuários e possui qualidade e valor econômico.

> Engenharia de *Software* é a aplicação de abordagens sistemáticas, disciplinadas e quantificáveis no desenvolvimento e manutenção de *software*. Desta forma, se preocupa em como realizar as diversas atividades envolvidas no processo de desenvolvimento de *software* de forma que se tenha um produto elaborado com maior qualidade e menor custo. Neste contexto, é uma área de conhecimento bastante abrangente envolvendo desde atividades mais técnicas como programação até áreas mais gerenciais como de qualidade nos processos utilizados (ARAUJO; SPINOLA, 2007, p. 3).

É possível caracterizá-la pela aplicação de princípios científicos, modelos, métodos, padrões e teorias que facilitam o gerenciamento, planejamento, modelagem, projeção, implementação, medição, análises, manter e aprimorar sistemas de software. Possui como

principal desafio encontrar maneiras de construir um software conceitualmente utilizando-se de técnicas como, especificar, projetar, construir e testar um sistema visando *software* de qualidade (PETERS, 2001).

Sommerville (2003) afirma que a qualidade de um software é medida pelo grau em que atende seus requisitos, comportamento, estrutura e organização do programa fonte. Há muitas propriedades que definem a qualidade de um *software*, tais como: eficiência e facilidade de uso, confiabilidade, capacidade de recuperação, documentação precisa e completa, entre outros.

De acordo com as definições citadas, conclui que a engenharia de *software* é uma área extensa que não está resumida somente a tarefas de codificações de um *software*, mas também cuida de aspectos técnicos e gerenciais desde a início no levantamento dos requisitos do sistema até a fase de manutenção. Possui como objetivos primários o aprimoramento de qualidade dos produtos de *software* objetivando sistematizar a produção, a manutenção e a evolução de modo que ocorra dentro de prazos e custos desejados utilizando princípios, métodos tecnológicos e processos contínuos para o seu aperfeiçoamento. Com isso, a engenharia de software trata do software como um produto que deverá ser útil aos seus usuários, possuindo um valor econômico e qualidade.

3. CONCLUSÃO

Em decorrência da complexidade encontrada nos ambientes organizacionais, as instituições encontram muitas dificuldades no processo de desenvolvimento de *software,* é uma área de grande expansão, pois existe uma grande demanda das empresas para a manutenção de *softwares* já existentes. A transformação de *software* para auxiliar na tomada de decisões vai contribuir com informações para o desenvolvimento da empresa. Uma empresa que não investe na qualidade dos seus sistemas corre o risco de perder clientes, e encontrar dificuldades para prospectar novos negócios.

Para atender o mercado da forma mais eficiente, as organizações precisam levantar informações necessárias sobre seu campo de atuação, seu negócio, seus concorrentes e especialmente seu público-alvo. Estas informações somente são emitidas através de processos de pesquisas que fazem parte da definição de um problema, seus objetivos estabelecidos, coleta e análise de dados desenvolvidos e a mensuração dos resultados e ações propostas.

Ao investir no desenvolvimento de um *software* a organização se destaca em um mercado cada vez mais competitivo, transmitindo confiabilidade, preparo e organização, tanto para o mercado como para os clientes. Substituindo a ferramenta atual com novas tecnologias de gerenciamento de dados, algo mais completo e evitando diversos processos que já se tornaram obsoletos, como uso de planilhas, arquivos e e-mail. Novos sistemas terão aplicabilidades diferentes, mas com base em sistemas já existentes.

Referências

ARAUJO, M.; SPINOLA, E. **Editorial Qualidade de Software**. Engenharia de Software Magazine, ano 1, ed. 1, 2007. Edição especial. p. 3. Disponível em: http://www.devmedia.com.br/articles/viewcomp.asp?comp=8028 Acesso em: 25/09/2022.

BATISTA, Emersos. **Sistema de Informação: o uso consciente de tecnologia para o gerenciamento.** São Paulo: Saraiva, 2006.

BOEHM, B. **A View of 20th and 21stCentury Software Engineering.** ICSE'06, 2006.

MOWEN, Maryanne M.; HANSEN, Don R. **Gestão de Custos.** São Paulo: Pioneira Thomson Learning, 2001.

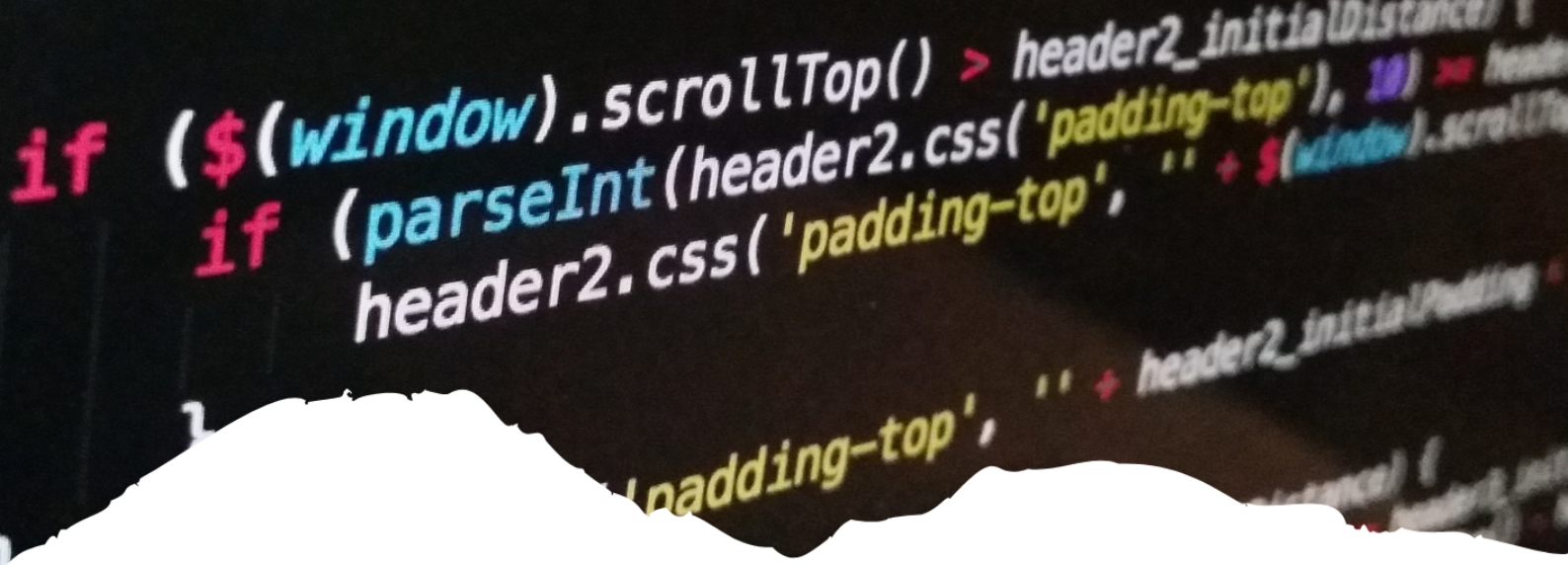
PETERS, James F. **Engenharia de Software, Teoria e Prática,** 1º ed, Rio de Janeiro: Campus, 2001.

PRESSMAN, R. S. **Engenharia de Software.** 3º ed. São Paulo: Person Makron Books, 2007.

REZENDE, Denis A. **Engenharia de Software e Sistemas de Informação,** 3º ed. Rio de Janeiro: Brasport, 2005.

SOMMERVILLE, Ian. **Engenharia de Software.** 8º ed, Pearson Education, 2011.

SOMMERVILLE, Ian. **Testes de Software.** Tradução: Mauricio de Andrade. 6. ed. São Paulo: Addison Wesley, 2003.



28

SEGURANÇA DA INFORMAÇÃO EM IOT: UMA REVISÃO DE LITERATURA

INFORMATION SECURITY IN IOT: A LITERATURE REVIEW

Washington Gonçalves Moura
Mirian Nunes de Carvalho Nunes
Marta de Oliveira Barreiros

Resumo

Este trabalho tem como objetivo geral realizar uma revisão de literatura sobre segurança da informação em Internet das Coisas (IoT). A natureza do problema estudado é a crescente utilização de dispositivos IoT, que trazem consigo muitos vulnerabilidades e riscos de segurança. A metodologia utilizada envolveu a pesquisa em bases de dados eletrônicas e a seleção de artigos relevantes sobre o assunto. Os resultados mostram que a segurança em IoT é um desafio complexo que requer a implementação de medidas efetivas para garantir a privacidade, integridade e disponibilidade das informações. Entre as principais considerações finais da pesquisa, destaca-se a importância da implementação de políticas de segurança para dispositivos IoT, a necessidade de desenvolvimento de técnicas de autenticação e criptografia mais robustas e a importância da conscientização e treinamento dos usuários para reduzir os riscos de segurança em IoT.

Palavras-chave: Segurança, Informação, IoT, Aplicação, Dispositivos.

Abstract

This work has as general objective to carry out a literature review on information security in Internet of Things (IoT). The nature of the problem studied is the increasing use of IoT devices, which bring with them a large number of vulnerabilities and security risks. The methodology used involved the search in electronic databases and the selection of relevant articles on the subject. The results show that IoT security is a complex challenge that requires the implementation of effective measures to ensure the privacy, integrity and availability of information. Among the key final considerations of the research are the importance of implementing security policies for IoT devices, the need to develop more robust authentication and encryption techniques, and the importance of user awareness and training to reduce IoT security risks.

Keywords: Security, Information, IoT, Aplication, Devices.

1. INTRODUÇÃO

A segurança da informação em IoT (Internet das Coisas) é um tópico cada vez mais importante, devido à crescente utilização de dispositivos interconectados em diferentes setores, desde residenciais até industriais. A IoT apresenta desafios únicos de segurança, pois a conexão entre dispositivos e a coleta de dados pode ser vulnerável a ataques mal-intencionados. Além disso, a diversidade de dispositivos e plataformas IoT dificulta a implementação de medidas de segurança padronizadas para garantir a segurança na IoT, é fundamental que sejam tomadas medidas desde o design dos dispositivos, passando pela implementação de protocolos de segurança, criptografia, autenticação e autorização, monitoramento contínuo e atualizações de segurança regulares. Também é importante garantir a privacidade dos dados coletados e armazenados pelos dispositivos IoT. A segurança da informação em IoT é um desafio constante e requer um esforço conjunto dos fabricantes, desenvolvedores, reguladores e usuários finais para garantir a confiabilidade, integridade e confidencialidade dos dados.

Diante do exposto o tema do presente trabalho é Segurança da informação em IoT: uma revisão de literatura, representado por uma interconexão entre dispositivos de meio físico com a internet e conhecido como IoT (do Inglês Internet Of Things) internet das coisas. Essa tecnologia já está internalizada no cotidiano da sociedade.

A segurança em IoT visa garantir a privacidade e a proteção de dados pessoais e promover a transparência na relação entre pessoas físicas e jurídicas. Com a legislação vigente, a coleta, tratamento e comercialização de dados pessoais só podem ser feitos com a autorização dos titulares desses dados. A questão da segurança dessa tecnologia não está acompanhando o mesmo ritmo que a aplicação da própria, tendo em vista que milhares de usuários fazem a inserção de seus dados pessoais em dispositivos com IoT.

Diante do exposto questiona-se, de que forma a segurança de informação podem ser implementados nos dispositivos IoT? Baixos níveis de segurança são os pontos focais para os usuários de tecnologia. Os brasileiros passam mais de seis horas conectados na Internet, para enviar e-mail, utilizar redes sociais, aplicativos para Smartphones, jogos e muitas outras tarefas, com isso as pessoas ficaram cada vez mais conectadas. A internet é um grande avanço da tecnologia, dessa forma surgiu uma oportunidade de negócio, com a criação e utilização de objetos inteligentes (IoT).

Dessa forma, para responder ao questionamento teve-se como objetivo geral descrever os aspectos de segurança da informação em sistemas de IoT e os objetivos específicos foram conceituar segurança da informação em IoT, apresentar pontos positivos da aplicação de segurança a informação em IoT e exemplificar a aplicação da segurança em IoT em implementação de dispositivos.

2. DESENVOLVIMENTO

2.1 Metodologia

O trabalho tratou de uma revisão bibliográfica, metodologia na qual foram pesquisados em livros digitais, dissertações e artigos científicos selecionados através de busca nas seguintes bases de dados Google acadêmico e SciELO. O período dos artigos pesquisados foram os trabalhos publicados nos últimos 5 (cinco) anos. As palavras-chave utilizadas na busca foram: Segurança, informação, IoT, aplicação e dispositivos. Os principais autores

citados foram: Estefânia Arata, Nairobi Oliveira, Dorival Junior, Westphall Johann, André Carvalho e Vagner Quincozes.

2.2 Resultados e Discussão

A Internet das Coisas (IoT) é um conceito emergente que se refere à interconexão de dispositivos físicos, veículos, edifícios e outras coisas com a finalidade de coletar, armazenar e transmitir dados. No entanto, a segurança da informação em IoT é uma preocupação importante, já que a exposição de dispositivos a ameaças cibernéticas pode levar a danos graves. Nesta seção, serão apresentados resultados e discussões sobre a segurança da informação em IoT, referenciando autores importantes no assunto.

Segundo Zhang e Xu (2020), a segurança da informação em IoT é uma questão complexa devido à grande quantidade de dispositivos envolvidos e à diversidade das tecnologias utilizadas. Os autores destacam que, para garantir a segurança da informação em IoT, é necessário implementar medidas de segurança em cada camada do sistema, desde a coleta de dados até a transmissão e armazenamento. Além disso, é importante realizar testes de segurança e atualizações regulares para garantir que os dispositivos IoT estejam sempre protegidos contra as últimas ameaças.

De acordo com Li et al. (2019), a criptografia é uma das principais medidas de segurança em IoT. Os autores destacam que a criptografia de ponta a ponta é essencial para proteger os dados coletados por dispositivos IoT durante a transmissão. Além disso, a criptografia também é importante para proteger os dados armazenados em dispositivos IoT. Os autores ressaltam que a criptografia deve ser implementada de forma eficiente e econômica para garantir a segurança da informação em IoT.

Por sua vez, Paul, Qu e Wen (2021) destacam a importância da autenticação e autorização em IoT. Os autores ressaltam que a autenticação é fundamental para verificar a identidade dos usuários e dispositivos IoT. Já a autorização é importante para garantir que apenas usuários autorizados tenham acesso aos dados coletados por dispositivos IoT. Os autores destacam que é necessário implementar medidas de autenticação e autorização em cada camada do sistema IoT para garantir a segurança da informação.

Os autores Al-Hamadi *et al*. (2020) enfatizam a importância da detecção e resposta a ameaças em IoT. Os autores destacam que é necessário implementar sistemas de detecção de ameaças em tempo real para identificar e responder rapidamente a possíveis ataques cibernéticos. Além disso, os autores ressaltam que é importante implementar sistemas de backup e recuperação para garantir a disponibilidade dos dados em caso de incidentes de segurança.

Segurança da informação em IoT é uma questão complexa que requer medidas de segurança em cada camada do sistema, incluindo criptografia, autenticação, autorização e detecção e resposta a ameaças. É importante realizar testes de segurança e atualizações regulares para garantir que os dispositivos IoT estejam sempre protegidos contra as últimas ameaças. Vários autores destacam a importância dessas medidas para garantir a segurança da informação em IoT.

Conforme os autores supracitados destacam-se alguns conceitos elencados pelos mesmos no que se refere a segurança da informação em IoT: Autenticação: É o processo de verificar a identidade de um usuário, dispositivo ou serviço antes de permitir o acesso aos dados. A autenticação pode ser baseada em senhas, tokens, certificados digitais ou outros métodos, criptografia: A criptografia é o processo de codificar informações para que

elas possam ser transmitidas de forma segura, a criptografia pode ser usada para proteger dados durante a transmissão e armazenamento, atualizações de software: As atualizações de software são importantes para corrigir vulnerabilidades de segurança e adicionar novos recursos e funcionalidades. É importante que os fabricantes forneçam atualizações regulares para os dispositivos IoT, proteção de dispositivos: Os dispositivos IoT devem ser protegidos contra ameaças externas, como vírus, malware e ataques de negação de serviço (DoS). Isso pode ser feito por meio de firewalls, atualizações de software, autenticação e outros métodos, controle de acesso: O controle de acesso é o processo de restringir o acesso aos dados coletados pelos dispositivos IoT. Isso pode ser feito por meio de políticas de acesso, autenticação e criptografia.

A IoT já vem se desenvolvendo há muito tempo, produtos e serviços estão conectados e compartilhando dados o tempo todo (TVs, casas, equipamentos do agronegócio e etc.). Segundo o site Everest Ridge a partir do ano de 2021 uma previsão de mais de bilhões de coisas estariam conectadas. Conforme visão dessa grande quantidade de aparelhos conectados, armazenando dados e trabalhando com coleta de dados (pessoais e profissionais) volta-se o olhar para a segurança da informação em IoT.

Para toda tecnologia desenvolvida existem desafios a serem concluídos. “Se as informações coletadas por esses dispositivos forem hackeados e comprometidos, vai prejudicar a confiança dos usuários dessa tecnologia “Portanto, é fundamental pensar em soluções de segurança da informação para IoT para que as empresas e consumidores obtenham os benefícios da Internet das Coisas sem correr seus riscos.” (CARVALHO, 2020).

Ecossistemas de TI (Tecnologia da informação) são locais onde grande quantidade de informações são trocadas por consumidores, indústrias e empresas, fato esse em conformidade com o período atual da era digital, sendo assim alvos atraentes para hackers. Um alto risco são câmeras de segurança e localização dos dispositivos de IoT para usuários e privacidade de dados. “Em termos de escalabilidade, quanto mais dispositivos estiverem conectados à rede, maior será o risco de exposição aos hackers como alteração das informações pessoais e comerciais, sequestro ou roubo de dados etc.

Pensando do ponto de vista da segurança da informação, muitas indústrias e empresas deixam brechas de segurança, tais como: Ausência de criptografia; Autenticação insuficiente ou fraca; Interface da Web insegura; Configurações de segurança com falhas; Interface móvel; Nuvem inseguras (SENA, 2015).

Os usuários com o intuito de blindarem seus tráficos de dados devem obter produtos em empresas com padrões de segurança e atualização de sistemas e dispositivos pois menciona-se que “Os cibercriminosos podem encontrar uma forma de explorar informações em vários pontos de um ecossistema de IoT” (KASPERSKY, 2021.).

O conceito de SI (Sistema da informação) está fortemente relacionado a proteção de um grupo de informações que buscam preservar o valor que estas possuem para uma pessoa ou organização. Como complemento a essa definição, sendo os principais aspectos de segurança da informação definidos pela tríade da Confidencialidade, Integridade e Disponibilidade (HARRIS, 2010). Confidencialidade visa garantir que somente quem deve acessar a informação de fato acesse a mesma. Integridade tem o intuito de garantir que a informação acessada realmente está correta, integra, não foi modificada ou alvo de fraude/falsificação. Disponibilidade visa garantir que a informação possa ser obtida sempre que for necessário, assim, estando sempre disponível para quem necessite fazer uso da mesma.

O princípio que gera a privacidade em SI e a confidencialidade, onde segundo (Sêmola 2014) menciona: Toda informação deve ser protegida de acordo com o grau de sigilo de

seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada.

Como fundamentação da SI temos o conjunto de normas da família ISO 27000 que traz diversos conceitos a fim de se obter uma maior segurança das informações através de um Sistema de Gestão de Segurança da Informação (SGSI) para uma organização. As normas são referências de segurança trazendo consigo uma série de controles, boas práticas e um conjunto de mecanismos para garantir contínua de revisão e melhoria nos processos de negócios a fim de evitar percas para uma companhia (Oliveira *et al*., 2016).

Conforme Santos *et al*. (2016), a IoT pode prover diversas classes de serviços, dentre elas, destacam-se os serviços de identificação, responsáveis por mapear entidades físicas (de interesse do usuário), entidades virtuais (EV) como, por exemplo, a temperatura de um local físico, coordenadas geográficas e serviços de agregação de dados que coletam e sumarizam dados obtidos dos objetos inteligentes, entre tantos outros segmentos.

A aplicação de segurança de informação em IoT tem muitos pontos positivos que ajudam a proteger os dados e garantir a privacidade dos usuários. Alguns dos principais benefícios incluem: proteção de dados sensíveis: A segurança de informação é crucial para proteger dados sensíveis, como informações financeiras, de saúde e de identificação pessoal. Ao aplicar medidas de segurança apropriadas em dispositivos IoT, é possível garantir que esses dados sejam protegidos contra acesso não autorizado e vazamento. Prevenção de ataques: A segurança de informação também ajuda a prevenir ataques cibernéticos, como vírus, *malware* e *phishing*, que podem comprometer a integridade dos dados e causar danos significativos. Garantia de privacidade: A privacidade é uma preocupação importante para os usuários de IoT, e a aplicação de medidas de segurança apropriadas pode ajudar a garantir que as informações pessoais sejam protegidas contra uso não autorizado. Confiança dos consumidores: Ao aplicar medidas de segurança de informação em dispositivos IoT, as empresas podem aumentar a confiança dos consumidores e melhorar sua imagem de marca. Isso é importante, especialmente quando se trata de dispositivos IoT que armazenam dados sensíveis. Melhoria da eficiência: Além de proteger os dados, a segurança de informação também pode melhorar a eficiência do sistema IoT. Por exemplo, a implementação de medidas de segurança pode ajudar a garantir que os dados sejam transmitidos de maneira segura e confiável, o que pode melhorar a eficiência geral do sistema (HABIB, 2021).

Em resumo, a aplicação de segurança de informação é crucial para garantir a privacidade dos usuários e proteger dados sensíveis em dispositivos IoT. Além disso, pode ajudar a prevenir ataques cibernéticos, aumentar a confiança dos consumidores e melhorar a eficiência do sistema.

É comum por parte dos fabricantes o alto investimento em poder de processamento e conectividade com baixo nível de segurança na IoT. Dessa forma, o dispositivo se torna mais suscetível a invasões de *hackers*. Isso porque existe a possibilidade de acesso e gerenciamento de microfones, câmeras de segurança e localização desses produtos. Manter os *hackers* longe do ambiente IoT é um dos grandes desafios da segurança da informação a ser vencido, devido aos diversos gargalos existentes. Dentre elas, as mais presentes nesses dispositivos são: a ausência de criptografia, autenticação insuficiente ou fraca, Interface da Web insegura, configurações de segurança com falhas e nuvens inseguras (CARVALHO, 2021).

“Por meio da capacidade de monitoramento inteligentes de processos, ambientes e pessoas, é possível o maior controle sobre as operações de maquinários, por exemplo. Os relatórios gerados indicam o nível de desempenho das atividades aos gestores” (CASTRO;

GOMES, 2019).

O mundo vem avançando cada dia mais em tecnologia. Uma infinidade de aparelhos digitais, ganham lugar de destaque em na vida pessoal e profissional das pessoas cotidianamente um alto índice de conexão tanto em ambientes corporativos e quanto em ambientes domésticos diante disso, há um cenário positivo que possibilita a melhoria nos negócios, proporcionando mais qualidade aos clientes, como até a criação de novos serviços e modelos de negócios.

IoT (Internet das Coisas) é algo recente comparado ao uso da computação, com diversas aplicações, porém temos diversas restrições, existentes na mesma, como exemplo a segurança da informação, por ser um meio interconectado, pode ter inúmeros riscos agregados a questão da privacidade do usuário, integridade dos dados, controles de acesso, capacidade, resistência a ataques, entre outros. Alguns dos problemas mencionados estão são pertinentes a falta de padronização quanto a arquitetura utilizada para IoT.

Com a popularização da Internet das Coisas (IoT), surgem constantemente novas soluções para garantir a segurança dos dispositivos e dos dados transmitidos. Alguns exemplos já aplicados incluem: Autenticação de usuário: para evitar o acesso não autorizado aos dispositivos, é comum a implementação de uma autenticação de usuário, seja por meio de senhas, códigos de segurança ou até mesmo biometria.

Criptografia: a criptografia é fundamental para garantir a privacidade dos dados transmitidos entre os dispositivos. Alguns exemplos de algoritmos de criptografia utilizados incluem AES, RSA e Elliptic Curve. Firewall: é comum a implementação de firewalls em dispositivos de IoT para bloquear acessos indesejados de fontes externas. Atualizações de software: para corrigir vulnerabilidades e garantir a segurança dos dispositivos, é importante realizar atualizações regulares do software. Certificados digitais: os certificados digitais são uma forma de verificar a autenticidade de dispositivos e evitar ataques de phishing. Monitoramento de segurança: alguns dispositivos de IoT possuem mecanismos de monitoramento de segurança para detectar comportamentos anômalos e alertar os usuários em caso de ameaças.

Esses são apenas alguns exemplos de medidas de segurança aplicadas em dispositivos de IoT. É importante destacar que, apesar de essas medidas serem eficazes, a segurança de um dispositivo de IoT depende de sua implantação e configuração corretas. Portanto, é fundamental investir em treinamentos e capacitações para garantir a segurança dos dispositivos em IoT.

A segurança da informação em IoT é aplicada em uma variedade de dispositivos, incluindo: câmeras de segurança inteligentes, termostatos inteligentes, dispositivos de automação residencial, roupas inteligentes, saúde wearables, carros conectados, entre outros. Alguns dispositivos também incluem recursos de segurança como criptografia de dados, autenticação de usuários, atualizações de software seguras e detecção de ameaças.

Existem vários tipos de *hardware* que podem ser utilizados para implementar segurança em IoT, incluindo: Dispositivos de criptografia: Como cartões de segurança, dispositivos de *hardware* de criptografia (HSM) e unidades de proteção de chaves (KMUs). *Firewalls*: Para controlar o tráfego de entrada e saída de dispositivos de IoT e protegê-los contra ameaças. Sensores de segurança: Para monitorar atividades suspeitas e detectar intrusões em tempo real. Dispositivos de autenticação: Como leitoras de impressão digital e reconhecimento facial para autenticar usuários.

Dispositivos de monitoramento de rede: Para monitorar o tráfego de rede e detectar anomalias ou atividades maliciosas. Gateways de IoT seguros: Para garantir a segurança

dos dados transmitidos entre dispositivos de IoT e a nuvem. Estes são alguns exemplos, mas existem muitas outras opções disponíveis no mercado, cada uma com suas próprias vantagens e desvantagens. É importante escolher o hardware certo para sua implementação, levando em consideração as necessidades específicas de segurança do seu sistema IoT.

Como fundamentação, ao da SI temos o conjunto de normas da família ISO 27000 que traz diversos conceitos afim de se obter uma maior segurança das informações através de um Sistema de Gestão de Segurança da Informação (SGSI) para uma organização .As normas são referências de segurança trazendo consigo uma série de controles, boas práticas e um conjunto de mecanismos para garantir continua de revisão e melhoria nos processos de negócio a fim de evitar percas para uma companhia (Oliveira *et al*., 2019).

VPN (Virtual Private Network) criado em estrutura da internet é um circuito virtual (não existe fisicamente), é como um túnel exclusivo de transferência de dados e toda a comunicação é encriptada de forma que agentes externos não consigam enxergar o conteúdo das mensagens que trafegam no mesmo (KUROSE; ROSS, 2013, p. 718). É um recurso de baixo custo pois pode aproveitar a estrutura física já existente da Internet tornando uma opção adotada em grande escala por organizações e governos.

A VPN pode prover os requisitos da CIA-triad, isto é, a integridade, a disponibilidade e a confidencialidade, entretanto não garante o anonimato até pelo fato de que não é criada com este fim. Alguns serviços de VPN (pagos ou gratuitos) prometem a não divulgação dos dados de acesso de usuários, mas apenas o fato da existência do cadastro é um ponto negativo na questão do anonimato. Este banco de dados está sujeito à invasão, fornecimento de informações por informações por força de Lei, entre outras possibilidades (JUNIOR, 2018).

Igualmente ao HTTP que é combinado com o TLS (*Transport Layer Security*) com objetivo de obter segurança nas trocas de mensagens, o CoAP é combinado com o DTLS (*Datagram Transport Layer Security*), para obter segurança semelhante à presente na Web. Assim como existem restrições de memória e processamento para os protocolos de comunicação, as ferramentas de segurança também sofrem com as mesmas limitações. Algoritmos complexos, que ocupam muita memória, ou arquivos relacionados à segurança, como certificados armazenadores de chaves, não são suportados por muitos dispositivos de IoT, que necessitam de abordagens eficientes para obterem segurança em suas atividades. Uma solução seria implementar criptografia a partir de um gateway de saída da rede. Assim, a transmissão de dados entre sensores ocorreria sem criptografia e um gateway usaria técnicas clássicas de segurança - RSA (*Rivest-Shamir-Adleman*), AES (*Advanced Encryption Standard, Diffie-Hellman* e certificados - para transmissão segura (JOHANN, 2018).

Existem vários códigos e protocolos de segurança utilizados em IoT, alguns dos mais comuns são: SSL/TLS: Este é um protocolo de segurança padrão para comunicações seguras na web. É amplamente utilizado em IoT para criptografar dados transmitidos entre dispositivos e servidores. 802.11i: Este é um padrão de segurança Wi-Fi que oferece criptografia de dados e autenticação de usuários. É amplamente utilizado em IoT para garantir a segurança de dispositivos sem fio. *Bluetooth Low Energy* (BLE): Este é um padrão de segurança de baixo consumo de energia para dispositivos sem fio que oferece criptografia de dados e autenticação de usuários. OAuth: Este é um protocolo de autorização aberto que permite aos usuários conceder permissões limitadas a aplicativos e serviços sem compartilhar suas senhas.

É amplamente utilizado em IoT para autenticação de usuários e acesso a dados. Zi-

gBee: Este é um padrão de comunicação sem fio para IoT que oferece criptografia de dados e autenticação de dispositivos. Estes são alguns dos códigos e protocolos de segurança mais comuns utilizados em IoT. No entanto, é importante ter em mente que a segurança de IoT é uma preocupação contínua e novos desenvolvimentos são feitos constantemente para melhorar a segurança destes dispositivos.

> A Intel oferece recursos básicos de segurança para ajudar a proteger aplicações de IoT, investindo em quatro categorias de segurança fundamentais, uma delas é a integridade da plataforma que mitiga a adulteração, aproveitando a raiz de hardware da proteção baseada na confiança de firmware, código e dados críticos da plataforma. A proteção aprimorada para dados, chaves e ID oferece opções integradas e discretas para credenciais resistentes à adulteração. Também oferece aceleração de criptografia e geração de chaves seguras para maior eficiência e desempenho geral e uma execução confiável que estabelece uma proteção baseada em hardware para ambientes de execução de aplicativos ou cargas de trabalho com recursos compartilhados (CARVALHO, 2021).

Tendo em vista verificar a sobrecarga de mecanismos criptográficos simétricos na camada de aplicação da IoT, os autores Quincozes *et al*. 2021 propõem estudo que envolve os protocolos CoAP e MQTT. O estudo é dirigido ao uso de cifras simétricas ao invés de cifras assimétricas, uma vez que, segundo os autores, aquelas possuem custo computacional e energético mais adequado para dispositivos com recursos limitado. Desse modo, algoritmos como o *Tiny Encryption Algorithm* (TEA), *Data Encryption Standard* (DES) e *Advanced Encryption Standard* (AES) foram avaliados através de experimentos práticos disponibilizado publicamente. Os resultados demonstram que o mecanismo TEA é uma boa opção em termos de uso de memória, *CPU*, consumo energético, tempo de resposta e dados recebidos/enviados. No entanto, ressaltasse que algoritmos como o TEA e o DES estão na lista de cifras não recomendadas por órgãos internacionais, como o *National Institute of Standards and Technology* (NIST) (*of Standards and Technology* 2014).

Por outro lado, os resultados revelaram que a adoção do algoritmo AES, tanto para o protocolo CoAP quanto para o protocolo MQTT, implicou em maiores sobrecargas em termos de consumo energético e de tempos de resposta, entre outras métricas avaliadas. No entanto, o AES é uma cifra forte e recomendada pelo NIST. De forma geral, ataques a sistemas de informação ferem a propriedades de segurança como a autenticidade, integridade, disponibilidade, confidencialidade, entre outras (TANENBAUM; WETHERALL, 2011). Por exemplo, ataque de negação de serviço, do inglês, Denial-of-Service (DoS) afeta a disponibilidade dos sistemas. Já o ataque da interceptação afeta o sigilo das mensagens. Dessa forma, os trabalhos da literatura propõem mecanismos e arquitetura a fim de mitigar ataques em favor da garantida das propriedades citadas anteriormente (QUINCOZES; VAGNER, 2021)

3. CONCLUSÃO

Em conclusão, este trabalho teve como objetivo geral realizar uma revisão de literatura sobre segurança da informação em IoT. Os resultados obtidos apontam que a segurança em IoT é um desafio complexo e que exige a implementação de medidas efetivas para garantir a proteção das informações. A revisão identificou que as principais vulnerabilidades em IoT estão relacionadas à falta de autenticação, criptografia fraca, falta de atualizações de software e hardware e à falta de conscientização dos usuários.

Embora a pesquisa tenha alcançado seu objetivo geral, algumas limitações devem ser consideradas. A revisão se baseou em artigos selecionados em bases de dados eletrônicas, o que pode ter limitado a compreensão de alguns aspectos do tema. Além disso, as limitações da própria tecnologia IoT, como a falta de padronização, também foram um desafio para a pesquisa.

Como recomendações para estudos futuros, sugere-se a realização de pesquisas empíricas para avaliar a eficácia das medidas de segurança em IoT, além de estudos que explorem novas abordagens para garantir a privacidade e segurança das informações em dispositivos IoT.

Em resumo, a revisão de literatura sobre segurança da informação em IoT mostrou que o tema é de extrema importância e que a implementação de medidas de segurança efetivas é essencial para garantir a proteção das informações. O estudo contribui para a compreensão do assunto e para a conscientização da necessidade de se investir em segurança em IoT.

Referências

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.**

AL-HAMADI, Hamid et al. Attack and defense strategies for intrusion detection in autonomous distributed IoT systems. **IEEE Access**, v. 8, p. 168994-169009, 2020.

ARATA, Estefânia, et al., segurança da informação para aplicações iot–Internet of things. **South American Development Society Journal**, Disponível em: <http://www.sadsj.org/index.php/revista/article/view/362/323>, Vol.:06, N°.: 18, p. 1/16, dezembro, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Local: ABNT, Ano.

BARDELLA, M. S.; OLIVEIRA, J. P. S. Segurança em IoT: conceitos, desafios e propostas. **Revista Eletrônica de Sistemas de Informação**, v. 15, n. 2, p. 1-18, 2016.

CARVALHO, A. P. Segurança em Internet das Coisas (IoT): uma revisão sistemática da literatura. **Revista de Informática Teórica e Aplicada**, v. 27, n. 1, p. 73-84, 2020.

CARVALHO, André, et al., **Segurança em IoT**, Artigo, https://dspace.uniceplac.edu.br/bitstream/123456789/1610/1/Andr%c3%a9%20Ferreira%20Almeida%20de%20Carvalho_%20Christyan%20Matteus%20Lima%20Santos_Lucas%20Vaz%20Gon%c3%a7alves.pdf, Bacharelado em Sistemas de Informação, Gama-DF, p.:2/18, 2021.

CASTRO, R. C. L.; GOMES, H. E. IoT e segurança da informação: um estudo sobre vulnerabilidades e desafios. In: **Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, 2019.

HABIB, Sami J. et al. An expert system for low-power and lossy indoor sensor networks. **Expert Systems**, v. 38, n. 4, p. e12650, 2021.

KASPERSKY. **Internet das coisas: o que é IoT?** 2021. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-iot. Acesso em: 10 mai 2023.

KUROSE, J.; ROSS, K. **A top-Down Approach**. Computer Networking, p. 284, 2013.

JUNIOR, Dorival, **Segurança da informação**: uma abordagem sobre proteção da privacidade em internet das coisas, Tese Doutorado em tecnologias da inteligência e Designer digital, São Paulo, p. 1/159, 2018.

LI, Shaohua et al. SecGrid: A secure and efficient SGX-enabled smart grid system with rich functionalities. **IEEE Transactions on Information Forensics and Security**, v. 15, p. 1318-1330, 2019.

MOURA, A. C. A.; RAMOS, R. R.; MOURA, F. L. P. Segurança em IoT: uma análise dos desafios e das soluções propostas. In: **Anais do XXIII Workshop sobre Segurança de Informações e Sistemas Computacionais**, 2019.

PAUL, Anup Kumar; QU, Xin; WEN, Zheng. Blockchain–a promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues. **Peer-to-Peer Networking and Applications**, v. 14, n. 5, p. 2926-2951, 2021.

OLIVEIRA, Nairobi, et al., **Segurança da Informação para Internet das Coisas (IoT):** uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD), https://sol.sbc.org.br/journals/index.php/reic/article/view/1704,-vol.:17,N°:04,p.1/14, Novembro, 2019.

QUINCOZES, Vagner, Et al., **desvendando a Camada de Aplicação na Internet das Coisas:** Teoria, Prática e Tendências, Cap. 7, p. 250, Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/78/338/595-.

RODRIGUES, R. N. Segurança da informação em Internet das Coisas (IoT): um estudo sobre as vulnerabilidades e os desafios. **Revista de Tecnologia da Informação e Comunicação**, v. 10, n. 2, p. 1-14, 2020.

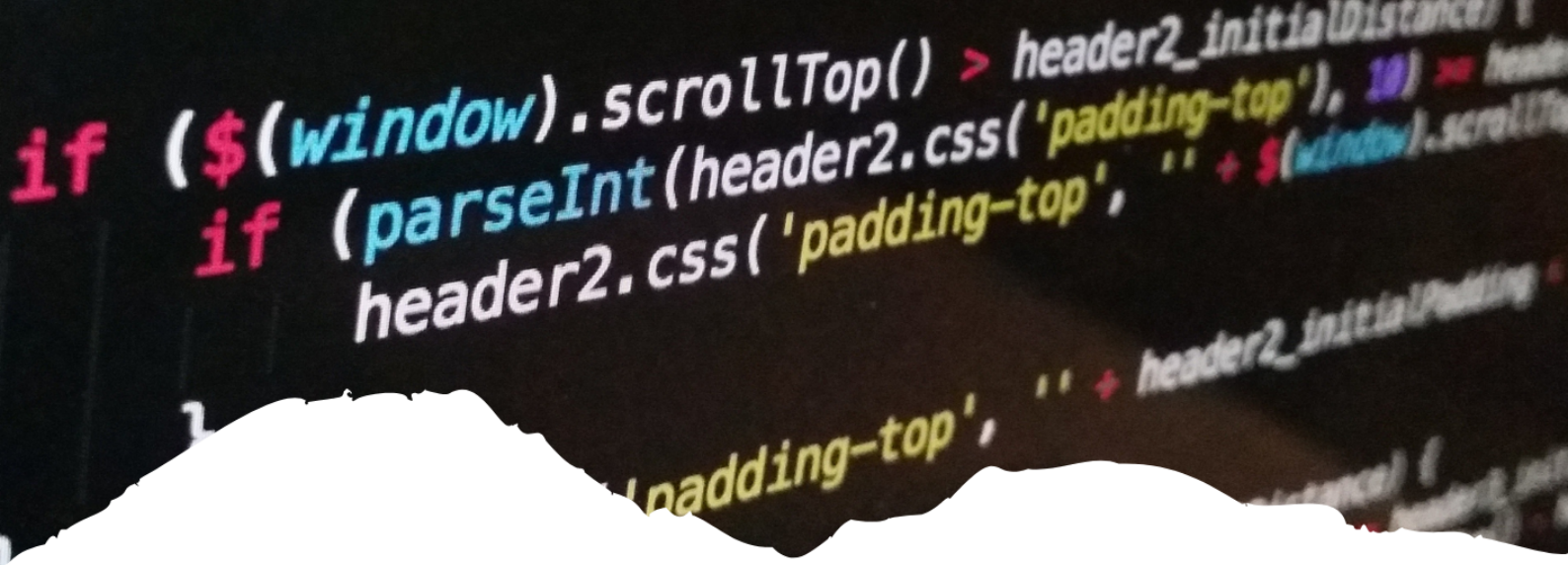
SANTOS, A. S.; SILVA, L. H.; PIMENTA, T. C. Segurança em IoT: estudo de caso em dispositivos de monitoramento residencial. In: **Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, 2017.

SENA, Eduardo Antônio de. **Fog Computing como arquitetura de rede distribuída para internet das coisas**. 2015.

SILVA, F. R.; MARTINS, E. G.; OLIVEIRA, J. P. S. Segurança em Internet das Coisas (IoT): uma revisão sistemática da literatura. In: **Anais do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, 2017.

WESTPHALL, J. **Desenvolvimento de uma Aplicação com dispositivo IoT usando Protocolos DTLS CoAP** (https://repositorio.ufsc.br/bitstream/handle/123456789/192164/Monografia_Johann_Westphall.pdf?sequence=1&isAllowed=y), TCC Bacharel em Ciências da Computação, SC, P.:1/95, 2018.

ZHANG, Qing; XU, Dilong. Security authentication technology based on dynamic Bayesian network in Internet of Things. J**ournal of Ambient Intelligence and Humanized Computing**, v. 11, n. 2, p. 573-580, 2020.



29

SEGURANÇA FÍSICA E LÓGICA DA INFORMAÇÃO EMPRESARIAL

PHYSICAL AND LOGICAL SECURITY OF BUSINESS INFORMATION

Stefano Gleydson Santos Penha

Mirian Nunes de Carvalho Nunes

Lilian Barros Santiago

Resumo

As empresas possuem informações extremamente valiosas, um bem ativo fundamental para o funcionamento da mesma, que devem ser protegidas com toda segurança possível. Com base nessa premissa esta pesquisa discorre sobre a segurança física e lógica da Informação Empresarial. Apresentou-se o seguinte questionamento como ponto de partida para investigação dessa segurança: como proporcionar segurança física e lógica das informações confidenciais de uma empresa? Para tanto determinou-se os seguintes objetivos: investigar a importância do sistema de informação para o ambiente empresarial; identificar as vulnerabilidades físicas e lógicas de sistemas de informação em empresas; classificar melhorias em sistemas físicos e lógicos em empresas. A pesquisa foi realizada por meio de revisão bibliográfica, qualitativa e descritiva, em sites como Google Acadêmico, SciElo em artigos, livros e dissertações a respeito do título encontrado nos últimos dez anos. Com base na pesquisa realizada, destacou-se a necessidade de as organizações implementarem medidas eficazes para garantir a proteção de seus dados e sistemas. Apresentou-se as principais ameaças à segurança física e lógica da informação, com ênfase em ataques de *malware, phishing*, entre outras, assim como a importância de uma abordagem holística para a segurança da informação, que envolve uma combinação de medidas técnicas, políticas e de conscientização dos funcionários. Por fim, elencou-se a necessidade de atualização constante das medidas de segurança, para acompanhar as evoluções das ameaças e novas tecnologias que surgem no mercado.

Palavras-chave: Segurança. Informação. Prevenção. Dados. Empresa.

Abstract

Companies have extremely valuable information, a fundamental asset for the operation of the same, which must be protected as safely as possible. Based on this premise, this research discusses the physical and logical security of Business Information. The following question was presented as a starting point for investigating this security: how to provide physical and logical security of confidential information of a company? For that, the following objectives were determined: to investigate the importance of the information system for the business environment; identify the physical and logical vulnerabilities of information systems in companies; classify improvements in physical and logical systems in companies. The research was carried out through a bibliographical, qualitative and descriptive review, on sites such as Google Academico, SciElo in articles, books and dissertations regarding the title found in the last ten years. Based on the research carried out, the need for organizations to implement effective measures to ensure the protection of their data and systems was highlighted. The main threats to the physical and logical security of information were presented, with emphasis on malware attacks, phishing, among others, as well as the importance of a holistic approach to information security, which involves a combination of technical measures, policies and of employee awareness. Finally, the need for constant updating of security measures was listed, in order to keep up with the evolution of threats and new technologies that appear on the market.

Keywords: Security. Information. Prevention. Data. Company.

1. INTRODUÇÃO

A segurança física e lógica da informação são dois aspectos cruciais para garantir a proteção de dados e sistemas em empresas e organizações. A segurança física envolve medidas de proteção para as instalações físicas como desktops, notebook, servidores entre outros que abrigam dados e sistemas, como controle de acesso, monitoramento de segurança, atividades e backup de dados. Já a segurança lógica refere-se a medidas de proteção contra ameaças virtuais, como hackers e vírus, incluindo senhas fortes, criptografia de dados e atualizações regulares de software. Ambos os aspectos são igualmente importantes e devem ser implementados para garantir a proteção adequada da informação. A falta de medidas de segurança pode levar a violações de dados e informações confidenciais, prejudicar a reputação da empresa e causar prejuízos financeiros e legais.

As informações contidas em uma empresa, são um bem extremamente valioso, um bem ativo fundamental para o funcionamento da mesma, onde esses dados precisam ser protegidos com toda segurança possível. Assim, o intuito deste trabalho consiste em apresentar políticas de segurança física e lógica para tecnologia da informação.

Com a atualização e o desenvolvimento tecnológico e a utilização de maiores instalações, a infraestrutura de TI e as comunicações tornaram-se mais complexas, a ponto de ser necessário reciclar equipes e métodos mais seguros para um bom funcionamento. A proteção de um sistema tornou-se uma ferramenta de trabalho essencial para as empresas, deixando o compartilhamento de dados uma prática moderna, que traz mais agilidade na comunicação e no processo.

Nesta era digital, a segurança física e lógica da informação é uma preocupação cada vez mais importante para empresas e organizações, pois a quantidade de informações armazenadas e compartilhadas eletronicamente cresce a cada dia. Por isso, é essencial que empresas e organizações levem a segurança física e lógica da informação a sério e implementem medidas de proteção adequadas para garantir a privacidade, confidencialidade, integridade e disponibilidade dos dados e sistemas.

Empresas investem principalmente em controles técnicos para reduzir o risco de incidentes de segurança da informação, mas esquecem que o elemento humano é um dos principais contribuintes para falhas de segurança. Uma política de segurança da informação é necessária para definir o que são boas práticas, normas e comunicar o foco e a visão da empresa para o uso dos recursos tecnológicos. Para manter um ambiente onde seus dados estejam protegidos, são necessárias regras e regulamentações que impeçam a divulgação de informações confidenciais e muito sensíveis, como arquivos de áudio, imagem, vídeo e voz.

A segurança física da informação refere-se à proteção dos ativos físicos que armazenam informações, como servidores, dispositivos de armazenamento, equipamentos de rede e outros dispositivos. A segurança física da informação envolve medidas de proteção para prevenir ou minimizar riscos como roubo, vandalismo, incêndios, falhas de energia, terremotos, entre outros.

Diante do exposto o artigo relata sobre “Segurança Física e Lógica Da Informação Empresarial”, com o fim de ajudar empresas. Para nortear o trabalho questionou-se o seguinte problema: como proporcionar segurança física e lógica das informações confidenciais de uma empresa? Para chegarmos a uma resposta, os objetivos são: investigar a importância do sistema de informação para o ambiente empresarial; identificar as vulnerabilidades fí-

sicas e lógicas de sistemas de informação em empresas; classificar melhorias em sistemas físicos e lógicos em empresas.

A segurança da informação é um tema cada vez mais relevante na sociedade moderna. Com a crescente digitalização dos dados, a necessidade de garantir a integridade, confidencialidade e disponibilidade das informações torna-se ainda mais crítica. A segurança da informação engloba diversos aspectos, como a segurança física e lógica, que serão abordados neste artigo científico.

2. DESENVOLVIMENTO

2.1 Metodologia

A metodologia utilizada neste trabalho foi a pesquisa bibliográfica, qualitativa e descritiva, utilizando-se de artigos, livros e dissertações a respeito do título deste artigo, com um objetivo geral de propor estratégias para evitar ataques cibernéticos, vazamentos de dados e ataques físicos em empresas de grande e pequeno porte, mostrando os melhores métodos a serem usados para que essa segurança seja exercida com sucesso. Para se chegar aos resultados desta pesquisa, fez-se uma minuciosa busca por autores a respeito do tema proposto, como: Bazzotti e Garcia (2000), Ferro e Neto (1999), Freitas (2009), Leite (2018), Spanceski (2004).

2.2 Resultados e Discussão

As informações contidas em um sistema de rede de uma empresa, podem ser vulneráveis a alguns ataques de hackers, assim necessita-se que algumas medidas de segurança física e lógica sejam tomadas, visando a proteção de dados, evitando sérios prejuízos.

A informática sempre foi vista como ferramenta de melhoria, porém, quando se fala em Segurança da Informação, alguns aspectos são notados de forma negativa no processo, tais como aumento de custos, perda de liberdade, aumento de complexidade, perda de desempenho, dentre outros. É primordial que haja medição e controle da eficiência e da eficácia dos serviços de tecnologia da informação. Também não se pode deixar de lado a otimização dos custos na obtenção do resultado final. Contudo “não se nega que a proteção dos ativos informacionais custa dinheiro e que a segurança naturalmente traz restrições” (FREITAS, 2009, p.17 e 18).

Segundo Leite (2018), a informação é um recurso cujo valor é inteiramente determinado pelo usuário e só há perda quando não tem o devido cuidado, é um recurso que deve ser gerenciado de forma correta e consciente, onde o objetivo da informação é garantir que uma empresa atinja seus objetivos por meio do uso eficiente de recursos, incluindo pessoas, tecnologia, finanças, história e a própria informação, normalmente, esses dados devem ser mantidos e guardados em sigilo.

Leite (2018), ainda alerta que o roubo de dados, não acontece apenas com empresas, mas com pessoas físicas também, inclui redes sociais, spots de relacionamento, compras online, troca de conversas confidenciais entre outros. Percebe-se, portanto, a importância da segurança física dos equipamentos de rede que ajuda a proteger equipamentos e ativos de infraestrutura, que muitas vezes representam algo de valor para a organização e devem ser protegidos e monitorados, sendo necessário estar atento aos problemas de acesso, infraestrutura predial, elétrica e monitoramento, sendo a maioria dos casos con-

centrada em data centers, locais estratégicos, contendo equipamentos de rede interna, que garante uma boa comunicação de empresas e sistemas.

Dessa forma ressalta-se que a segurança lógica, tem como objetivo a forma de como um sistema é protegido seja por regras ou softwares para controle de acesso. Normalmente é utilizada para proteção de ataques e vulnerabilidades, também serve para proteger sistemas de erros não intencionais e a remoção acidental de dados. Para isso são implementados processos tecnológicos como *firewalls*, antivírus, políticas de segurança entre outros necessários para proteção do usuário (LEITE, 2018, p. 15).

De acordo com o que discorremos a respeito da segurança física e lógica das informações, percebeu-se a importância de ambas tanto para empresas como para pessoas físicas, por meio de métodos efetivos, garantindo uma proteção de qualidade aos seus usuários.

A segurança da informação é um tema crítico para empresas e indivíduos, e a segurança física e lógica da informação são elementos fundamentais para garantir a integridade, confidencialidade e disponibilidade das informações. É importante que as empresas implementem medidas de segurança física e lógica da informação para prevenir ou minimizar riscos de perda de dados ou de invasões virtuais. As empresas devem ter políticas de segurança da informação claras, bem definidas e atualizadas, além de treinamentos regulares para seus funcionários, para garantir a segurança da informação em todos os níveis.

Bazzotti e Garcia (2000) falam que os processos de desenvolvimento através dos sistemas de informação atingem toda a sociedade, sendo assim, todos inclusive as empresas tendem a se encaixar no modelo proposto para que se mantenham no ambiente competitivo do mercado.

Esse modelo é chamado 'Era da informação', a qual é necessário ter em mente a tecnologia de informação e os sistemas de informação como grandes precursores e responsáveis pelo valor adicional às tomadas de decisões. Através dos canais de informação as organizações definem de onde serão adquiridos os dados, e as redes de comunicação definem para onde os dados serão direcionados. Para a formação dos sistemas e a consequente obtenção dos elementos fundamentais para a tomada de decisão é necessário o conhecimento dos conceitos de dados, informação e conhecimento (BAZZOTTI, GARCIA, 2000, p. 02).

O processo de crescimento tecnológico e o aquecimento da economia, o aumento da disponibilidade de crédito e o acesso a novos mercados estão entre os fatores que melhoram significativamente a competitividade das grandes e pequenas empresas, para manter esse nível ou continuar crescendo, grande e pequenas empresas e grandes organizações precisam gerenciar adequadamente seus recursos adquiridos. Um dos caminhos mais comuns é adotar uma solução de sistema de gestão empresarial. Nessa perspectiva, é importante ressaltar que,

> As pequenas e a médias empresas têm seus dados armazenados, geralmente, em servidores de rede ou em estações compartilhadas, e o acesso físico a estes equipamentos nem sempre é restrito. Na maioria das vezes, esse mesmo servidor ou estação possui acesso liberado e ilimitado à Internet, o que aumenta o risco de um incidente de segurança. Na média empresa, o cenário é menos problemático, porém não o ideal, principalmente, devido à conscientização dos funcionários sobre segurança da informação. O controle de acesso aos recursos de TI, equipamentos para fornecimento ininterrupto de energia e firewalls são algumas das formas de se gerir a segurança desta camada (NETTO; SILVEIRA, 2007, p.379).

A segurança lógica refere-se à proteção de dados por meio de medidas técnicas, como criptografia, autenticação, firewalls, controle de acesso, auditoria de logs, entre outras. Essas medidas são implementadas em sistemas e redes de computadores para proteger a integridade, confidencialidade e disponibilidade dos dados.

Já a segurança física refere-se à proteção dos recursos físicos da empresa, tais como os equipamentos de TI, os dados armazenados fisicamente e as instalações em que esses recursos são mantidos. A segurança física é alcançada por meio de medidas de controle de acesso físico, como fechaduras, câmeras de vigilância, cercas, sistemas de alarme, entre outras.

Ambos os aspectos da segurança da informação são importantes para garantir que os dados permaneçam protegidos contra ameaças externas e internas. As ameaças externas podem incluir *hackers*, vírus de computador, *malware* e outras formas de ataques cibernéticos. As ameaças internas podem incluir funcionários mal-intencionados, negligência, erro humano, entre outros.

A integração de medidas de segurança lógica e física é essencial para proteger efetivamente os dados de uma organização. É importante que as empresas implementem políticas e procedimentos claros para a segurança da informação, treinem seus funcionários para garantir a conformidade e monitorem continuamente suas redes e sistemas para detectar e responder rapidamente a ameaças em potencial.

Conhecendo sobre a importância tanto da segurança lógica, como a física, faz-se necessário apresentar métodos, onde as empresas podem utilizar seus equipamentos ligados em uma rede com mais segurança, evitando roubo de dados e possíveis ataques.

Segundo Spanceski (2004), planejar uma segurança eficaz em um sistema de rede, não é uma tarefa fácil, pois envolve um conjunto de conhecimentos de segurança, ambiente de rede, organização, cultura, pessoas e tecnologia, sendo uma tarefa muito trabalhosa, onde envolve muitas pessoas de diferentes funções, que vai do executivo até a recepcionista, no entanto, a maior dificuldade será em fazer cumprir essa política criada, todos os funcionários devem entender a política, entender as regras e procedimentos que são estabelecidos para que todos os funcionários a cumpram de fato.

> O planejamento da política deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. A política de segurança pode ser dividida em vários níveis, podendo ser de um nível mais genérico, como o objetivo que os executivos possam entender o que está sendo definido, nível dos usuários de maneira que eles tenham consciência de seus papéis para a manutenção da segurança na organização, e podendo ser de nível técnico que se refere aos procedimentos específicos como, por exemplo, a implementação das regras de filtragem do firewall (SPANCESKI, 2004, p. 34 e 35).

Ao desenvolver a política, devem ter como participantes integrantes de recursos humanos, gerentes e profissionais em segurança da informação. Esta equipe preparará o documento oficial, fará uma análise profunda e aprovará assim que concluída, bem como atribuirá as funções a membros da equipe que garantirão que as regras sejam aplicadas. Uma política de segurança da informação protege a empresa e o usuário caso ocorra alguma violação de informação, para que ambos tenham recursos e meios legais na justiça.

Toda PSI (Política de Segurança da Informação), não deve ficar restrita apenas ao setor de tecnologia da informação, deve estar ligada diretamente a visão, missão e metas

de negócio institucionais, onde seu conteúdo, pode variar de empresa para empresa, por motivos de cada instituição ter informações e prioridades diferentes, além do grau e maturidade dos usuários (LEITE, 2018). A partir desse desafio,

> [...] uma organização que queira ter eficácia na proteção de suas informações, deve buscar convergir esses dois tipos de segurança, a lógica e a física dentro de seu sistema. Não basta somente instalar câmeras de monitoramento e logo após não armazenar estes dados para um futuro acesso do conteúdo. Como também não é suficiente, por exemplo, controlar o acesso externo de pessoas à organização se por vezes os próprios funcionários da empresa podem causar algum incidente de segurança. É necessário unir as duas formas de controle, podendo assim evitar possíveis ataques, ou até mesmo corrigir e detectar outras ameaças (REGO, 2011, p.20).

Além de todos esses métodos de segurança citados, que podem ser utilizados para garantir uma proteção eficaz nos equipamentos ligados a uma rede, podem também ser de grande valia outras ações para que o mesmo aconteça, como palestras de conscientização, sinalizações, lembretes em redes sociais da empresa, e-mails, entre outros. No quadro 1 apresenta-se exemplos de controle de segurança física e lógica da informação, e verifica-se métodos eficazes para garantir êxito na segurança das informações empresariais.

MECANISMOS QUE PERMITEM O CONTROLE DA SEGRANÇA FÍSICA E LÓGICA DA INFORMAÇÃO	
Autorização e Autenticação	Mecanismo que controla e fornece permissão para os indivíduos autorizados acessaram os sistemas de informação, onde através desse processo, se pode ter a certeza de que o usuário realmente é quem está dizendo ser.
Firewall	Mecanismo para proteger as fontes de informação de um sistema, controlando o acesso entre a rede interna segura da unidade e as redes externas não confiáveis, o mesmo é programado para evitar e relatar a qualquer momento algum tipo de ameaça ao sistema de informação das empresas.
Detector de intrusos	O IDS (Intrusion Detection System) é o mecanismo que busca e procura prováveis intrusões indesejadas na rede, sendo principal fonte de pesquisa de detector de intrusos são as auditorias, reconhecendo comportamentos padrões ou ações intrusivas recorrentes.
Criptografia	Mecanismo que permite descrever mensagens codificadas e cifradas, usado para autenticar a identidade de usuários, proteger as comunicações feitas dentro da rede e manter a integridade durante a transferência e troca de informações, permitindo que haja troca de mensagens privadas, ou seja, somente o emissor e o receptor da mensagem terão acesso ao conteúdo da mensagem, fazendo criptografia de ponta a ponta.
Assinatura digital	Mecanismo que consiste na criação de um código pelo emissor de uma mensagem, por meio de uma chave privada, permitindo ao remetente identificar através de uma chave pública, ou seja, do próprio emissor, se o mesmo realmente é quem diz ser.
Redes Privadas Virtuais	A VPN (Virtual Private Networks), são redes compostas por “túneis” de criptografia em pontos autorizados, criadas usando a própria Internet ou outras redes (públicas ou privadas) para a transferência de informações de maneira segura entre as redes internas corporativas ou usuários remotos.

Infraestrutura de Chaves Públicas (ICP)	Mecanismo de segurança baseada em tecnologia para estabelecer e garantir a confiabilidade de chaves públicas de criptografia, este mecanismo atrela as chaves públicas as suas entidades, possibilitando que outras entidades verifiquem a validade das chaves públicas, podendo ser feito assim um sistema distribuído.

Quadro 1: Exemplo de controle de segurança física e lógica da informação

Fonte: Rego (2011, p.20,21,22,23).

Cada um desses mecanismos é fundamental para prevenir ameaças cibernéticas e garantir a confidencialidade, integridade e disponibilidade dos dados. É crucial que as organizações implementem uma abordagem abrangente de segurança da informação e sigam as melhores práticas para assegurar a proteção adequada de seus ativos de informação.

As empresas devem estar atentas a diversas ameaças que podem comprometer a segurança lógica de suas informações, com isso é muito importante ficar atento as seguintes orientações segundo descreve Santos e Sott (2023):

1. Uma das principais ameaças são os vírus, que podem danificar ou alterar sistemas e informações. Para evitar esse tipo de problema, é importante ter um antivírus configurado corretamente e sempre atualizado. Além disso, é fundamental ter cuidado com e-mails e programas baixados na internet, pois podem conter vírus.
2. Outra ameaça é o risco de perda de informações devido a incêndios. Para evitar esse tipo de problema, é preciso ter equipamentos anti-incêndio adequados e um local seguro, de fácil acesso ao corpo de bombeiros e longe de locais com objetos explosivos.
3. Investir em treinamento para os funcionários, para que possam manusear equipamentos com segurança e evitar perda de informações.
4. As senhas também merecem atenção especial, pois muitos funcionários acabam deixando-as anotadas em papéis ou arquivos de texto no computador. Para evitar esse tipo de problema, é importante não deixar senhas escritas em papéis sobre a mesa, fazer a troca periódica das senhas e utilizar caracteres variados, como letras, números e símbolos. As senhas são pessoais e intransferíveis e nunca devem ser passadas a outras pessoas.
5. O lixo também pode ser uma fonte de vulnerabilidade, por isso, o que não for mais utilizado pela empresa deve ser inutilizado antes de ir para o lixo. Os papeis podem ser queimados ou picotados em vários pedaços e jogados em diferentes lixeiras. Já os cartões de memória, pen drivers CDs, DVDs e HD antigos devem ser destruídos ou inutilizados.
6. Por fim, é importante evitar o uso indevido dos serviços de internet em nome da empresa e investir em programas de bloqueio de acesso a sites e programas desnecessários para os funcionários. Além disso, é fundamental utilizar *firewalls* configurados e atualizados para evitar invasões de pessoas mal-intencionadas nos sistemas da empresa. Medidas de segurança como políticas de segurança podem ajudar a evitar ou resolver problemas, caso seja necessário.

De acordo com as dicas mencionadas, percebemos diferentes aspectos da segurança da informação e a importância de proteger os dados de uma empresa. Foi destacado algumas das principais ameaças à segurança, como vírus, incêndios, funcionários sem treinamento, senhas fracas, uso indevido da internet em nome da empresa e invasões. Além disso, observamos as dicas práticas para melhorar a segurança lógica da empresa, como a

instalação de antivírus atualizado, a proteção contra incêndios, o treinamento de funcionários, o uso de senhas seguras, a proteção do lixo e o uso de firewall.

3. CONCLUSÃO

Concluiu-se, portanto, que a segurança das informações empresariais requer uma abordagem dupla, com a segurança física e lógica trabalhando juntas. A segurança física visa controlar o acesso físicos às informações por meio de equipamentos e ferramentas, enquanto a segurança lógica protege as informações digitais por meio de criptografia e controle de acesso.

A convergência dessas duas formas de segurança é crucial para garantir uma proteção eficiente das informações, e é importante que a organização implemente medidas adequadas de segurança, como cartões de acesso e biometria, para garantir a confidencialidade, disponibilidade e integridade das informações. Proteger as informações empresariais é um tema sério que requer atenção e comprometimento constante da organização

Referências

BAZZOTTI, C.; GARCIA, E. A importância do sistema de informação gerencial na gestão empresarial para tomada de decisões. **Ciências Sociais aplicadas em revista**, *[S. l.]*, v. 6, n. 11, 2000. Disponível em: https://saber.unioeste.br/index.php/csaemrevista/article/view/368. Acesso em: 31 out. 2022.

FERRO, Derival Alves; NETO, Mário Ferreira. **A Importância do sistema integrado de gestão empresarial para as instituições privadas ou públicas**. http://www. cpgls. pucgoias. edu. br/8mostra/Artigos/SOCIAIS% 20APLICADAS/A% 20IMPO RT% C3% 82NCIA% 20DO% 20SISTEMA% 20INTEGRADO% 20DE% 20GEST% C3% 83O% 20EMPRESARIAL% 20PARA% 20AS% 20INSTITUI% C3, v. 87, p. C3, 1999.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação**. Acesso em, v. 13, 2009..

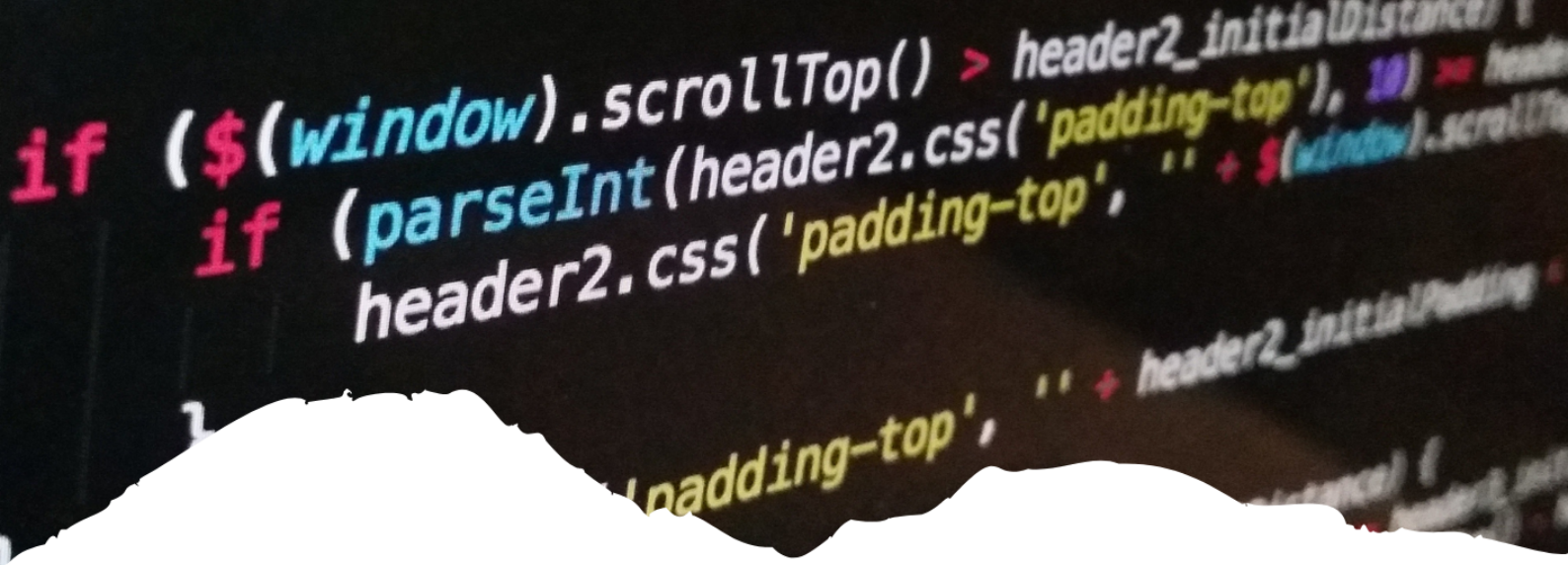
LEITE, Luciano Monteiro. **Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos**. 2018. 33 f. Trabalho de Conclusão de (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná, Curitiba, 2018.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, p. 375-397, 2007.

REGO, Hugo Bauer. **A importância da Segurança da informação para os sistemas de automação**. 2011.

SANTOS, Ronan Leandro Coelho dos; SOTT, Mário Rubens W. **Aspectos da Segurança da Informação**: Sua Importância para as Organizações.2023.

SPANCESKI, Francini Reitz. **Politica de segurança da informação–Desenvolvimento de um modelo voltado para instituições de ensino**. Monografia do Trabalho de Conclusão de Curso em Sistemas de Informação, 2004.



30

A ROBÓTICA USADA COMO TRATAMENTO DO AUTISMO (TEA)

ROBOTICS USED AS AUTISM TREATMENT (ASD)

Hanani Santos Teixeira

Resumo

A complexidade do Transtorno do Espectro Autista e sua possível aparência levaram ao desenvolvimento durante a última década de um método de intervenção muito promissor: os robôs assistidos por terapia. O desenvolvimento tecnológico e os resultados promissores dos estudos realizados sobre o assunto, juntamente com a recente incorporação robótica no contexto educacional, fazem com que nós contemplemos a viabilidade de introduzir este método de intervenção no contexto educacional. O presente estudo demarca os últimos avanços deste método a partir da contribuição de especialistas e analisa as consequências positivas que os robôs sociais podem ter para o tratamento do transtorno do espectro autista. Este artigo também propõe discutir sobre como a área da robótica pode ser um meio de auxílio e uma ótima ferramenta para ajudar a tratarem o transtorno do espectro autista – Tea no que se refere a usar a robótica, como forma de interação e socialização com a pessoa em questão, sendo assim uma ótima ferramenta de aprendizado, desenvolvimento e interação social

Palavras-chave: Autismo. Robô social. Intervenção. Educação. Recurso.

Abstract

The complexity of Autism Spectrum Disorder and its possible appearance led to the development during the last decade of a very promising intervention method: therapy-assisted robots. Technological development and the promising results of studies carried out on the subject, together with the recent incorporation of robotics in the educational context, make us contemplate the feasibility of introducing this method of intervention in the educational context. The present study marks the latest advances of this method based on the contribution of experts and analyzes the positive consequences that social robots can have for the treatment of autism spectrum disorder. This article also proposes to discuss how the field of robotics can be a means of assistance and a great tool to help treat autism spectrum disorder - Tea in terms of using robotics as a way of interacting and socializing with the person. in question, thus being a great tool for learning, development and social interaction

Keywords: Autism. Social robot. Intervention. Education. Resource.

1. INTRODUÇÃO

O Transtorno do Espectro Autista, doravante TEA, é caracterizado por uma condição do neurodesenvolvimento que causa um prejuízo significativo e persistente no domínio da comunicação social, juntamente com padrões restritos e repetitivos de comportamento, atividades ou interesses, tudo isso faz com que as pessoas com esse transtorno percebam a realidade de uma forma diferente, dificultando sua conexão com o ambiente e fazendo com que seu desenvolvimento seja significativamente alterado. Pode a robótica auxiliar no ensino e aprendizagem de pessoas com TEA?

O objetivo é apresentar os avanços da engenharia e da robótica combinando-os para oferecer uma alternativa no tratamento de crianças e adultos com TEA: a terapia assistida por robô é um método de intervenção que, segundo vários autores e

Estudos que serão detalhados nas próximas seções, estão apresentando resultados muitos bons no tratamento de pessoas com TEA, pois têm grande afinidade com brinquedos mecânicos principalmente robôs. A tecnologia robótica possui objetivos claros em relação ao desenvolvimento do autismo, pois desenvolve a sua motricidade fina, a concentração, observação e criatividade, estimulando a organização de ideias de maneira mais conveniente. A robótica estimula também o trabalho em equipe e a troca de ideias, focando na interação entre os participantes, no desenvolvimento da autoconfiança e da autoestima, estabelecendo conceitos de criação de novas ideias, além de ser interdisciplinar e multidisciplinar, pois foca na elaboração de projetos com outras disciplinas.

A escolha do tema e da pesquisa ressalta a importância que a robótica e os avanços tecnológicos possam gerar benefícios e melhorar a qualidade de vida de crianças e adultos diagnosticados com essa síndrome, além de estimular o desenvolvimento social e comunicativos assim como aprimorar a sua capacidade de aprendizado e de solucionar problemas.

2. A ROBÓTICA SOCIAL

Os robôs sociais, também conhecidos como “robôs socialmente interativos”, “artefatos relacionais” ou “brinquedos robóticos” têm sido enquadrados em situações sociais de interação entre um indivíduo e um robô em contextos lúdicos, educativos e terapêuticos. Um protótipo desse tipo de dispositivo é o Furby (FERNAEUS et al., 2010). Portanto, entendemos robô social como: Robôs para atividades básicas de lazer, como brincadeiras, criatividade, aprendizado, entretenimento e relaxamento. (...) são brinquedos interativos e possuem um componente de software, o que os distingue de outros mecanismos ou artefatos de baixa tecnologia (FERNAEUS et al., 2010). A diferença básica entre um robô social e qualquer outro brinquedo, ferramenta ou instrumento é sua interação com o ambiente. Ao contrário de outros dispositivos, os robôs sociais são projetados para interagir diretamente com o mundo ao seu redor (BREAZEAL, 2009; FERNAEUS et al., 2010;) como Diclstein-Fischer e Ficher (2014) indicam, “eles são projetados com a intenção de se comunicar e interagir com os seres humanos.

Segundo Dautenhahn (2007), os robôs sociais ou interativos apresentam uma série de características: expressam e/ou percebem emoções, comunicam-se por diálogo de alto nível ou por comunicação não verbal, reconhecem outros agentes, estabelecem ou mantêm relações sociais, usam sinais naturais (aparência, gestos etc.), tem personalidade ou caráter

distinto e pode aprender ou desenvolver habilidades sociais. A presença dessas características em maior ou menor grau são diferentes em cada robô. Juan Carlos Cruz e Yeliza Andrea Salazar (2014) apontam que uma das grandes vantagens desses dispositivos é que eles podem ser programados para responder a diferentes situações e podem aprender e mudar a maneira como respondem ao mundo. Assim, suas respostas e interações tornam-se mais sofisticadas e isso permite que a motivação e a atenção da criança aumentem. No entanto, poucos estudos foram realizados sobre o efeito a longo prazo dos benefícios desse tipo de terapia e alguns autores apontam que isso pode levar à falta de apego humano (TANAKA; KIMURA, 2009).

O uso de robôs na terapia é limitado pelo grande custo envolvido e pela falta de disponibilidade desses dispositivos, que normalmente ficam restritos ao ambiente clínico ou privado (ALEXANDER et al., 2011). No entanto, alguns desses robôs foram recentemente comercializados a um custo moderadamente acessível e isso possibilitaria a expansão desse tipo de terapia para outras áreas, como a educação. Esses robôs surgem de uma tendência robótica recente denominada robótica de assistência social, uma subárea da robótica que visa projetar robôs para ajudar e atender às necessidades especiais de pessoas com dificuldades sociais, físicas ou de interação (BERNIER et al., 2012). Atualmente, está sendo investigado o uso de tais robôs como ferramenta para a prática de habilidades sociais, treinamento de empatia, ensino de idiomas ou em terapias comportamentais (AUYEUNG et al., 2012). São cada vez mais utilizados na reabilitação, terapia e educação (CASTIELLO et al., 2008).

Eles também têm sido investigados como uma ferramenta de apoio para pessoas de idade avançada ou com déficits físicos, como acidente vascular cerebral e paralisia parcial das extremidades (BERNIER et al., 2012). Além do mais Colton e outros. (2008) indicam que outro grupo da população infantil também poderia se beneficiar do uso de robôs sociais, como crianças com transtorno específico de linguagem (DEL). Esse tipo de terapia permite o surgimento de interações triádicas entre criança, robô e terapeuta que podem desencadear interações sociais entre a criança e o terapeuta (RICKS; COLTON, 2008).

3.TERAPIA COM ROBÔS

Um dos usos mais difundidos de robôs sociais que está sendo estudado atualmente é a terapia em pessoas com TEA. Segundo Paola Pennisi et al. (2015) crianças com autismo mostram uma clara atração por sistemas tecnológicos. A esse respeito, autores como Juan Carlos Cruz e Yeliza Andrea Salazar (2014) acrescentam que “as crianças autistas têm grande afinidade com brinquedos mecânicos, principalmente robôs. A previsibilidade do comportamento repetitivo e monótono do robô é o fator reconfortante que torna as crianças autistas altamente atraídas por robôs.” Por esse motivo e por outros, acredita-se que seja um método viável para o tratamento desse tipo de distúrbio. Conforme indicado por Paola Pennisi et al. (2015) “A robótica social pode ser um método promissor para o tratamento de transtornos do espectro do autismo (ASD)”. Esta afirmação é corroborada por Gideki Kozima, Cocoro Nakagawa e Yasuda (2005) no seu estudo realizado com o Keepon, um robô a que nos referiremos mais adiante, no qual asseguram que as crianças com TEA apresentavam expressões faciais que nem os indivíduos mais próximos da criança ambiente que eles tinham visto antes e até desenvolveram comportamentos pró-sociais em relação ao robô.

As plataformas robóticas são um método particularmente interessante para interagir com crianças com autismo, pois as estimula a abandonar seu mundo introspectivo e as

convida a responder aos estímulos produzidos pelo robô (CRUZ SALAZAR, 2014). Alguns fatores que tornam os robôs sociais um meio ideal para terapia de TEA são: sua simplicidade, sua adaptabilidade comportamental a diferentes cenários e sua capacidade de oferecer uma interação esperada e mais simples (AKHTAR et al., 2012). Além disso, Ueyama (2015) sustenta que esses robôs encorajam crianças com TEA a tomar a iniciativa e estimular respostas emocionais. Em suma, o uso desses robôs é usado para ajudar crianças com TEA a se comunicar, interagir, reconhecer emoções e desenvolver sua competência social (UEYAMA, 2015) treinando o olhar compartilhado e a atenção conjunta, aprimorando a imitação e troca de turnos, ensinando habilidades faciais e emoções corporais, e iniciar interações sociais (BARAKOVA, 2011).

A maioria dos estudos realizados até agora foi realizada em ambientes laboratoriais ou institucionais como parte de programas educacionais ou terapêuticos específicos (FERNAEUS et al., 2010). Os benefícios da robótica para interação social foram demonstrados em estudos de caso de três ou quatro crianças, mas há poucos estudos em larga escala (DIEHL et al., 2012 citado por BERNIER et al., 2013). Pennisi et al. (2015) realizou uma revisão dos diferentes estudos sobre o tema realizados até o momento. Em questões de desempenho de crianças com TEA em condições humanas ou com o robô, os autores refletem que até o ano de 2015, 13 estudos indicam melhores desempenhos em relação ao robô do que a um agente humano. Além disso, durante o jogo, o contato visual e tátil, a manipulação, a postura e a produção verbal foram melhores nas sessões com o robô.

Segundo os mesmos autores, foram realizados dezesseis estudos que analisaram o comportamento social: oito deles mostraram que o robô pode ser um estímulo melhor que um humano para a melhoria dos comportamentos sociais, quatorze indicam que crianças com TEA apresentam comportamentos sociais em relação ao robô e nove determinaram melhores resultados quando o robô atuou como mediador. Os mesmos autores indicam que três dos quatro estudos que analisam a melhora da linguagem com esse tipo de terapia corroboram que o robô promove a melhora da linguagem. Os autores apontam que, em termos de imitação nesse tipo de terapia, quatro mostraram que crianças com TEA melhoram a imitação se forem usados robôs. De fato, em um dos estudos realizados com 24 participantes com TEA, foi demonstrada a melhora das habilidades de linguagem na interação triádica (KIM et al., 2013; citado por PENNISI et al., 2015).

Todos os estudos que Pennisi et al. (2015) mostram que os robôs podem ser bons motivadores e ajudar a atrair a atenção das crianças para a tarefa (LEE; TAKEHASHI; NAGAI; OBINATA et al., 2012; LEE; OBINATA, 2013; WAINER et al.,

2010; WAINER et al. 2014; YEE et al., 2012. YIN et al., 2013). Como resultado dos diferentes estudos realizados, foram desenvolvidos diferentes projetos que utilizam a robótica. Um deles é o Projeto Robota que tem como foco a pesquisa de desenvolvimento de brinquedos robóticos educativos e investiga a possibilidade de utilizar o robô para avaliar a capacidade de imitação de crianças e ensinar-lhes comportamentos simples (COSTA et al., 2010). Outro dos projetos que enfoca o possível uso de robôs para ajudar pessoas com problemas de comunicação a adquirir e/ou manter suas competências e habilidades de comunicação é o Communication-Care Project (KOZIMA; NAKAGAWA; YASUDA, 2005). Outro dos projetos em funcionamento é a terapia LEGO que utiliza a ferramenta LEGO Mindstrom que segundo Cruz e Salazar (2014) é muito eficaz para trabalhar com crianças com TEA.

Além disso, os mesmos autores descrevem outros projetos em desenvolvimento, como IROMEC, KEEPOM ou layROB, além do Projeto AURORA que analisaremos posteriormente devido à sua ligação com o ambiente educacional. As implicações positivas do

uso desses dispositivos para a terapia do autismo são inúmeras (PENNISI et al., 2015; CABIBIHAN et al., 2013). Uma das grandes vantagens oferecidas pela terapia assistida por robô é que ela permite que indivíduos com TEA se conectem com o ambiente de maneira mais fácil (PENNISI et al., 2015; DAUTENHAHN, 1999). Laurie Dickstein-Fischer e Gregory S. Fischer (2014) acrescentam que estes podem aumentar as possibilidades de interação social com outros agentes humanos. Além disso, ao contrário de outros programas e aplicativos virtuais, o robô permite uma interação multimodal de forma natural através de gestos, expressões, contato etc. o que os torna ainda mais atrativos (CABIBIHAN et al., 2013). Cristina A. Costescu, Daniel O. David e Bram Vanderbroght (2015) afirmam que crianças com TEA parecem gostar mais da tarefa de interagir com o robô do que um adulto. Além disso, Ueyama (2015) defende que o uso de robôs melhora a participação de crianças com TEA durante a terapia e que a interação com o robô não é desconfortável para elas, pois foi observado que a resposta emocional a esses dispositivos melhora em relação à interação com humanos.

3.1 Vantagens e desvantagens da terapia com robôs

Uma das grandes vantagens oferecidas pela terapia assistida por robô é que ela permite que indivíduos com TEA se conectem com o ambiente de maneira mais fácil (PENNISI et al., 2015**;** DAUTENHAHN, 1999). LaurieDickstein-Fischer e Gregory S. Fischer (2014) acrescentam que estes podem aumentar as possibilidades de interação social com outros agentes humanos. Além disso, ao contrário de outros programas e aplicativos virtuais, o robô permite uma interação multimodal de forma natural através de gestos, expressões, contato etc. o que os torna ainda mais atraentes (CABIBIHAN et al., 2013). Cristina A. Costescu, Daniel O. David e Bram Vanderbroght (2015) sustentam que crianças com TEA parecem gostar mais da tarefa de interagir com o robô do que um adulto. Além do mais, Uyama (2015) defende que o uso de robôs melhora a participação de crianças com TEA durante a terapia e que a interação com o robô não é desconfortável para elas, pois foi observado que a resposta emocional a esses dispositivos melhora em relação à interação com humanos. Além do mais, Paola Pennisi e cols. (2016) indicam que algumas implicações positivas do uso desses dispositivos são que crianças com autismo reagem melhor a um robô do que a um agente humano e reduzem comportamentos estereotipados e repetitivos. Além disso, os robôs provocaram um grande número de comportamentos sociais por parte das crianças com autismo e melhoraram a linguagem espontânea das crianças com TEA durante as sessões. Como qualquer outra ferramenta, os robôs sociais também apresentam desvantagens, Os estudos realizados até agora são muito limitados e é necessário esclarecer se os benefícios ocorrem apenas durante as sessões de terapia ou são generalizáveis para outros contextos (PENNISI et al., 2016). Os robôs podem reforçar a tendência de entrar em comportamentos estereotipados repetitivos (KLJAJEVIC, 2010). A terapia pode ser cara, embora existam robôs no mercado a custo moderado disponíveis para médicos, pais ou professores (ADMONI; MATARICO; SCASSELLATI, 2012). As dificuldades organizacionais e o medo da complexidade técnica de controlar o robô geram desconfiança na hora de implementar esse tipo de terapia (BARAKOVA, 2011).

4. ROBÓTICA SOCIAL EM CONTEXTO EDUCACIONAL

FumihideTanaka e Takeshi Kimura (2009) realizou um estudo em uma sala de educação infantil da Califórnia usando o robô RUBI. A partir do estudo, eles concluíram que o

robô era uma ferramenta muito boa para atrair e manter a atenção das crianças. Aponta ainda que os robôs para educação devem auxiliar e apoiar os professores sob seu controle, enfim, *"é uma* ferramenta para os professores enriquecerem o ambiente educacional*"*. Alguns estudos quantitativos foram realizados em escolas com pequenos humanoides como QRIO e Robivie (TANAKA; KIMURA, 2009). Dois dos projetos que estão sendo realizados atualmente são realizados em ambientes educacionais. Estamos nos referindo ao projeto AURORA e ao projeto Robot4Autism*,* que explicaremos a seguir. O Projeto AURORA é um projeto realizado na Bentfield Primary School no Reino Unido (ROBINS et al., 2004). Como indicado Cruz e Salazar (2014) o projeto investiga o papel terapêutico e educacional que os robôs podem desempenhar para crianças com TEA e usa dois robôs: Robota e Kaspar. O projeto visa ensinar habilidades sociais básicas para crianças com TEA, promovendo o aspecto didático e as relações triádicas. Os objetivos do projeto são ajudar crianças com TEA a se conectarem com o mundo social e estudar a interação humano-robô (DUTENHAHN, 1999). O Robot4Autism se concentra em crianças em idade escolar com TEA e busca trabalhar habilidades sociais relevantes usando robôs humanoides e tablets (NEILON; ROLLINS, 2014). Fumihide Tanaka e Takeshi Kimura (2010) eles estão convencidos do potencial positivo da tecnologia robótica como ferramenta de apoio aos professores para melhorar a qualidade da educação infantil. Kerstin Dautenhahn (1999) já anunciava que máquinas inteligentes humanoides não faziam parte de nossas vidas e que seria um processo longo e difícil. "O equilíbrio entre os benefícios e riscos desta tecnologia é sempre dinâmico" (TANAKA; KIMURA, 2010).

5. CONCLUSÃO

A robótica vem sendo utilizada em diversos estudos multidisciplinares, principalmente no tratamento de pessoas especiais com autismo, e vem contribuindo muito para o desenvolvimento e consequentemente, para a melhoria da qualidade dos autistas. Houve e ainda a grandes avanços no que tange a educação dos mesmos e é possível atualmente verificar que os autistas têm muito interesse pelos robôs e isso gera um facilitador para o avanço nos processos de inclusão deles.

A exploração das capacidades motoras, cognitivas e da segurança ao lidar com robôs faz com que o resultado dos experimentos seja bem-sucedido. Porém, o alto custo dos robôs ainda impossibilita a utilização deles, sendo necessária a criação de políticas que viabilizem o acesso do autista a eles em mais locais, com base nos diversos estudos realizados, é evidente a melhoria da qualidade de vida da criança autista com a utilização de robôs, uma vez que os robôs são previsíveis, simples e de fácil compreensão, desencadeando assim no autista uma maior motivação além de estimular habilidades sociais como contato visual e a imitação.

Assim como nas casas, e nas indústrias o avanço da tecnologia também trouxe praticidade, agilidade e o aumento da produção com a utilização de robôs.

Os robôs autônomos e sociais são capazes de desenvolver tarefas sem a necessidade constante da supervisão humana, uma vez que são equipados com diversos sensores, como câmeras, sensor de proximidade e contato, o que permite perceber o que ocorre em volta e tomar decisões corretamente.

O trabalho apresentou resultados positivos no que diz respeito ao auxílio na socialização de pessoas com Transtorno do Espectro Autista, como resultados paliativos, destacou-se a melhoria na comunicação e interação no convívio familiar, como também maior desempenho nas terapias cotidianas, e diminuição da ida as mesmas, que por sua vez, são

bastante inacessíveis a famílias de baixa renda. Todo o trabalho teve como base a inclusão de crianças com autismo ao dia a dia de outras crianças (não portadoras do TEA), auxiliando em processos sociais e educacionais. Por fim, é importante destacar a necessidade de documentação e máxima divulgação das ações com o intuito de subsidiar outros estudos, bem como novas parcerias com instituições dando um suporte maior as crianças que já utilizam das ferramentas. A terapia para o paciente diagnosticado com TEA trata-se de um desafio, pois é um tratamento integrativo com terapia medicamentosa e intervenções comportamentais individualizadas, objetivando a eficácia para o paciente. Porém, o processo é longo e gradativo para definir corretamente a intervenção personalizada. A terapia robótica é uma via promissora e demonstrou nos estudos preliminares bons resultados. A maioria dos estudos selecionados demonstram a eficiência com o uso de robôs na prática clínica dos indivíduos com TEA, com destaque para amplificação, captação e entendimento dos gestos, importante principalmente em indivíduos não-verbais, a estimulação de compreensão emocional e cognição social, reverberação situacional como ferramenta auxiliar a vocalização, limitação de estereotipias. Contudo, no geral, a quantidade limitada de participantes, a variabilidade da faixa etária, o período curto de tempo e descontinuidade das práticas terapêuticas, por si só não ser suficiente para ajudar as crianças com o reforço social, ao estimular o prazer mútuo e motivação social. Apesar da idade destoante ser comum, o ideal seria implementar terapias quanto mais cedo para se expor resultados promissores, muitas crianças com pouca idade aparentam gostar da tecnologia robótica, contribuindo como facilitador das pesquisas e tratamento.

Referências

ADMONI, H.; MATARIC, M.; SCASSELLATI, B. Robots for Use in Autism Research. **Annual Review of Biomedical Engineering**, v. 14, p. 275-294, 2012. doi: 10.1146/annurevbioeng-071811-150036.

AHLUWALIA, A. et al. Realistic Humanlike Robots for Treatment of ASD, Social Training, and Research; Shown to Appeal to Youths with ASD, Cause Physiological Arousal, and Increase Humanto-Human Social Engagement. Association for Computing Machinery. **The 5th ACM International Conference on PErvasive Technologies Related to Assistirem Environments**, 2012.

AKHTAR, F. et al. Humanoid Robot NAO Interacting with Autistic Children of Moderately Impaired Intelligence to Augment Communication Skills. **International Symposium on Robotics and Intelligent Sensors** 2012, p. 1533-1538, 2012. doi: 10.1016/j.proeng.2012.07.346.

ALEXANDER, E. el al. An Affordable Compact Humanoid Robot for autism Spectrum Disorder Interventions in Children. **Engineering in medicine and Biology Society (Ed.). 33rd Annual International conference of the IEEE EMBS**, p. 5319- 5322, 2011. doi: 10.1109/IEMBS.2011.6091316.

AUYEUNG, Bonnie et al. Prenatal versus postnatal sex steroid hormone effects on autistic traits in children at 18 to 24 months of age. **Molecular autism**, v. 3, p. 1-5, 2012.

BARAKOVA, E. Robots for social training of autistic children. Empowering the therapists in intensive training programs. **IEEE (Ed.), Information and Communication Technologies (WICT)**, 2011 World Congress on. 2011. p. 14-19. doi: 10.1109/ WICT.2011.6141197.

BERNIER, E. et al. Social Robots as Embedded Reinforcers of Social Behavior in Children with Autism. **Journal Autism Dev Disord**, v. 43, p. 1038-1049, 2012. doi: 10.1007/s10803- 012-1645-2.

BREAZEAL, Cynthia. Role of expressive behaviour for robots that learn from people. **Philosophical Transactions of the Royal Society B: Biological Sciences**, v. 364, n. 1535, p. 3527-3538, 2009.

CABIBIHAN, John-John et al. Why robots? A survey on the roles and benefits of social robots in the therapy of children with autism. **International journal of social robotics**, v. 5, p. 593-618, 2013.

COSTESCU, Cristina A.; VANDERBORGHT, Bram; DAVID, Daniel O. Reversal learning task in children with autism spectrum disorder: a robot-based approach. **Journal of autism and developmental disorders**, v. 45, p. 3715-3725, 2015.

CRUZ SALAZAR, Tania et al. **Las pieles que vestimos. Corporeidad y prácticas de belleza en jóvenes chiapanecas**. Universidad de Ciencias y Artes de Chiapas, 2014.

CRUZ, J. C.; SALAZAR, Y. A. *Aplicación robótica para realizar terapias en niños con autismo,* 2014.

DAUTENHAHN, Kerstin. Robots as social actors: Aurora and the case of autism. In: **Proc. CT99, The Third International Cognitive Technology Conference, August, San Francisco**. 1999. p. 374.

DAUTENHAN, K. Social intelligent robots: dimensions of human-robot interaction. **Psicological Transactions of The Royal Society**, v. 362, p. 679-704, 2007. doi: 10.1098/ rstb.2006.2004.

DICKSTEIN-FISCHER, Laurie; FISCHER, Gregory S. Combining psychological and engineering approaches to utilizing social robots with children with Autism. In: **2014 36th annual international conference of the IEEE engineering in medicine and biology society**. IEEE, 2014. p. 792-795.

FERNAEUS, Ylva et al. How do you play with a robotic toy animal? A long-term study of Pleo. In: **Proceedings of the 9th international Conference on interaction Design and Children**. 2010. p. 39-48.

KLJAJEVIC, Vanja. SYNTACTIC DEFICITS IN AUTISM: CAN INTERACTIVE TECHNOLOGIES HELP? SINTAKSIČKI DEFICITI U AUTIZMU: DA LI INTERAKTIVNE TEHNOLOGIJE MOGU POMOĆI?. **Curr Top Neurol Psychiatr Relat Discip. Vol**, v. 18, n. 2, 2010.

KOZIMA, Hideki; NAKAGAWA, Cocoro; YASUDA, Yuriko. Interactive robots for communication-care: A case-study in autism therapy. In: **ROMAN 2005. IEEE International Workshop on Robot and Human Interactive Communication, 2005.** IEEE, 2005. p. 341-346.

LEE, Jaeryoung et al. Which robot features can stimulate better responses from children with autism in robot-assisted therapy?. **International Journal of Advanced Robotic Systems**, v. 9, n. 3, p. 72, 2012.

LEE, Jaeryoung; OBINATA, Goro. Developing therapeutic robot for children with autism: A study on exploring colour feedback. In: **2013 8th ACM/IEEE International Conference on Human-Robot Interaction (HRI)**. IEEE, 2013. p. 173-174.

NEILON, M.; ROLLINS, P. Technology-aided Instruction is now classified as one of the 27 intervention practices for children with autism. 2014.

PENNISI, P. et al. Autism and social robotics: A systematic review. **Autism Research**, v. 9, n. 2, p. 165-183, 2015. doi: 10.1002/aur.1527.

PENNISI, Paola et al. Autism and social robotics: A systematic review. **Autism Research**, v. 9, n. 2, p. 165-183, 2016.

RICKS, Daniel J.; COLTON, Mark B. Trends and considerations in robot-assisted autism therapy. In: **2010 IEEE international conference on robotics and automation**. IEEE, 2010. p. 4354-4359.

ROBINS, Ben et al. Effects of repeated exposure to a humanoid robot on children with autism. In: **Designing a more inclusive world**. Springer London, 2004. p. 225-236.

TANAKA, F.; KIMURA, T. The Use of Robots in Early Education: A Scenario Based on Ethical Consideration. IEEE (Ed.). **The 18th IEEE International Symposium on Robot and Human Interactive Communication**. 2009. p. 558-560. doi: 10.1109/ROMAN.2009.5326227.

WAINER, Joshua et al. A pilot study with a novel setup for collaborative play of the humanoid robot KASPAR with children with autism. **International journal of social robotics**, v. 6, p. 45-65, 2014.

WAINER, Joshua et al. The effectiveness of using a robotics class to foster collaboration among groups of children with autism in an exploratory study. **Personal and Ubiquitous Computing**, v. 14, p. 445-455, 2010.

YEE, Alvin Wong Hong et al. Developing a robotic platform to play with pre-school autistic children in a classroom environment. In: **Proceedings of the Workshop at SIGGRAPH Asia**. 2012. p. 81-86.

YIN, Tzu-Chi; TUNG, Fang-Wu. Design and evaluation of applying robots to assisting and inducing children with autism in social interaction. In: **Universal Access in Human-Computer Interaction. User and Context Diversity: 7th International Conference, UAHCI 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part II 7**. Springer Berlin Heidelberg, 2013. p. 524-533.

Nesta obra os organizadores fazem uma abordagem sobre os temas relacionados a aplicação da Inteligência Artificial, da segurança da informação e o uso da lei geral da proteção de dados. Temas estes que apresentam soluções e o uso de ferramentas para potencializar as atividades e negócios em empresas como o uso da IA e torná-los mais seguros das ameaças da Internet. Os assuntos abordados vêm colaborar com os temas atualmente discutidos nesta área bem como trazer aos acadêmicos, professores e profissionais atuante um excelente material para suas pesquisas e aplicações.

ISBN: 978-65-80751-83-9

Pascal
Editora