

Uma visão abrangente da computação

Organizadores:
Catterina Dal Bianco
Wagner Elvio de Loiola Costa
Roberto Max Louzeiro Pimentel

2022



1
volume

**CATTERINA DAL BIANCO
WAGNER ELVIO DE LOIOLA COSTA
ROBERTO MAX LOUZEIRO PIMENTEL**
(Organizadores)

**UMA VISÃO
ABRANGENTE DA
COMPUTAÇÃO**
VOLUME 1

EDITORA PASCAL
2022

2022 - Copyright© da Editora Pascal

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

Conselho Editorial

Dr. Will Ribamar Mendes Almeida

Dr. Raimundo Luna Neres

Dr. Raimundo J. Barbosa Brandão

Dr. Saulo José Figueredo Mendes

M.Sc. José Ribamar Santos Moraes Filho

Dados Internacionais de Catalogação na Publicação (CIP)

B578u

Coletânea Uma visão abrangente da computação / Catterina Dal Bianco, Wagner Elvio de Loiola Costa, Roberto Max Louzeiro Pimentel (Org). São Luís - Editora Pascal, 2022.

196 f. : il.: (Uma visão abrangente da computação; v. 1)

Formato: PDF

Modo de acesso: World Wide Web

ISBN: 978-65-80751-24-2

D.O.I.: 10.29327/566370

1. Computação. 2. Inteligência artificial. 3. Computação forense. 4. Proteção de dados. I. Bianco, Catterina Dal. II. Costa, Wagner Elvio de Loiola. III. Pimentel, Roberto Max Louzeiro. IV. Título.

CDU: 004::343.98

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores.

2022

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 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

Catterina Dal Bianco

Possui graduação em ENGENHARIA ELÉTRICA pela Universidade Federal do Maranhão (1987). Atualmente é Coordenadora da Faculdade Pitágoras de São Luis dos cursos de Engenharia Elétrica, Engenharia de Controle e Automação e Engenharia da Computação. É Conselheira do Crea-MA, é membro da Câmara Especializada de Engenharia Elétrica (titular), membro da Comissão de Ética Profissional (titular), Membro da Comissão de Educação e Atribuição Profissional - CEAP, membro da Comissão do mérito, membro da Comissão do Crea-Junior (suplente). Tem experiência na área de Engenharia Elétrica, com ênfase em Telecomunicações, atuando principalmente no seguinte tema: gestão de projetos e sistemas de telecomunicações.

Wagner Elvio de Loiola Costa

Possui graduação em Engenharia de Eletricidade pela Universidade Federal do Maranhão (1995) e mestrado em Engenharia Elétrica pela Universidade Federal do Maranhão (2012). Atualmente é técnico laboratório área, classe d, nível 416 da Universidade Federal do Maranhão, professor da Faculdade Atenas Maranhense e professor da Faculdade ISL Wyden São Luis. Tem experiência na área de Ciência da Computação, com ênfase em Arquitetura de Sistemas de Computação, atuando principalmente nos seguintes temas: redes de computadores, segurança e gerenciamento de redes e IoT.

Roberto Max Louzeiro Pimentel

Possui especialização (Lato-Sensu) em Análise e Projeto de Sistemas pela Universidade Federal do Maranhão (2012), graduação em Sistema de Informação pelo Centro Universitário do Maranhão (2005). Tem experiência na área de Ciência da Computação, com ênfase em Sistemas de Computação. Atualmente desenvolve atividades de Gerenciamento de Projetos em Tecnologia da Informação na Secretaria de Estado da Educação do Maranhão.

SUMÁRIO

CAPÍTULO 1.....	8
A RELEVÂNCIA DAS TÉCNICAS E PRINCÍPIOS DA ENGENHARIA DE SOFTWARE PARA O DESENVOLVIMENTO E APERFEIÇOAMENTO CONTÍNUO DE UM SOFTWARE Thiago Sodré Sales	
CAPÍTULO 2.....	21
HUMANOS E ROBÔS: INTELIGÊNCIA ARTIFICIAL Maycon Richard Gomes Silva	
CAPÍTULO 3.....	27
SEGURANÇA EM BANCO DE DADOS Lucas Delgado Freitas	
CAPÍTULO 4.....	40
A INFLUÊNCIA DA INTELIGÊNCIA ARTIFICIAL NA EXPERIÊNCIA DOS USUÁRIOS DE JOGOS ELETRÔNICOS Matheus Guilherme Rocha dos Santos	
CAPÍTULO 5.....	53
SEGURANÇA DA INFORMAÇÃO Alexsandro Pereira Azevedo	
CAPÍTULO 6.....	70
COMPUTAÇÃO FORENSE NO COMBATE AOS CRIMES CIBERNÉTICOS Victor de Souza Pereira Catterina Dal Bianco Ernane Frasão Barbosa	
CAPÍTULO 7.....	80
ANÁLISE DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS Deric Martins Trindade Gonçalves	
CAPÍTULO 8.....	99
INTELIGENCIA ARTIFICIAL: MACHINE LEARNING APLICADO ÀS REDES SOCIAIS Wagner Elias Oliveira Rabelo	

CAPÍTULO 9.....	113
INTELIGÊNCIA ARTIFICIAL EM EVOLUÇÃO INDUSTRIAL Luis Eduardo Silva de Sousa	
CAPÍTULO 10.....	127
ANÁLISE DE DADOS EM BI (<i>Business Intelligence</i>) OPORTUNIDADES NA GESTÃO DE TOMADAS DE DECISÃO E DEFINIÇÃO DE ESTRATÉGICA DE EMPRESAS DO SETOR ATACADISTA José Vinicius Sousa Lemos	
CAPÍTULO 11.....	137
UTILIZAÇÃO DOS SERVIÇOS EM NUVEM NO AMBIENTE EMPRESARIAL, E COMO ELES PODEM AJUDAR NA ACELERAÇÃO E OTIMIZAÇÃO DOS PROCESSOS Hercio Lucas Coelho Goncalves	
CAPÍTULO 12.....	148
APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL Karoline Costa Rodrigues	
CAPÍTULO 13.....	166
SEGURANÇA DE DADOS Nara Virginia Marinho Arraes	
CAPÍTULO 14.....	183
SEGURANÇA EM DATABASE Lucas Evangelista Chaves Junior	

CAPÍTULO 1

A RELEVÂNCIA DAS TÉCNICAS E PRINCÍPIOS DA ENGENHARIA DE SOFTWARE PARA O DESENVOLVIMENTO E APERFEIÇOAMENTO CONTÍNUO DE UM SOFTWARE

*THE RELEVANCE OF SOFTWARE ENGINEERING TECHNIQUES
AND PRINCIPLES FOR THE DEVELOPMENT AND CONTINUOUS
IMPROVEMENT OF A SOFTWARE*

Thiago Sodré Sales¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

Este trabalho é resultante de revisão bibliográfica e um estudo sobre a relevância das técnicas e princípios da engenharia de software para o desenvolvimento e aperfeiçoamento contínuo de um software. E terá também como objetivo abordar as principais técnica e metodologia da engenharia de software. Um bom desenvolvimento e uma boa evolução contínua de um software são de alta importância para permanência de qualquer software no mercado de softwares pagos ou não, muito mais pelo fato de estarem inseridos na grande maioria das áreas do conhecimento humano da sociedade contemporânea e, assim como a sociedade evolui, softwares também devem evoluir da melhor forma possível. Em vista de tudo que foi dito, com o intuito de dar agilidade nos processos de desenvolvimento e evolução e, de garantir maior qualidade para os softwares, surgiu a engenharia de software com suas técnicas e metodologias.

Palavras-chave: Software; Técnicas; Engenharia; Metodologia.

Abstract

This work is the result of a bibliographic review and a study on the relevance of the techniques and principles of software engineering for the development and continuous improvement of software. And it will also aim to address the main technique and methodology of software engineering. A good development and a good continuous evolution of a software are of high importance for the permanence of any software in the market of paid or unpaid software, much more because they are inserted in the great majority of the areas of human knowledge of contemporary society and, as well as society evolves, software must also evolve in the best possible way. In view of all that has been said, in order to speed up the development and evolution processes and to ensure greater quality for the software, software engineering with its techniques and methodologies emerged.

Keywords: Software; Techniques; Engineering; Methodology.



1. INTRODUÇÃO

Devido à inegável importância dos softwares para a sociedade contemporânea, o desenvolvimento e evolução dos mesmos têm crescido muito nos últimos anos. O uso de computadores pessoais, smartphones e vários outros dispositivos digitais crescem exponencialmente a cada dia, pois existe uma crescente demanda por soluções que automatizem os diversos processos das diversas áreas do conhecimento humano.

O desenvolvimento e evolução de software não podem ser confundidos com uma mera programação, pois é o que de fato ocorre muitas das vezes pelos iniciantes da área de desenvolvimento de software, isso pelo fato de estarem evoluindo suas habilidades como desenvolvedores de e ao se depararem com problemáticas mais complexas, uma simples abordagem pessoal centrada pura e basicamente na programação se torna ineficiente e ineficaz.

Em vista de tudo que foi dito, com o intuito de dar maior agilidade nos processos de desenvolvimento e evolução e, de garantir maior qualidade em geral e aumentar a produtividade no desenvolvimento de software cobrindo todas as áreas de suas aplicações e de diversos tipos tais como, portais web, sistemas corporativos, plataformas diversas, ferramentas direcionadas de software e etc., é que surgiu a engenharia de software com suas técnicas e metodologias.

A extrema importância dos softwares tem se confirmado devido a sua ampla difusão e aplicabilidade dos mesmos no cotidiano da sociedade contemporânea. Como garantir confiabilidade, qualidade, menores custos e maior produtividade no desenvolvimento e evolução contínua desses softwares?

Nos capítulos deste trabalho foram apresentados diversos problemas que estão relacionados ao mau desenvolvimento e evolução dos softwares, assim também como as principais metodologias e técnicas da engenharias de software para se alcançar sucesso e grande aproveitamento no desenvolvimento e evolução dos mesmos e, além desses será também expostos fatores importantes dessas técnicas para um ótimo desenvolvimento progressivo dos softwares.

O tipo de pesquisa realizado neste trabalho foi uma revisão de literatura, na qual foram realizadas consultas a livros, dissertações, sites e em artigos científicos que foram selecionados através de busca em bibliotecas e sites acadêmicos. O período dos trabalhos pesquisados compreende publicações dos últimos 15 anos, as palavras-chave utilizadas na busca foram: engenharia de software, técnicas de software, metodologias de software e modelo de software.

2. DEFINIÇÃO E HISTÓRICO DE SOFTWARE

Definido de forma bem direta e resumida software é o conjunto de artefatos e não apenas o código fonte (SOMMERVILLE, 2003), ou seja, uma sequência de instruções lógicas a serem executadas, a fim de modificar, manipular ou redirecionar dados e ou informações, o mesmo pode ser formado por bibliotecas, funções e módulos.

De acordo com Pressman (2006) os softwares possuem categorias, abaixo são algumas que estão dispostas das seguintes formas:

- Software de sistema são programas que apoiam outros programas, como o software que realiza a comunicação com o hardware (sistema operacional) e software que auxilia no desenvolvimento de outro software (compiladores).
- Software de aplicação, são implementados para auxiliar no negócio de uma determinada empresa ou entidade.
- Software científico e de engenharia, são softwares especializados no processamento de números.
- Software embutido são programas desenvolvidos para executarem dentro de produtos bem específicos, como por exemplo, a função de programação de uma geladeira.
- Software de web são aplicações que são executados via Internet utilizando-se um navegador.
- Software de inteligência artificial são softwares que fazem os usos de algoritmos não numéricos, estes tipos de software se encaixam na robótica.

Em 1969 ocorreu um evento que se tornaria o marco inicial da indústria de software, que foi a importante decisão da International Business Machines (IBM) de comercializar o software separadamente dos equipamentos, pois até então o software era tido apenas como parte integrante do equipamento e, sua importância era relativamente muito menor em se comparando com o hardware. Assim o software iria se tornar mais tarde altamente comercializável e, não demorou muito para o surgimento e rápida expansão de empresas especializadas no desenvolvimento e comercialização de softwares.

Inicialmente, como já era de se esperar que, da mesma forma que ocorreu com hardware, o mercado de software se resumia às grandes empresas e órgãos dos governos principalmente devido às suas aplicabilidades e ao elevado custo dos equipamentos que os utilizavam. No entanto com o avanço exponencial das tecnologias o que propiciou o surgimento dos computadores pessoais, microcomputadores e computadores portáteis o que também barateou de forma bem significativa o hardware, as pequenas empresas, médias empresas, escritórios, profissionais liberais e famílias contribuíram fortemente para a crescente expansão e evolução dos softwares.



2.1 Crise do software

A engenharia de software é uma abordagem sistemática e disciplinada para o desenvolvimento de software (PRESSMAN, 2006), esse termo surgiu na década de 1960 e foi utilizado oficialmente em 1968 na NATO Science Committee. Sua criação se deu na tentativa de contornar a crise do software, que foram as grandes dificuldades encontradas em frete de se desenvolver e ou evoluir softwares de qualidade devido ao rápido crescimento da demanda, da complexidade dos problemas a serem resolvidos e da inexistência de metodologias e técnicas para o desenvolvimento desses, de forma que pudessem ser avaliados e que funcionassem adequadamente (ENGHOLM, 2010), e de dar um tratamento de engenharia (mais sistemático, controlado e de qualidade mensurável) ao desenvolvimento de sistemas de software complexos.

As causas da crise do software, termo utilizado nos anos de 1970, estão relacionadas à complexidade do processo de desenvolvimento de software e que ainda na atualidade se manifesta das seguintes formas: Projetos com prazos estourados, projetos com orçamentos estourados, baixa qualidade do software desenvolvido, requisitos não condizentes, projetos que não se pode gerenciar, manutenibilidade impraticável (JALOTE, 2005), dentre outros que serão abordados a seguir.

2.2 Erros no desenvolvimento de softwares

Projetos de software falham quando eles não atendem aos critérios requeridos, a maioria dos projetos ultrapassa o orçamento e muitas vezes ficam aquém das expectativas dos clientes, ou é finalizado antecipadamente não atingindo as metas de desempenho e de qualidade.

Sobre falha de software segundo Lawhorn (2010) aplicações mal definidas (falha de comunicação entre cliente e TI) contribuem para um crescimento de 66% de falha do projeto e, entre 60% a 80% das falhas do projeto podem ser atribuídas diretamente à má coleta de requisitos, análise, e gestão, 50% das falhas são identificadas e tratadas durante o desenvolvimento, 40% dos problemas são encontrados pelos usuários finais, 25% a 40% de todos os gastos em projetos são desperdiçados um resultado de retrabalho e, até 80% dos orçamentos são consumidos consertando falhas ocasionadas.

Os três principais fatores-chave do sucesso de projeto e desenvolvimento e evolução de softwares são entrega no prazo, dentro ou abaixo do orçamento, o software funciona conforme esperado. Poucos projetos alcançam todos os três fatores, a maioria das entregas são feitas com softwares que possuem falhas e um ou mais dos outros critérios apresentados e, um número substancial de entregas de produtos de software são canceladas tendo falhas a tal ponto. Vários fatores estão relacionados a problemas com desenvolvimento de software algumas das razões mais vitais para o fracasso são as seguintes:

2.2.1 Levantamento de requisitos

De acordo com Vazquez e Simões (2016) a extração de requisitos de um produto de software é a primeira tarefa do seu desenvolvimento. Às vezes, o objetivo de um projeto pode se apresentar aparentemente muito simples devido a uma baixa exigência requerida na fase de definição do projeto, muitos projetos têm requisitos de alto nível, mas são apresentados de forma vaga e geralmente inútil, isso leva os desenvolvedores a não ter total capacidade de construir o que eles acreditam ser necessário, pois não possuem conhecimento real do negócio para qual o projeto está sendo desenvolvido. Inevitavelmente, quando o software é entregue, o usuário se depara com um produto de software incapaz de atender suas necessidades como usuários.

Definir requisitos claros e reais para um projeto de software pode demandar uma quantidade de tempo e muita comunicação, mas às vezes metas e objetivos a serem alcançados podem não está tão claro, porque geralmente o cliente não tem a experiência para descrevê-los de forma satisfatória, pois o ideal seria que usuário/clientes fosse capaz de saber o que eles exige o projeto e de especificá-lo claramente, a figura 1 segue como exemplo de falhas na comunicação.

Minha esposa disse:
- Amor, vá ao mercado e compre uma caixa de leite. Se tiver ovos, traga seis.
Eu voltei com seis caixas de leite.
Ela disse:
- Por que você comprou seis caixas de leite?
Respondi:
- Porque eles tinham ovos!

Figura 1 - Piada popular na internet, que ilustra falha na comunicação.

Fonte: Carlos Eduardo Vazquez, Guilherme Siqueira Simões. Engenharia de Requisitos: software orientado ao negócio (2016, p.60)

No entanto, como usuário não é especialista em TI cabe aos desenvolvedores extrair requerimentos através de suas habilidades, experiência e técnicas da engenharia de software.

2.2.2 Falta de envolvimento do usuário

Estudos e pesquisas realizadas por instituições acadêmicas têm apontado que, a falta de apoio atuante e o não envolvimento dos usuários finais nos projetos de software são duas das principais dificuldades na gestão desses projetos, sem envolvimento do usuário o projeto perde qualidade de usabilidade. Segundo Vazquez e Simões (2016) um dos critérios, do sucesso do projeto de software depende do envolvimento dos usuários desde o início do projeto e bem como assim ao longo de todo o desenvolvimento do mesmo. Isto exige tempo e esforço também por parte do usuário final, que muitas vezes não dispõe de tempo para engajar-se em uma nova tarefa dentre as já existentes do seu dia-a-dia de trabalho e que por assim pode achar que o projeto não é alto em suas prioridades. O usuário precisa continuamente apoiar o projeto, o desenvolvedor deve envolver o usuário, pois ajuda na identificação dos requisitos e entrega de todas as funcionalidades bem definidas do projeto de software.

2.2.2.1 Indecisões/Indefinições

Não é incomum haver algumas mudanças nos requisitos de um projeto de software durante o seu desenvolvimento. Quando há restrições de ambiente e a exigência do cliente muda com certa frequência, o desenvolvedor deve seguir a abordagem orientada por componentes enquanto desenvolve o sistema. Novos requisitos ou modificações podem ser tratados separadamente até que possam ser incorporadas ao projeto sem grandes impactos, contudo mudanças descontroladas ou desordenadas podem causar grandes impactos negativos no sistema em desenvolvimento o que pode ocasionar-lhe muitas falhas.

3. METODOLOGIAS DE DESENVOLVIMENTO DE SOFTWARE

Até 1970, o processo de “desenvolvimento de software” era realizado de forma desestruturada. Reflexo de falta de padrão, planejamento e organização que resultavam em produtos que não correspondiam com as reais necessidades dos clientes (PRESSMAN, 2011). A partir de então surgiu a necessidade de tornar o desenvolvimento de software um processo que agregasse planejamento, estrutura e padronização (NETO, 2004). As metodologias tradicionais também amplamente conhecidas como “pesadas” ou guiadas à documentação possuem característica marcante dividir o processo em etapas e/ou fases bem definidas.

Segundo Soares (2004), essas metodologias emergiram de um quadro de desenvolvimento de software muito diferente do que é visto em 2018, com base em mainframes e terminais burros, naquele período o custo alterar/corrigir era muito alto, já que o acesso a esses computadores era limitado e não havia modernas ferramentas de apoio ao desenvolvimento, como analisadores de código e depuradores. Por causa disso, o software precisava ser todo planejado e documentado antes de ser implementado (LUDVIG; REINERT, 2007).

Ainda em 1970 surgiu o primeiro modelo de processo de desenvolvimento de software a ser publicado, derivado de processos mais gerais da engenharia de sistemas (ROYCE, 1970).

O modelo cascata é uma das metodologias de desenvolvimento de software mais tradicionais e comumente usadas para desenvolvimento de software. Este modelo de ciclo de vida é frequentemente considerado como o estilo clássico do desenvolvimento de software, também conhecido como modelo seqüencial linear ou ciclo de vida de software, considera as atividades fundamentais do processo de especificação, desenvolvimento, validação, evolução e representa cada uma delas em fases distintas, porém encadeadas como: especificação de requisitos, projeto de software, implementação, teste e assim por diante, esse modelo esclarece o processo de desenvolvimento de software em um fluxo seqüencial linear, o que significa que qualquer fase no processo de desenvolvimento começa somente se a fase anterior for concluída conforme figura 2.

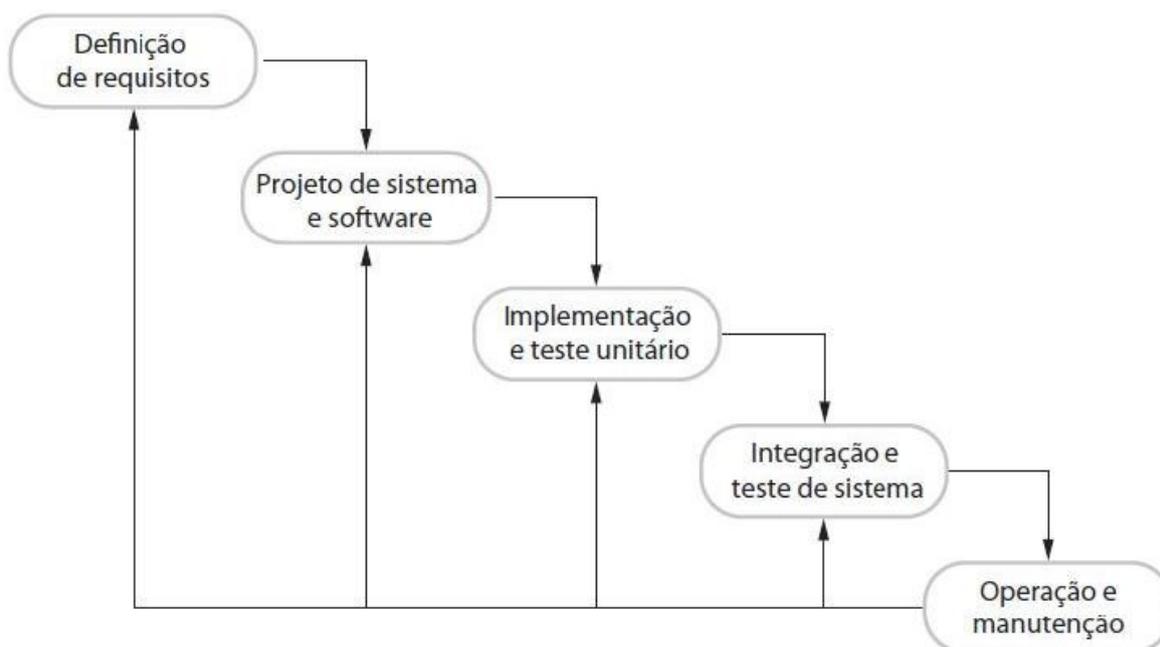


Figura 2: Modelo cascata.

Fonte: Ian Sommerville. Engenharia de Software (2011, p.20)

O modelo funciona com a conclusão e aprovação de cada fase que gera respectivo documento, protótipo do software ou mesmo uma versão do sistema (NETO, 2004). E como dito anteriormente não se deve prosseguir para as etapas seguintes sem finalização das anteriores. Na fase do projeto de sistema os requisitos são levantados; na implementação são investigados problemas do projeto e efetuada a verificação para que cada unidade (módulos) atenda a sua especificação; na integração e teste todas as unidades são integradas e testadas, caso não haja problemas durante a integração são entregues ao cliente; no fim a manutenção e operação suportam a correção dos erros durante o ciclo de vida da aplicação. Entretanto, por conta das mudanças os custos e retrabalho pode levar ao congelamento de partes do processo, como a especificação, e dar continuidade as outras fases, adiando a solução dos problemas e muitas vezes criando outros.

Nos anos seguintes, especificamente anos 80, surgiu o processo de desenvolvimento que trazia consigo várias respostas aos problemas existentes no modelo cascata. O modelo espiral foi proposto por Barry Boehm (1988) e considerado um modelo evolucionário, diferente do seu predecessor que, ao invés de fazer uso de um conjunto atividades seqüenciadas o processo é realizado de forma espiral. Cada volta representa uma fase do processo do modelo e está dividida em quatro partes (SOMMERVILLE 2011).

Usando o modelo espiral, o software será desenvolvido em várias versões, consideradas evoluções da primeira versão já que trazem consigo uma serie de novas funcionalidades antes previstas nas etapas anteriores. Nas primeiras iterações, a versão pode ser um protótipo ou um modelo já nas iterações posteriores são produzidas versões cada vez mais completas do sistema (PRESMAN, 2011).

Barry Boehm sugeriu, em resposta as limitações existentes na abordagem tradicional, que o processo de desenvolvimento poderia ser realizado em uma série de incrementos. O modelo incremental surgiu a partir de uma adaptação do modelo seqüencial linear e assume que o software irá agregar novas funcionalidades. A cada nova funcionalidade ou conjunto de novas funcionalidades será um incremento e seguirá as fases do modelo

linear (PRESSMAN, 2011). O modelo incremental é mais aplicado em projetos de longa duração, nos quais os requisitos de projetos têm alto risco de sofrerem alterações e onde novas funcionalidades são acrescentadas ao longo do tempo, projetos com prazo de entrega é curto. Como existe uma versão estável do produto, o primeiro incremento é frequentemente chamado de núcleo do produto (PRESSMAN, 2011), serve de base para os outros incrementos, o modelo combina características dos fluxos de processos.

O produto é decomposto em um número de componentes, cada um dos quais é projetado e construído separadamente (denominado como builds). Cada componente é entregue ao cliente quando está completo. Isso permite a utilização parcial do produto e evita um longo tempo de desenvolvimento. Ele também cria um grande desembolso inicial de capital com a longa espera subsequente evitada. Este modelo de desenvolvimento também ajuda a aliviar o efeito traumático da introdução de um sistema completamente novo de uma só vez.

A Rational Software desenvolveu o Rational Unified Process (RUP) para ser uma metodologia de alta produtividade e de fácil adaptação, amplamente utilizado por pequenas e grandes equipes de desenvolvimento, por razões de sua natureza configurável. Possui quatro fases distintas no processo de software, no entanto ao contrário do modelo cascata, onde as fases são equilibradas com as atividades do processo, as fases do RUP são rigorosamente relacionadas aos negócios e não a parte técnica. Segundo Sommerville (2011) na fase de concepção o objetivo está em torno de constituir um business case para o sistema, identificando todas as entidades externas que vão de fato interagir com o sistema e suas respectivas interações. Na fase de elaboração o foco é em estabelecer apurada compreensão sobre problema dominante além de desenvolver o plano do projeto e identificar riscos. Durante a fase de construção o projeto é de fato construído e testado, no final, deve ser entregue um sistema funcionando e a respectiva documentação associada. Por fim a fase de transição consiste na transferência da equipe de desenvolvimento para os usuários no ambiente de produção.

Segundo Sommerville (2011), na década de 1980 e início da década de 1990, acreditava-se que a melhor maneira de desenvolver um software era por meio de um planejamento cuidadoso do projeto, com qualidade da segurança formalizada, uso de ferramentas CASE (Computer-aided software engineering) e de um processo de desenvolvimento rigoroso e controlado. Porém essa abordagem, conhecida posteriormente como metodologia tradicional, exige muito tempo e esforço em planejamento, projeto e documentação do sistema e não é adaptada para mudanças. Segundo Brooks (1994), "a principal falha do modelo cascata é que ele assume a construção de todo o sistema de uma só vez" e complementa que a especificação total de um software antes do início de desenvolvimento é impossível.

Extreme Programming (XP) é uma metodologia ágil de engenharia de software. Essa metodologia, que é conhecida abreviadamente como metodologia XP, é usada principalmente para criar software em um ambiente muito instável. Permite maior flexibilidade dentro do processo de modelagem. O principal objetivo do modelo XP é reduzir o custo dos requisitos de software. É bem comum no modelo XP que o custo de alterar os requisitos no estágio posterior do projeto possa ser muito alto.

O XP, como outras metodologias ágeis, abrange mudanças e utiliza ciclos de desenvolvimento curtos ou iterações para permitir a mudança e a evolução do software ao

longo do tempo.

A Metodologia de Desenvolvimento do Scrum segundo Schwaber (2004) pode ser aplicada a praticamente qualquer projeto. Este processo é adequado para projetos de desenvolvimento que estão mudando rapidamente ou requisitos altamente emergentes. O modelo de desenvolvimento de software Scrum começa com um breve planejamento, reunião e conclusão com uma revisão final. Essa metodologia de desenvolvimento é usada para o desenvolvimento rápido de software, que inclui uma série de iterações para criar o software necessário. É uma metodologia ideal, pois facilita o rastreamento dos projetos de progresso mais lentos.

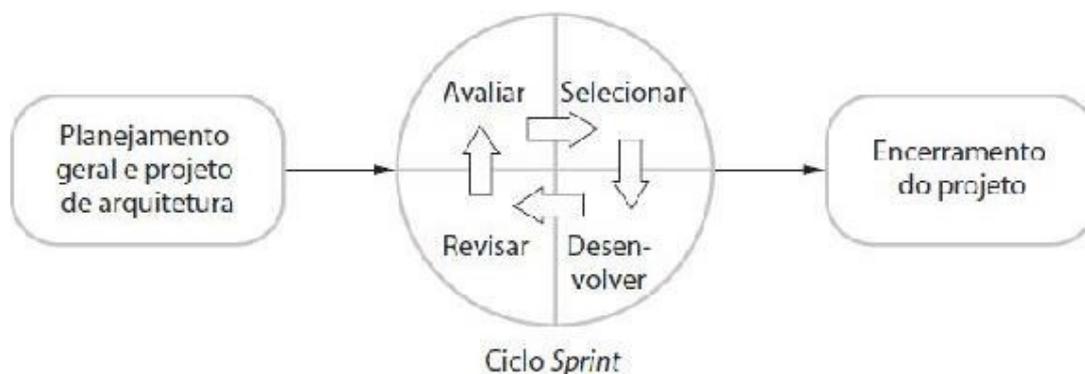


Figura 3 – O processo Scrum

Fonte: Sommerville Engenharia de Software (2011, p.50)

A idéia básica por trás do Scrum é que o desenvolvimento de software é dividido em iterações menores chamadas sprints, que têm uma quantidade definida de trabalho que é bloqueado e feito nesse período de tempo. Os resultados são entregues incrementalmente ao cliente no final de cada sprint.

4. ELEMENTOS CRUCIAIS DAS METODOLOGIAS DA ENGENHARIA DE SOFTWARE

Todo projeto de software possui um ciclo de vida fixo. É composto pela execução das fases conceitual, elaboração e aprovação da proposta pelo cliente, planejamento e organização que se traduz na divisão do projeto em marcos, fases, versões e/ou etapas. São planejadas com intuito de verificar todos os aspectos de controle e execução. Além disso, a implementação, caracterizada pelo desenvolvimento formal das etapas, visando atender os objetivos propostos. No encerramento do projeto de desenvolvimento realiza-se a verificação e confirmação dos resultados junto ao cliente, feedback final e a desmobilização dos recursos e da equipe. Os processos que rodeiam a construção de software ainda necessitam ser profundamente estudados, dado que, o processo de gerência software fundamenta seus esforços em medir, organizar e gerenciar o desenvolvimento e evolução de sistemas e, neste sentido, não existe uniformidade em padrões capazes de quantificar todos os aspectos que envolvem a atividade. Esta situação é facilmente percebida, visto que de tempos em tempos novos modelos e conceitos surgem geralmente apoiando-se nos erros e/ou trazendo uma nova roupagem as abordagens e modelos existentes.

Segundo Sommerville (2011) objetivo básico dessas metodologias é fornecer um

bom desenvolvimento de software de acordo com os requisitos do projeto.

As metodologias de desenvolvimento de software são usadas para estruturar, planejar e controlar o processo de desenvolvimento de um sistema de informações. Este tipo de metodologias de desenvolvimento preocupa-se com os processos de desenvolvimento de software, por isso não envolve nenhum aspecto técnico, mas apenas a preocupação com o planejamento adequado para o desenvolvimento do software (PRESMAN, 2011).

Abaixo serão abordados alguns fatores importantes das metodologias de desenvolvimento e evolução de software descrito anteriormente apontando principalmente suas vantagens e desvantagens.

Modelo em cascata:

- Segundo Audy, Prikladnicki (2007) esse modelo esclarece o processo de desenvolvimento de software em um fluxo sequencial linear, significa que qualquer fase no processo de desenvolvimento começa somente se a fase anterior for concluída. Essa abordagem de desenvolvimento não define o processo para retornar à fase anterior para lidar com mudanças nos requisitos.

Como vantagens do modelo em cascata podem ser destacadas:

- Modelo em cascata é muito simples e fácil de entender e usar, é por isso que é realmente benéfico para desenvolvedores iniciantes.
- É fácil de gerenciar, devido à rigidez do modelo. Além disso, cada fase tem resultados específicos e processo de revisão individual.

Desvantagens do modelo em cascata:

- Este modelo só pode ser usado quando requisitos iniciais muito precisos estiverem disponíveis.
- A principal desvantagem desse método é que, quando um aplicativo está em fase de teste, não é possível voltar e editar algo.

Modelo Espiral:

- É um modelo sofisticado que se concentra na identificação e redução precoce dos riscos do projeto. Segundo Pressman (2011) nesta metodologia de desenvolvimento de software, os desenvolvedores começam em pequena escala, em seguida, explora os riscos envolvidos no projeto, faz um plano para lidar com os riscos e, finalmente, decide se deve dar o próximo passo do projeto para fazer a próxima iteração da espiral. O sucesso de qualquer modelo de ciclo de vida em espiral depende do gerenciamento confiável, atencioso e bem informado do projeto.

Vantagens do modelo espiral:

- A grande quantidade de análise de risco, portanto, evitar o risco possível é certamente reduzido.
- Este modelo é bom para grandes projetos de tamanho e críticos.

Desvantagens do modelo espiral:

- O sucesso de todo o projeto depende da fase de análise de risco, portanto, falhas nesta fase podem danificar projetos inteiros.
- Não é apropriado para projetos de baixo risco.

Scrum:

- A Metodologia de Desenvolvimento do Scrum pode ser aplicada a praticamente qualquer projeto. Este processo é adequado para projetos de desenvolvimento que estão mudando rapidamente ou requisitos altamente emergentes. Segundo Sommerville (2011) o modelo de desenvolvimento de software Scrum começa com um breve planejamento, reunião e conclusão com uma revisão final. Essa metodologia é usada para o desenvolvimento rápido de software, que inclui uma série de iterações para criar o software necessário. É uma metodologia ideal, pois facilita o rastreamento dos projetos de progresso mais lentos.

Vantagens do desenvolvimento do Scrum:

- Nesta metodologia, a tomada de decisões está inteiramente nas mãos das equipes.
- Esta metodologia permite que o projeto não seja considerado muito significativo para o desenvolvimento bem-sucedido.

Desvantagens do desenvolvimento do Scrum:

- Esse tipo de modelo de desenvolvimento é sofrido se os custos e tempo do projeto de estimativa não forem precisos.
- É bom para projetos pequenos e rápidos, mas não é adequado para projetos de grande porte.

5. CONSIDERAÇÕES FINAIS

A partir da análise do material desta pesquisa é possível associar de forma segura que a prática e utilização de metodologias e técnica da engenharia de software à re-

sultados de sucesso em projetos de software. No entanto, apenas com os dados citados nessa pesquisa não aprofundam a respeito das características de cada metodologia de software, o que dificultou afirmar por via de dados concretos a real eficiência existente relacionada à utilização de tais metodologias e técnicas da engenharia de software, sendo esta a razão deste estudo, relacionar a importância da utilização das metodologias e técnicas da engenharia de software para o desenvolvimento e evolução de softwares. Ainda assim, é possível constatar mediante os dados que: sucesso em projetos de software são obtidos a partir da implementação de softwares com características que agregam valor, sendo a agilidade, organização e robustez de software fatores importantes e indispensáveis para o desenvolvimento dos softwares dados em virtude de metodologias e técnicas de desenvolvimento de software devidamente aplicado.

Principalmente em aplicações de software de auto risco, ou aplicações mais dinâmicas, onde uma falha ou demora no desenvolvimento podem ocasionar perdas astronômicas de recursos financeiros e humanos, por tanto com o resultado dessa pesquisa é possível deduzir que os objetivos foram sim atingidos e que as metodologias e técnicas de softwares só influenciam positivamente e proporcionam melhores condições para o desenvolvimento e evolução dos softwares.

Referências

ATKINSON, C., HUMMEL, O. (2012) “**Iterative and Incremental Development of Component Based Software Architectures**”, CBSE '12 Proceedings of the 15th ACM SIGSOFT Symposium on Component Based Software Engineering, p.77-82.

AUDY, Jorge; PRIKLADNICKI, Rafael. **Desenvolvimento distribuído de Software**. Campus: São Paulo, 2007.

ENGLHOLM JR, H. **Engenharia de Software na Prática**. São Paulo: Novatec, 2010.

GALORATH.COM. **Software Project Failure Costs Billions. Better Estimation & Planning Can Help**. Disponível em: <<https://galorath.com/blog/software-project-failure-costs-billions-better-estimation-planning-can-help/>>. Acessado em: 23/09/2018.

JALOTE, P. **An Integrated Approach to Software Engineering**. 3. ed. New York:Springer, 2005, 566p.

PRESSMAN, R. S. **Engenharia de Software**. 6. ed. Rio de Janeiro: McGraw-Hill, 2006, 720p.

SCHWABER, K. **Agile Project Management with Scrum**. Seattle: Microsoft Press, 2004.

SILVA, E. L. MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

SOMMERVILLE, I. **Engenharia de software**. 6. ed., São Paulo: Addison Wesley, 2003, 592p.

SOMMERVILLE, I. **Engenharia de Software**. tradução Ivan Bosnic e Kalinka G.de O. Gonçalves ; revisão técnica Kechi Hiramã. — 9. ed. — São Paulo: Pearson Prentice Hall, 2011.

VAZQUEZ, CARLOS EDUARDO; SIMÕES, QUILHERME SIQUEIRA. **Engenharia de Requisitos: software orientado ao negócio**. Rio de Janeiro: Brasport, 2016.

CAPÍTULO 2

HUMANOS E ROBÔS: INTELIGÊNCIA ARTIFICIAL

HUMANS AND BOTS: ARTIFICIAL INTELLIGENCE

Maycon Richard Gomes Silva¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

Este artigo foi feito com o objetivo de esclarecer mais as formas de convivência entre humanos e robôs evidenciando a utilização da inteligência artificial nos robôs e como ela se envolve diretamente com os seres humanos

Palavras-chave: Inteligência artificial; John McCarthy; Alan Turing; Aprendizado de máquina; humanos e Robôs

Abstract

This article was done with the objective of clarifying more the ways of coexistence between humans and robots, evidencing the use of artificial intelligence in robots and how it is directly involved with human beings.

Keywords: Artificial intelligence; John McCarthy; Alan Turing; machine learning; Robots and Humans.

1. INTRODUÇÃO

Compreende-se que, a inteligência artificial está presente no nosso dia a dia e cada vez mais evidente os avanços dessa tecnologia como boot chats, carros que se locomovem sozinhos, a convivência do homem com os robôs torna-se mais notória como a inteligência artificial está presente no nosso dia a dia. Quando se fala em humanos e robôs as vezes essa interação tecnológica pode passar despercebida, mas com uma análise mais crítica conseguimos identificar algum tipo de inteligência artificial inserida nos robôs que modelam toda a forma e define como será a interação entre humanos e robôs.

Entende-se assim que há uma necessidade em demonstrar de forma mais fácil e pratica as principais mudanças e evoluções da convivência de humanos e robôs e as principais ferramentas de inteligência artificial utilizadas para a implementação dos robôs na sociedade, por meio de pesquisa e revisões com um intuito de ajudar interessados a detectar esse tipo de ferramenta e entender como se deu essa evolução, além de ajudar a tomar decisões que podem levar a aderir um tipo de serviço para a sua empresa por exemplo e sem informar das futuras ,mudanças que serão causadas por essa interação.

O desenvolvimento deste trabalho abrange várias áreas de conhecimento no âmbito da ciência da computação, como engenharia de software, banco de dados, programação, inteligência artificial entre outras, além de abranger áreas como, a robótica evidenciando suas principais características e comportamento na sociedade. Mostrado a relação direta dos Robôs com a inteligência artificial, este trabalho demonstra como se dá a evolução dessas novas tecnologias e como isso influencia na história da humanidade. Sendo assim a conclusão deste trabalho científico pode ser útil para toda a comunidade de novos pesquisadores na área de robótica, além disso pode ser de grande utilidade e interesse a so-

cidade de forma geral que desconhece as mudanças ocasionadas pelo convívio com robôs.

A inteligência artificial vem cada vez mais ganhando espaço nas nossas vidas e os robôs são uma das formas mais marcantes que percebemos a sua existência e como sua existência auxilia de forma incrível atividades do homem quem antes demandavam muito esforço. Sabendo disso, quais foram as principais mudanças ocasionadas pela evolução dos robôs na sociedade, e quais as principais ferramentas da inteligência artificial que são utilizadas nos robôs e como a convivência com robôs ainda mudará a vida do homem?

O objetivo geral tem o enfoque em compreender a inserção dos robôs na nossa vida e como a inteligência artificial está vinculada para sempre evoluir o aprendizado e tecnologias dos robôs em nossas vidas. Os objetivos específicos têm foco em identificar os principais fatores que influenciaram para a inserção dos robôs na vida do homem, destacar os principais recursos utilizados para a implementação do IA nos robôs e mapear as principais mudanças e evoluções que os robôs causaram no convívio com o homem.

Este artigo foi elaborado mediante uma pesquisa descritiva, segundo Gil (1996), que proporciona uma proximidade com a questão os procedimentos de coleta dos dados supracitados, foi através de pesquisa bibliográfica e documental, com abordagem quali-quantitativa, com o intuito de relacionar os dados para a interpretação. Ao longo da construção da pesquisa foram definidos os objetivos deste trabalho, que com a análise dos dados foram transformados em gráficos e infográficos para melhor visualização. Tornando assim, os dados tanto em quantidade como em qualidade enriquecendo o resultado final deste trabalho.

2. INTELIGÊNCIA ARTIFICIAL

2.1 A Conferência de Dartmouth

Em 1956 aconteceu uma Conferência em Dartmouth College, NH, USA, onde se reuniram nomes como John McCarthy, Nathan Rochester, Marvin Minsky, Claude Shannon e outros matemáticos e pessoas importante para AI, onde o próprio nome do campo de pesquisa foi batizado de inteligência artificial pelo McCarthy, onde a máxima do setor foi definida como (Conferência em Dartmouth) "Cada aspecto de aprendizado ou outra forma de inteligência pode ser descrita de forma tão precisa que uma máquina pode ser criada para simular isso".



Figura 1 – Marvin Minsky, John McCarthy e Claude Shannon
Fonte: Wordpass (2014)

2.2 Inteligência de máquina

Antes a inteligência artificial tinha como foco principal e mais famoso a forma racional de resolver os problemas e como um exemplo mais evidente podemos observar o teste de Turing que testa a capacidade de uma máquina exibir comportamento inteligente equivalente a um ser humano, ou indistinguível deste.

Só que existia uma barreira neste tipo de análise de paradigmas lógicos como simbólico: metáfora linguística o probabilístico: lida com incerteza, Conexionista: metáfora cerebral Evolucionista: metáfora da natureza.

Isso deu um grande espaço para as redes neurais e para os paradigmas estatísticos e probabilísticos que com base dados alimentados poderiam tomar uma decisão e aprender mesmos quando não há informações suficientes.

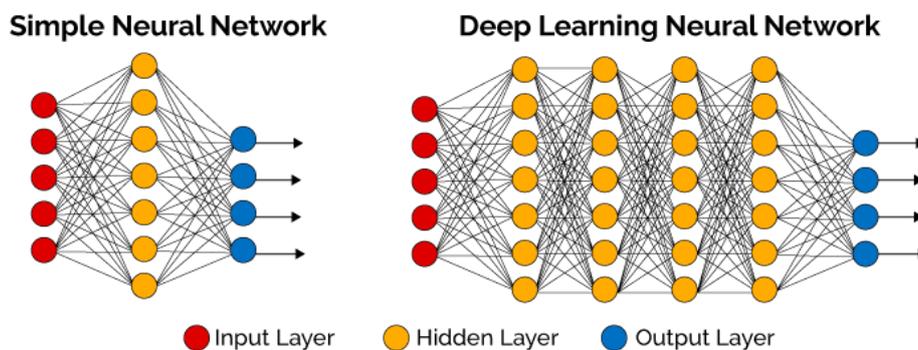


Figura 2 – Deep Learning vs. Rede Neural Artificial simples
 Fonte: <https://becominghuman.ai/>

2.3 Inserção dos robôs

Os robôs estão cada vez mais inseridos na sociedade, suas utilidades são infinitas, além de obtermos mais segurança e resultado em atividades laborais os robôs também ajudam a explorar áreas de estudos que antes eram impossíveis para o homem.



Figura 3 – Robô Humanoide: Sophia
 Fonte: Hanson Robotics.

Os robôs são agentes físicos que executam tarefas manipulando o mundo, eles são

equipados com dois elementos imprescindíveis para o seu funcionamento, são os efetadores como pernas, rodas, articulações e garras esses elementos tem como única função exercer força física sobre o ambiente, e também com sensores que lhe permitem perceber seu ambiente.

As três principais categorias dos robôs, manipuladores, móvel e robôs humanoides já faz parte do cotidiano de muitas pessoas e podem ser notadas em diversas atividades. A maior parte dos robôs se enquadra na categoria de manipuladores, eles são fisicamente fixos em seu local de trabalho como ilustrado na figura 4, por exemplo, em uma linha de montagem industrial ou na estação espacial internacional, fazendo assim com que os manipuladores recebam qualquer tipo de efetador para realizar o trabalho.



Figura 4 – Manipulador robótico industrial.
Fonte: Por Nachi Robotic Systems

3. A IMPLEMENTAÇÃO DOS IA NOS ROBÔS

A implementação da inteligência artificial nos robôs se vem pelas formas de aprendizado que são implementadas em seus sistemas, utilizando diversos tipos de sensores e efetadores para a percepção do mundo a sua volta.

Essa forma de aprendizagem é feita a partir de dados que são extraídos e recebidos pela interação do robô ao ambiente inserido, sendo assim qualquer componente de programa do robô pode ser aprimorado pela inteligência artificial sendo assim necessária fatores determinantes que servem de alicerce para as melhorias a serem implementadas dentro da aprendizagem. De acordo com Russell e Norvig (2013, p. 807) esses fatores são: “que componente deve ser melhorado, o conhecimento prévio que o agente já tem, que representação é usada para os dados e para o componente, que feedback está disponível para aprendizagem.

Essa implementação de aprendizagem nos robôs faz com que os robôs tenham a capacidade de monitorar sua própria precisão e desempenho, além detectar quando uma manutenção é necessária atuando também em ambientes novos e desconhecidos, sem precisar de programação prévia.

4. HUMANOS E ROBÔS

Vivemos em um mundo globalizado e tecnológico, desde a evolução industrial se tornou inevitável a vida dos seres humanos sem as máquinas, sem os robôs. Essa convivência vem fazendo com que acontecesse uma mudança na forma em que o ser humano vive, grandes lavouras, montadoras por exemplo, que outrora necessitava de uma gigantesca mão de obra se tornaram automatizadas graças aos robôs e assim além de ocorrer uma mudança nas vagas de empregos a convivência homem e robô se torna mais forte.

Muitas vezes essa interação se passa despercebido aos olhos humanos, mas, na maioria das vezes, não construímos robôs para trabalharem isoladamente. Nós os construímos para nos ajudar, e trabalhar em ambientes humanos, ao nosso redor e conosco.

5. CONSIDERAÇÕES FINAIS

Nesse artigo abordou como se deu o avanço da inteligência artificial e como foram feitas as transformações sociais pelo uso dos robôs na convivência com os humanos, destacou a inserção dos robôs na sociedade e a inserção do aprendizado de máquina nos robôs para melhorar a eficiência dos próprios.

Pode-se perceber que os tipos de aprendizados podem ser feitos por diversos equipamentos utilizando a inteligência artificial por trás para dar suporte e destinos aos objetivos aguardados pela máquina, com isso se torna infinitamente o uso de possibilidade para novos descobrimentos na área.

E por últimos percebe-se essa interação direta com os seres humanos e como ajudar as máquinas a se fortalecerem contribuindo assim, ainda mais, com serviços prestados por elas para o nosso dia a dia.

Referências

SMITH, MCGUIRE, HUANG **The History of Artificial Intelligence**. disponível em: < <https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf>>

DORMEHL, **uma história de inteligência artificial em 10 pontos de referência**, disponível em: < <https://www.digitaltrends.com/cool-tech/history-of-ai-milestones/>>

STUART J. RUSSELL E PETER NORVIG. **Artificial Intelligence: A Modern Approach** 3º e 4º edição.

CAPÍTULO 3

SEGURANÇA EM BANCO DE DADOS

DATABASE SECURITY

Lucas Delgado Freitas¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

O tipo de estudo a ser elaborada neste trabalho, será uma revisão de literatura, onde será exercida uma pesquisa em artigos online, livros, monografias e sites da web. Os seus fins específicos foram: Desenvolver a qual a importância da proteção ao Banco de Dados; Apresentar a criptografia em banco de dados; Compreender a principal ameaça de segurança à base de dados SQL. Um dos recursos de proteção aos dados é a criptografia, que é o meio de codificar os dados em informações que de início parecem sem sentido e só consegue ter acesso à informação a pessoa que tem a chave ou senha para decodificar, descriptografar o arquivo. A segurança do banco de dados tem o poder de manter e garantir a integridade, a disponibilidade e a confidencialidade dos dados, restando as informações apenas a quem elas devem pertencer. A importância do trabalho é passar a relevância da segurança em banco de dados, exibir uma técnica de segurança do mesmo e apresentar uma grande ameaça aos Sistemas de Gerenciamento de Banco de Dados que interagem com bases de dados via SQL. Existe um mecanismo de criptografia no MySQL, que possibilita por meio de algoritmos, encriptar e decriptar os dados da tabela. Os dois algoritmos mais utilizados, são o *Message - Digest algorithm 5* (MD5) e *Advanced Encryption Standard* (AES). Entre os diferentes tipos de ataques que existe, o principal deles é o *SQL injection*. A injeção SQL acontece quando o *cracker*, o invasor, uma pessoa má intencionada consegue inserir uma série de instruções SQL dentro de uma *query*, utilizando manipulação das entradas de dados de uma aplicação.

Palavras-chave: Banco de dados; Criptografia; Injeção de SQL; SQL.

Abstract

The type of study to be elaborated in this work will be a literature review, where a research will be carried out in online articles, books, monographs and web sites. Its specific purposes were: To develop the importance of the protection of the Database; Present the encryption in database; Understand the main security threat to the SQL database. One of the protection features to the data is encryption, which is the means of encoding the data into information that initially seem meaningless and can only access the information to the person who has the key or password to decode, decrypt the file. Database security has the power to maintain and ensure the integrity, availability and confidentiality of the data, retaining the information only to whom they should belong. The importance of the work is to pass the relevance of database security, display a security technique of the same and present a great threat to the Database Management Systems that interact with databases via SQL. There is an encryption mechanism in MySQL that enables algorithms to encrypt and decrypt the table data. The two algorithms most used, are Message - Digest algorithm 5 (MD5) and Advanced Encryption Standard (AES). Among the different types of attacks that exist, the main one is SQL injection. SQL injection happens when the cracker, the attacker, a malicious person is able to insert a series of SQL.

Keywords: Cryptography; Database; SQL Injection; SQL

1. INTRODUÇÃO

O problema de pesquisa deste trabalho, foi apresentar a importância da segurança em um Banco de Dados.

No mundo de hoje em dia precisamos armazenar diversos tipos de informações, e esses dados vem crescendo cada dia mais. Para que esse armazenamento seja possível, não podemos abrir mão de algumas tecnologias que nos ajudam nesse trabalho e o banco de dados é uma dessas tecnologias. Com o uso da internet, os sistemas se tornam presentes em vários locais ao mesmo tempo, o que também os torna vulneráveis. Existem muitos dados sensíveis, como CPF, senhas, números de cartões de créditos que necessitam de uma segurança mais reforçada, com o propósito de garantir a integridade e o sigilo das informações. Um dos métodos de proteção aos dados é a criptografia, que é o processo de codificar os dados em informações que a princípio parecem sem sentido e só consegue ter acesso à informação a pessoa que tem a chave ou senha para decodificar, descriptografar o arquivo. Dentre as diversas formas de ataque a um Sistema Gerenciador de Banco de Dados, a mais conhecida é a injeção de SQL, que é uma técnica de injeção de código que pode destruir o banco de dados. O cracker se aproveita de falhas nos sistemas que interagem com base de dados via SQL.

A segurança do banco de dados tem a importância de manter e garantir a integridade, a disponibilidade e a confidencialidade dos dados, mantendo as informações apenas a quem elas devem pertencer. Seja com dados bancários, dados de clientes de uma loja qualquer, dados de boletins escolares ou qualquer outra informação contida em um SGBD, se forem descobertos, alterados ou excluídos esses dados, vai ocasionar problemas. Por isso, tem-se a importância da proteção, segurança de um banco de dados. A importância do trabalho é exibir a relevância da segurança em banco de dados, exibir uma técnica de segurança do mesmo e exibir uma grande ameaça aos Sistemas de Gerenciamento de Banco de Dados que interagem com bases de dados via SQL.

Antigamente as empresas guardavam suas informações em arquivos físicos, o que se tornou obsoleto, pelo fato de gerar um grande acúmulo de papéis, desse modo dificultando a organização e o acesso às informações, sem contar que em casos de desastres como incêndio, desabamento, enchente, poderia ocorrer perda de informações, sem ter como recuperar. Por isso as empresas passaram a investir em compra de computadores para que as informações fossem armazenadas em banco de dados digitais. Nos bancos de dados empresariais, contém muitas informações valiosas. O acesso de pessoas não autorizadas pode levar prejuízos a empresa, como vazamento de informações de clientes, dados bancários, senhas, o que pode levar a perda de mercado ou até mesmo ações judiciais.

A segurança das informações deve ser muito bem elaborada e estruturada, tendo em vista que uma falha em qualquer ponto pode envolver todo um ambiente. Nos bancos de dados, os ataques nem sempre tem como objetivo o roubo de dados, mas também a alteração desses dados contidos no sistema, destruição mal intencionada, entre outros. Existem vários métodos, que se diversificam de acordo com a pretensão final do ataque. O que é criptografia de dados? A criptografia de dados transforma um texto qualquer em



um texto incompreensível. Assim, somente pessoas autorizadas poderão ter acesso a informação contida naquele texto. A criptografia confunde dados de uma chave ou de uma senha, tornando assim os dados inúteis sem a chave de descryptografia ou senha. Existe um mecanismo de criptografia no MySQL, que permite por meio de algoritmos, encriptar e deciptar os dados da tabela. Os dois algoritmos mais utilizados, são o *Message-Digest algorithm 5* (MD5) e *Advanced Encryption Standard* (AES). Entre os diversos tipos de ataques que existe, o principal deles é o SQL injection. Esse tipo de ameaça se aproveita de falhas nos sistemas que interagem com a base de dados via SQL. A injeção SQL ocorre quando o cracker, o invasor, uma pessoa má intencionada consegue inserir uma série de instruções SQL dentro de uma query, usando manipulação das entradas de dados de uma aplicação.

O tipo de pesquisa a ser realizada neste trabalho, será uma revisão de literatura, onde será realizada consulta em artigos online, artigos, livros, monografias e sites da web. As fontes utilizadas são do período dos últimos 10 anos de 2008 ao ano de 2018. As palavras chaves utilizadas: Banco de Dados. Segurança. Injeção SQL. SQL Injection. Criptografia. SQL. Critérios de exclusão: pouca abordagem do assunto nos textos e sem referências bibliográficas.

2. PROPRIEDADES DA SEGURANÇA DA INFORMAÇÃO

O principal objetivo da Segurança da Informação, consiste na defesa de dados, principalmente dados sensíveis. São utilizadas políticas de uso, processos e métodos para que dados sigilosos não sejam expostos e para que os mesmos também sejam acessados somente por quem tem autorização a eles. A Segurança da Informação é baseada em três pilares: Confidencialidade, Integridade e Disponibilidade. A falha de qualquer um desses pilares leva a uma má proteção de dados.

2.1 Confidencialidade

Por ter haver com sigilo e segredo, esse pode ser a propriedade mais interessante da segurança da informação. Confidencialidade é a garantia de que as informações dadas serão protegidas contra a sua revelação não autorizada. O objetivo da confidencialidade de acordo com a Organização Internacional de Normalização (ISO) na norma ISO/IEC 17799 é "garantir que a informação seja acessível apenas àqueles autorizados a ter acesso", ou seja, deixa aquela informação inacessível para aquele usuário, entidade ou processo não autorizado. Pode-se dizer que a confidencialidade é uma medida para garantir que as informações não caiam em mãos erradas. Além de proteger os dados, fazendo restrição com controle de acesso somente a quem tem autorização, os que recebem liberação para acesso ao sistema devem ser monitorados e ter todas as ações executadas e documentadas para análises posteriores, se houver necessidade.

2.1.1 Confidencialidade Reforçada

Como reforçar a confidencialidade? A adoção de medidas preventivas, fazendo a limitação de conteúdo de acordo com a área de atuação. Não acessar ou compartilhar as informações sigilosas em locais públicos ou que tenham baixa segurança virtual, como *lan houses*. Conscientização a não violação de regras, como por exemplo, evitar conectar dispositivos externos à rede corporativa. Definindo o acesso às informações somente a pessoas autorizadas, que é elaborada através de níveis, de modo que funcionários de cargos mais elevados tenham um maior acesso aos dados que os funcionários de cargos mais baixos.

Para garantir a confidencialidade utiliza-se mecanismos de criptografia, que mantém a confidencialidade de uma informação com o uso de chaves assimétricas.

2.2 Integridade

Disponibilidade de informações confiáveis, ter a certeza de que aquela informação é a correta, e a garantia de que os dados não foram alterados ou modificados, que estão corretas e dispostas em formato compatível com o de utilização, ou seja, informações íntegras. Significa que a informação não foi alterada de forma não autorizada ou indevida. A informação perde a sua eficácia e confiabilidade quando falsificada ou alterada de forma errada, o que torna vulnerável às decisões tomadas a partir daquela informação, o que também tira a credibilidade da organização ou empresa que a forneceu.

Qualquer alteração realizada nas informações independentemente do nível de permissão que o usuário tiver, são rastreadas, monitoradas e documentadas. O que torna o nível de confiabilidade do banco de dados ainda maior, porque garante que a edição seja efetuada somente por pessoas autorizadas, mantendo o estado original quando armazenados. É adotado a criptografia de dados para conseguir bons níveis de integridade. Da mesma forma como uma pessoa conhecida por ser íntegra é confiável, a integridade da informação significa que ela realmente representa o significado demonstrado.

2.3 Disponibilidade

Garante que a informação possa ser acessada sempre que necessário, ou seja, estará sempre disponível para quem precisar de acordo com seu nível de acesso. De uma maneira muito mais direta de que a integridade, está ligado à questão operacional de uma empresa. As informações podem ser acessadas e modificadas por qualquer pessoa autorizada por um dispositivo, rede e período de tempo apropriado. Dependendo do tipo de informação, o prazo apropriado pode significar coisas diferentes.

Por exemplo, um vendedor precisa ter acesso ao sistema de uma loja para verificar a disponibilidade de um determinado produto para informar a um cliente que está aguardando na loja, logo ele precisa ter um acesso imediato, para poder dar a resposta ao clien-



te que está aguardando. Já um gerente pode se contentar com um relatório de vendas na manhã do dia seguinte.

Tecnologia voltada à manutenção e preservação do acesso aos dados é essencial para uma infraestrutura. Através de processos de manutenção de *hardwares* e eliminação de conflitos de *softwares*, a disponibilidade tem uma garantia de forma mais eficiente.

Atualizações do sistema também são necessárias de modo periódico, utilizando a largura de banda de comunicação compatível com as necessidades. Plano de Recuperação de Desastres (RD) contendo procedimentos e diretrizes para se administrar crises, manter a continuidade dos negócios e recuperar dados perdidos.

As características de disponibilidade são:

- Pontualidade. Sempre que necessários, os sistemas de informação deverão estar disponíveis;
- Continuidade. No caso de um fracasso ou indisponibilidade, o pessoal ainda tem que ter acesso ao sistema para continuar a trabalhar;
- Robustez. Não deve haver limitação de capacidade de funcionários trabalhando ao mesmo tempo num mesmo sistema de informação.

A falha na disponibilidade pode causar impactos grandes às corporações, empresas ou organizações, existem vários exemplos como, casos de incalculáveis prejuízos financeiros (às vezes, acima de R\$ 1 bilhão) causados por conta da indisponibilidade de sistemas. Outro exemplo seria no decorrer de uma auditoria, a indisponibilidade de um relatório de balanço financeiro de uma empresa pode ser motivo suficiente para que esta organização seja multada ou mesmo condenada pela justiça.

De modo geral, a disponibilidade significa poder ter acesso sempre que necessário, e para garantir isso deve-se fazer a manutenção e atualização de *hardwares* e *softwares* (servidores e redes).

3. CRIPTOGRAFIA

Vem da junção de duas palavras gregas, que são: "Kryptós", que significa "oculto/escondido" e "gráphein", que significa "escrever/escrita".

É uma técnica que transforma informações legíveis em informações ilegíveis, é a prática de codificar e decodificar informações. Faz com que textos simples fiquem de um modo incompreensível para quem não tem acesso às convenções combinadas. Segundo Fiorim (2015) "Criptografia é um sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário possa ler".

Outro conceito pode ser dado por França:

A Criptografia é a ciência que oculta o significado de uma mensagem e tem como ferramenta os recursos matemáticos para cifrar e decifrar mensagens. O ato de cifrar consiste em transformar um texto normal em texto secreto, e o ato de decodificar é a operação inversa, consiste em transformar um texto cifrado em texto normal. Veremos os conceitos históricos da criptografia, suas definições e aplicações matemáticas.

3.1 Criptografia Em Banco De Dados Sql

É muito comum o uso de informações sensíveis, para a elaboração de um sistema. Com o objetivo de garantir a integridade e o sigilo do seu conteúdo, há a necessidade de certo nível de segurança no momento do armazenamento. Para atender esses requisitos, ocultamos os dados de visitantes não autorizados, fazendo uma alteração no conteúdo original, deixando o conteúdo visível apenas para aqueles a quem o acesso é permitido. Existem três elementos fundamentais que precisamos compreender para usar os mecanismos de criptografia do SQL Server: a Chave Mestra, o certificado e a chave simétrica e assimétrica (OLIVEIRA, 2016).

Existem dois aplicativos para chaves, que é uma chave mestra de serviço (*Service Master Key - SMK*) e outra chave mestra para que seja usada para o banco de dados (*Database Master Key - DMK*)

A SMK serve para o gerenciamento das chaves de criptografia, ela é gerada no momento em que é iniciada a instância do SQL Server. Cada instância tem a sua chave mestra. A API (*Application Programming Interface*) de proteção de dados (DPAPI) é responsável pela criptografia da SMK, que usa um serviço de credenciais da conta do serviço SQL Server. O algoritmo DES triplo é o algoritmo de criptografia desta chave que é de 128 bits e só pode ser descriptografada pela mesma conta que a criou. A DMK também é uma chave de 128 bits que usa o algoritmo DES triplo.

Cada banco de dados tem sua própria DMK, usada na criptografia das chaves assimétricas e privadas de um certificado. Com o uso da SMK, uma cópia da chave é criptografada para poder habilitar a descriptografia da chave mestra (CUPCIK, 2017). Quando é criada, a DMK é criptografada pelo DES triplo e por uma senha.

De acordo com Oliveira (2016), que declara:

A Master Key é a raiz hierárquica da criptografia do SQL Server, representando uma chave mestra, única para cada banco de dados, que é utilizada para proteger as chaves privadas dos certificados, chaves assimétricas e simétricas. Para criar uma Master Key podemos utilizar o seguinte comando, no qual precisamos obrigatoriamente informar uma senha.



```
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'senha' --Setando uma senha para a Chave Mestra
GO
```

Figura 1 - Criando uma senha para chave mestra
Fonte: www.devmedia.com.br

Na figura 1, tem a demonstração em código SQL para a criação de uma senha para a chave mestra.

Temos como segundo objeto na hierarquia de criptografia os certificados, que contém uma chave pública e tem a opção de conter uma chave particular. O *SQL Server* gera os certificados ou se preferir, podemos usar certificados gerados externamente. A utilidade do certificado se dá pela opção de exportar e importar chaves para os arquivos do próprio certificado. Para gerar um certificado, precisamos de uma senha, que é utilizada para a proteção dos próximos objetos da hierarquia de criptografia, mas para que seja gerado é necessária a existência de uma *Master Key* (OLIVEIRA, 2016).

```
CREATE CERTIFICATE MeuCertificado
ENCRYPTION BY PASSWORD = 'SENHA@123'
WITH SUBJECT = 'Meu Certificado'
GO
```

Figura 2 - Criando certificado
Fonte: www.devmedia.com.br

Na figura 2, tem a demonstração em código SQL para a criação de um certificado.

O próximo objeto da hierarquia que está relacionado à criptografia, é a chave simétrica. Conhecida como criptografia de chave secreta, é uma forma de criptografia que utiliza a mesma chave tanto para criptografar quanto para decriptografar. Uma chave única é criada e compartilhada entre o emissor e o receptor. Algoritmos de chaves simétricas são mais rápidos, porém não tem o mesmo nível de segurança de um com chave assimétrica. Utiliza-se um certificado no momento em que é criada para criptografar a chave e é criptografada também através de uma chave simétrica ou assimétrica e de uma senha. Precisa informar qual o algoritmo de criptografia será utilizado. Utilizando um certificado e o algoritmo de criptografia AES_256, a figura abaixo demonstra a criação de uma chave simétrica:

```
CREATE SYMMETRIC KEY MinhaChave
WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE MeuCertificado
```

Figura 3 - Criando chave simétrica
Fonte: www.devmedia.com.br

Na figura 3, tem a demonstração em código SQL para a criação de uma chave simétrica.

3.1.1 Algoritmo MD5 (*Message-Digest algorithm 5*)

Desenvolvido pela empresa RSA Data Security, Inc., descrito na *Request for Comments* (RFC) 1321, algoritmo unidirecional de *hash* de 128 bits, softwares ponto a ponto (P2P) utilizam para verificação de integridade de arquivos e *login*. Foi desenvolvido para substituir o MD4 que continha problemas de segurança. Pelo fato de ser unidirecional, ele não pode ser decifrado. É realizada a comparação de duas *hash* para poder ser realizada a verificação, já que ele não pode ser transformado no seu texto original. Qualquer mensagem, seja ela do tamanho que for, o algoritmo gera um valor *hash* de 128 bits, é impossível descobrir duas mensagens que gerem o mesmo valor. Vários protocolos de padrão de internet utilizam o MD5. (VALE, 2007). Já no MySQL, ele gera um valor hexadecimal de 32 dígitos. O comando utilizado no *SQL Server*, é: `SELECT HASHBYTES('MD5', 'password')`

Ele retorna o valor da senha "*password*" em MD5, mas retorna um tipo de dado que não tem como realizar comparação, o que dificulta o seu uso. Porém tem uma solução para isso, com a utilização de uma função que retorna o *hash* igual ao gerado. O comando é: `SELECT SUBSTRING (sys.fn_sqlvarbasetostr(HASHBYTES('MD5', 'password')),3,32)`. Faz retornar o valor da senha em MD5 em forma de *string*.

3.1.2 Algoritmo AES (*Advanced Encryption Standard*)

Também conhecida pelo nome Rijndael, foi desenvolvido para substituir o Data Encryption Standard (DEA). O Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos realizou uma competição para que fosse desenvolvido um algoritmo que seria chamado de AES e que atendesse algumas especificações: teria que ser um algoritmo publicamente definido; teria que ser projetado para que o tamanho da chave fosse expansível; ser disponibilizado livremente; ser uma cifra simétrica de bloco e que fosse implementável tanto em software quanto em hardware. O processo seletivo que teve início em 1997 chegou ao seu fim em 2000, e foi selecionado o algoritmo Rijndael, desenvolvido pelos criptografos Vicent Rijmen e Joan Daemen. (MATHIAS, 2005).

O AES é uma primitiva criptográfica destinada a compor sistemas de cifragem e decifragem simétrica (i.e. mesma chave para cifrar e decifrar). É uma cifra de bloco, ou seja, opera em blocos de tamanho fixo (128 bits, ou 16 bytes). Como toda cifra de bloco, pode ser transformada numa cifra de fluxo (de modo a operar em dados de tamanho arbitrário) através de um modo de operação. Pode trabalhar com chaves de 128, 192 ou 256 bits (o algoritmo Rijndael, que originou o AES, permite mais tamanhos de chaves). (GIBSON, 2014).

```
CREATE SYMMETRIC KEY SK03
WITH
ALGORITHM = AES_256
ENCRYPTION BY PASSWORD = 'ThisIsMyAES_256EncryptionTest';
```

Figura 4 - criptografando senha com AES
Fonte: stackoverflow.com



Na figura acima, temos a demonstração do código em SQL da criação de uma chave simétrica criptografada com o algoritmo AES.

```
OPEN SYMMETRIC KEY SK03 DECRYPTION BY PASSWORD='ThisIsMyAES_256EncryptionTest'
SELECT
  [OriginalValue]
  ,CONVERT(varchar(MAX), DECRYPTBYKEY([EncryptedValue]))
FROM
  _EncryptionTest
CLOSE SYMMETRIC KEY SK03;
```

Figura 5 - Decriptografia SQL
Fonte: stackoverflow.com

Na figura acima, temos a demonstração do código em SQL da decriptografia.

4. ATAQUE COM SQL INJECTION.

É a maior ameaça a sistemas de segurança, utiliza as falhas no código de uma aplicação. Por meio de *input*, temos a possibilidade de manipular uma consulta via SQL. Podemos pensar no *SQL Injection* como uma falha lógica no sistema. Isso porque é aberto a várias interpretações.

O *SQL Injection* é o nome dado a uma falha na codificação de uma aplicação qualquer (seja web ou local) que possibilita, por meio de um input qualquer, a manipulação de uma consulta SQL. Essa manipulação é chamada Injeção, então, o termo Injeção SQL. Resumindo: o *SQL Injection* é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e bancos de dados relacionais (PAYÃO, 2017).

O ataque consiste de injeções de código SQL diretamente nos campos de entrada de dados, assim podendo realizar alteração de comandos no SQL, revelando os dados escondidos, como exemplo: senhas, número de cartões de crédito, cpf, senhas bancárias, entre outros dados sensíveis. Mas para que isso ocorra, tem que combinar com os parâmetros estáticos e receber dados das entradas dos usuários.

Para um melhor entendimento do funcionamento do *SQL Injection*, podemos verificar a seguinte situação: Em uma tela de *Login* onde temos os campos de usuário e senha no formulário, no momento em que é inserido o nome e a senha, a aplicação faz uma consulta na tabela de usuários do banco de dados para realizar a verificação do cadastro do usuário, da seguinte maneira:

LOGIN

user:

password:

Temos a consulta da seguinte forma:

```
SELECT * FROM users WHERE user = 'campo_usuario' AND pass = 'campo_senha'
```

Dessa maneira a busca seria feita com o nome de acesso "usuario" e a senha "123456". Com um nome de um usuário válido é possível "burlar" a digitação da senha, tendo acesso a conta daquele usuário.

LOGIN

user:

password:

O *cracker* terá acesso à conta, pelo simples fato de ter usado a sequência de caracteres "--", essa sequência faz com que todo o resto do comando após ela fique comentado, assim não sendo executado o trecho do código que solicita a senha. O código:

```
"select * from users where username = ' " + username +
```

```
" `and password = ` " + password + "` `";
```

Código esse que solicita o nome e a senha. A parte do código que fica comentada fazendo com que não seja solicitada a senha é:

```
" ` and password = ` " + password + "` `";
```

Que é a parte do código que pede a senha.

Outra situação é se o *cracker* não souber de nenhum usuário válido. Nesse caso, ele pode realizar a autenticação usando as credenciais do primeiro usuário cadastrado na tabela "users" do banco de dados.

LOGIN

user:

password:

Podemos observar mais uma vez o uso dos caracteres "--", que serve para que o restante do código não seja executado, assim também não necessitando o uso de senha para ter acesso validado. A comparação usada no campo *user* "1=1", será sempre verdadeira, pois 1 sempre será igual a 1, dessa maneira todos os registros da tabela são retornados

usando o nome cadastrado do primeiro usuário.

O invasor pode realizar um *delete* nos registros da tabela "users", fazendo com que ninguém mais tenha acesso ao sistema.

LOGIN

user:

password:

A única coisa não vista antes é o uso do " ; ", que finaliza um comando no SQL para dar início ao outro comando "delete from".

Foi feita a demonstração de algumas falhas devido a erros de interpretação da linguagem SQL. Existem muitas outras técnicas de ataque através de comandos SQL, que variam de simples injeções de códigos SQL a comandos mais extensos e bem elaborados.

5. CONSIDERAÇÕES FINAIS

Esse trabalho propôs de maneira conceitual e estratégica, uma Abordagem sobre a segurança em banco de dados, fazendo ênfase às propriedades da segurança da informação, à criptografia de dados SQL e um dos ataques a banco de dados mais usados na atualidade.

Foram demonstradas as propriedades da segurança da informação em relação à proteção de banco de dados, trazendo os conceitos de cada propriedade e relatando acerca de cada uma das mesmas. Deve-se seguir cada uma das propriedades para que se tenha um banco de dados seguro. A falha de qualquer propriedade, leva ao comprometimento de um sistema.

Foi levantado neste trabalho o conceito de criptografia que como foi citado, é um dos mecanismos de segurança aos bancos de dados, foi abordado também sobre a criptografia em banco de dados que utilizam a linguagem estruturada SQL. Ao longo do capítulo que trata sobre a pesquisa de criptografia em banco de dados, foi discutido sobre dois algoritmos de criptografia, o MD5 e o AES, que são utilizados para verificação de integridade de arquivos.

Como visto, temos a apresentação da maior ameaça a banco de dados via SQL. Foi disposto a definição de *SQL Injection*, mostrando os meios de invasão, que é por manipulação pura de SQL, levando a se pensar no *SQL Injection* como uma falha lógica no sistema, pelo fato de ser aberto a várias interpretações. Foi demonstrada uma técnica simples de invasão utilizando o *SQL Injection*.



CAPÍTULO 4

A INFLUÊNCIA DA INTELIGÊNCIA ARTIFICIAL NA EXPERIÊNCIA DOS USUÁRIOS DE JOGOS ELETRÔNICOS

*THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON THE EXPERIENCE
OF ELECTRONIC GAME USERS*

Matheus Guilherme Rocha dos Santos¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

O tema deste trabalho está envolto sobre a problemática da influência da inteligência artificial na experiência dos usuários de jogos eletrônicos, esse tema se torna necessário ser trabalhado a medida que esse mercado cresce e ganha espaço, pois, muitas empresas e desenvolvedoras independentes podem possuir erros em não entender a influência de IAs na experiência do usuário. Entendendo suas aplicações e técnicas é possível escolher um caminho melhor de desenvolvimento, com o objetivo de entreter o usuário, passando por desafios como jogos tediosos e jogos extremamente difíceis. Com o objetivo de poder entender a influência da inteligência artificial na experiência dos usuários de jogos eletrônicos, isso foi possível com o embasamento nos meios digitais, como: artigos científicos, monografias e livros com data de dez anos incluindo o atual. Através desta pesquisa e condensação de conhecimentos foi possível entender: como a influência da inteligência artificial atinge a experiência dos usuários de jogos eletrônicos, essa necessidade surge a medida que é preciso entender como o desenvolvimento de IAs influencia na experiência do usuário de jogos eletrônicos.

Palavras-chave: IA em jogos eletrônicos. Inteligência artificial. Experiência no usuário de jogos eletrônicos. Influência da IA em jogos eletrônicos.

Abstract

The theme of this work is wrapped around the problem of the influence of artificial intelligence in the experience of users of electronic games, this theme becomes necessary to be worked as this market grows and gains space, because many companies and independent developers may have errors in not understanding the influence of AIs on the user experience. Understanding its applications and techniques, it is possible to choose a better development path, with the aim of entertaining the user, going through challenges such as tedious games and extremely difficult games. In order to be able to understand the influence of artificial intelligence on the experience of users of electronic games, this was possible based on digital media, such as: scientific articles, monographs and books dating back ten years including the current one. Through this research and condensation of knowledge, it was possible to understand: how the influence of artificial intelligence affects the experience of users of electronic games, this need arises as it is necessary to understand how the development of AIs influences the user experience of electronic games.

Keywords: AI in electronic games. Artificial intelligence. User experience of electronic games. Influence of AI in electronic games.

1. INTRODUÇÃO

Com o avanço da tecnologia, muitos mercados começaram a ver a oportunidade e a necessidade em utilizar ferramentas avançadas em seus meios. No mercado de jogos eletrônicos não é diferente, pode se analisar isso no crescimento exponencial na qualidade em que jogos são desenvolvidos por grandes empresas como Rockstar Games, Ubisoft, Sony, entre outras. Porém uma grande dificuldade é vista quando analisamos a influência da inteligência artificial na experiência dos usuários de jogos eletrônicos. Para entendermos melhor essa influência, precisamos adentrar nesse mundo dos jogos, mais especificamente na programação utilizando inteligência artificial e analisarmos como isso influencia em seus diversos usuários.

Uma grande ferramenta que vem sendo usada a décadas e está em alta em dias atuais é a IA (Inteligência Artificial), que diferente da IA da computação que visa resolver problemas gigantescos de matemática, a IA em jogos é utilizada para gerar ações “robotizadas” dentro do jogo, visando uma interação com o player (jogador do jogo). Então, a IA em jogos, tem um papel importante que muitas vezes são esquecidas no momento da produção e do desenvolvimento dos jogos pelos desenvolvedores, que é a experiência do usuário ou a sensação em que o player irá sentir no momento da jogabilidade.

A influência da inteligência artificial na experiência dos usuários de jogos eletrônicos tem grande importância para o mercado de jogos, pois tal influência interfere diretamente na experiência do usuário dentro dos jogos, causando relevância para quem atua nos setores das vendas, e para o consumidor que irá compra, avaliar, recomendar e divulgar, gerando assim satisfação positiva ou negativa para as ambas as partes. Jogos complexos, tratando-se na programação, como, The Sims, desenvolvido a partir os anos 2000 e jogos menos complexos como, Pong, desenvolvido em 1972, por mais que diferentes, possuem um objetivo em comum, a experiência do usuário. Ambos buscam, de maneiras únicas e próprias, entreter o jogador e garantir um experiência boa, se não perfeita, para o usuário.

Com o objetivo de entender como a inteligência artificial influencia na experiência dos usuários de jogos eletrônicos, esse trabalho apresentará, em três objetivos, a compreensão e o entendimento das ações de uma inteligência artificial nos jogos eletrônicos, analisando tipos de técnicas de IAs aplicadas em jogos, buscando compreender suas peculiaridades e aplicações, analisando como a experiência do usuário de jogos eletrônicos está ligada a qualidade da inteligência artificial, concluindo com o objetivo de situar pontos que levam a clareza em desenvolvedores e empresas do setores a trabalharem com excelência, visando uma entrega com maior qualidade do produto final ao consumidor.

Este trabalho foi realizado através de leituras bibliográficas, pesquisas em sites da internet, sempre buscando fontes confiáveis de autores onde possuem expertise na área, leituras de artigos científicos, dissertações e trabalhos acadêmicos publicados. A soma deste conteúdo resultou em uma análise de forma ampla e certa sobre os objetivos propostos, atenuando a experiência do usuário em jogos eletrônicos resultada pelas inteligências artificiais desenvolvidas.

2. INTELIGÊNCIA ARTIFICIAL EM JOGOS ELETRÔNICOS

De acordo com Marcelo de Souza e Adilson Vahldick (2013, p.157), “o desenvolvimento de jogos é um campo que atrai muitos desenvolvedores e que vem crescendo com o passar dos anos.” Com isso, a utilização de técnicas de programação e principalmente a utilização de novas ferramentas, como Inteligência Artificial (ou IA), são vistas de forma atrativa entre os desenvolvedores, considerando que a experiência do usuário seja o ponto chave de um jogo de sucesso.

A diferença entre IA acadêmica e a IA para jogos como fala André Kishimoto (2004), é que no primeiro caso, o principal objetivo é solucionar problemas extremamente difíceis e complexas, (como exemplo, buscar imitar o reconhecimento que humanos tem sobre objetos). No segundo caso, não banalizando, o principal objetivo é a diversão que o usuário terá, em outras palavras, buscar aumentar a experiência do usuário.

De acordo com Paul Tozour (2002), o principal objetivo da IA em jogos é garantir resultados que agregam na experiência do usuário, ou seja, a IA se preocupa em como o sistema age, proporcionando uma jogabilidade em que o usuário se sinta empolgado e mais interessado em continuar jogando, usufruindo totalmente do que o jogo pode proporcionar.

Ao utilizar IA em jogos, buscamos a evolução na imersão e a jogabilidade que o jogo traz, como aborda Kishimoto (2004). Conforme cresce a evolução e o crescimento do mercado de jogos eletrônicos, assim também passa a crescer a preocupação na entrega de uma melhor experiência para o usuário, exigindo assim uma elaboração mais inteligente das IAs, desde a elaboração de personagens nos jogos até os cenários utilizados no mesmo.

De acordo com Kishimoto (2004), nos primeiros jogos eletrônicos desenvolvidos, a IA era conhecida por “programação de jogabilidade” pois eram desenvolvidas sem a intenção de interferir bruscamente nos jogos, sendo utilizadas somente para programações básicas, como a movimentação de personagens. Conforme os anos foram passando, a necessidade de boas técnicas de desenvolvimento foi sendo trabalhadas, à medida que o mercado, paralelamente, foi se desenvolvendo e crescendo também. Funcionalidades novas, demandas novas, empresas sempre buscando destaques em um mercado que ainda engatinhava para uma evolução de destaque, como conhecemos hoje em dia.

Ano	Descrição	IA utilizada
1962	Primeiro jogo de computador, Spacewar, para 2 jogadores.	Nenhuma
1972	Lançamento do jogo Pong, para 2 jogadores.	Nenhuma
1974	Jogadores tinham que atirar em alvos móveis em Pursuit e Qwak.	Padrões de movimento
1975	Gun Fight lançado, personagens com movimentos aleatórios.	Padrões de movimento
1978	Space Invaders contém inimigos com movimentos padronizados, mas também atiram contra o jogador.	Padrões de movimento
1980	O jogo Pac-man conta com movimentos padronizados dos inimigos, porém cada fantasma (inimigo) tem uma “personalidade” sobre o modo em que caça o jogador.	Padrões de movimento

Tabela 1 - Linha de tempo da IA em jogos
Fonte: (SCHWAB, 2004)



Conforme a Tabela 1 mostra, pode-se analisar a evolução do uso de IAs e principalmente a evolução no desenvolvimento das mesmas de acordo com Schwab (2004), também pode-se ver a similaridade entre o crescimento e o desenvolvimento de jogos eletrônicos mais complexos com o uso das IAs. Pode se destacar, conforme se passava as décadas, a constatare evolução das técnicas de IAs que os desenvolvedores vinham utilizando.

De acordo Yamamoto (2002), conforme cresce o mercado de jogos em aspectos de qualidade, aumenta também a exigência de um jogo bem desenvolvido e trabalhado. A medida que a exigência cresce, a evolução no desenvolvimento de IAs é extremamente importante, levando em consideração que a experiência do usuário seja o ponto crucial para o sucesso de um jogo no mercado. Tendo em vista que o mercado de jogos eletrônicos se encontra em uma grande alta, tanto de usuários quanto desenvolvedoras e seus jogos, o ponto crucial que destaca e diferencia um jogo eletrônico, é a forma em que ela é desenvolvida e se a mesma causa um impacto positivo no usuário final.

Para Ricardo Rodrigues (2021), os anos 80 e 90 foram marcados por uma grande evolução no mercado, primeiro pelo lançamento de revistas como "Computer and Video Games" (1981) e "Computer Gaming World" (1981), onde incentivou a formação das primeiras comunidades gamers, onde usuários poderiam compartilhar suas experiências em seus diversos jogos. O outro marco importante foi a expansão da internet nessa época, se tornando mais popular, mudou não somente o estilo de vida das pessoas, mas também ajudou no crescimento do mercado de jogos, trazendo consigo o lançamento de novas plataformas, como o Windows '95 com uma possibilidade de conexão com a internet, tornando possível agora a migração de jogos eletrônicos dos consoles para as telas dos computadores.

Com o nascimento e o crescimento de grandes comunidades gamers, a troca de informações entre os usuários facilitou o crescimento de grandes desenvolvedoras que se destacavam, entre elas a famosa Nintendo, Sony, Sega, entre outras, onde elas disputavam posições no mercado, buscando ser um diferencial. Com essa evolução, grandes ferramentas foram sendo utilizadas e desenvolvidas em IAs, dando destaque a primeira aparição do famoso jogo Super Mario Bros, onde com uma simples mecânica de colisão, dependendo de como você colide com o inimigo te trará um benefício ou um malefício, o jogo traz uma experiência diferente a aquela época, sendo vista hoje como uma obra prima.

2.1 Jogos com suas aplicações em IAs

Considerando a evolução de IAs em jogos eletrônicos, programadores e desenvolvedores utilizam diversos algoritmos, que a cada período são implementados com o objetivo de melhorar, não só o desenvolvimento de jogos, mas a experiência que ela carregará para o usuário final. Entre diversos algoritmos aplicados, ganha-se destaque alguns deles como os determinísticos, padrões de movimentos, máquinas de estados, lógica fuzzy, algoritmos de busca como A*, dijkstra e waypoints, algoritmos genéricos e redes neurais.

Para Alex Lattaro (2018), jogos eletrônicos possuem um simples objetivo, a diversão,

colocando essa característica em prioridade podemos analisar alguns algoritmos aplicados em jogos lançados no mercado. Devem ser vistos pontos como, a interação do jogo com o usuário, a assimetria do comportamento segundo essa interação com o usuário, em alguns aspectos, pode ser vista também a intencionalidade que o algoritmo apresenta, sua ampla rede de possibilidades, levando o usuário a ter mais opções de escolhas e interatividades com o jogo.

Jogos como a famosa franquia GTA, possuem uma característica própria em seu desenvolvimento, utilizando-se do algoritmo genérico, existe uma possibilidade de se desenvolver um DNA próprio, aonde valores e parâmetros próprios são desenvolvidos para determinada ação do usuário. Analisando uma determinada ação disponível no jogo como, a liberdade de interagir com qualquer pedestre, podemos ver esse algoritmo em ação, onde todos refletem uma ação segundo a interação do usuário.

Outra ação analisada no mesmo jogo acontece quando chega o anoitecer e pode se ver NPC (Personagens não jogáveis) chegando em seus carros a frente de suas casas, assimilando a trabalhadores chegando de seus serviços. Detalhes como esse e outros presente nos jogos acrescentam de forma significativa na experiência que o usuário irá ter ao presenciar tais momentos.

Outra ferramenta que recheia a experiência do usuário, é a rede neural, que, segundo Lattaro (2018), é utilizada quando o sistema precisa aprender a interagir com o jogador de maneira inteligente, ou seja, a rede neural implementada dentro de um jogo possui a finalidade de aprender com o usuário e imitar seus pensamentos, fazendo assim um jogo mais desafiador, e extremamente intuitivo, levando o usuário a ter uma experiência diferente de outros jogos disponíveis no mercado.

Tal funcionalidade é implementada dentro de jogos da franquia FIFA mais atuais, aonde segundo seus desenvolvedores, a IA programada possui a finalidade de aprender com o usuário, olhando suas táticas, movimentos e ações tornando assim um jogo mais desafiador para o usuário. Assim como diz Thiago Fachini, "FIFA é desenvolvido para ser um jogo completo, e proporcionar uma experiência futebolística (e até mesmo de gestão futebolística) plena. E é inviável projetar uma experiência futebolística satisfatória sem construir um mecanismo que permita ao videogame confrontar as habilidades do usuário e desafiá-lo a jogar mais e melhor." Perceber-se a importância que as IAs vem trazendo no mercado de jogos. Desde grandes desenvolvedoras até desenvolvedores solos buscam fazer um trabalho com excelência, fugindo de um jogo não fluido, trazendo para o usuário.

Observa-se que a experiência do usuário é um dos fatores determinísticos para o sucesso de um jogo, desde os mais complexos até o mais simples, como pode analisar-se no jogo Flappy Bird, lançado em 2013, o jogo possui uma mecânica simples porém desafiadora para o usuário, aonde a maior dificuldade é passar pelos espaços vazios deixados por canos na tela de forma aleatória, contabilizando assim os pontos. Tal mecânica fez com que usuários tentassem cada vez mais bater seu próprio recorde, enfrentando assim, novamente o mesmo desafio.

3. TIPOS DE IAS E SUAS APLICAÇÕES

Como descreve Coppin (2004), o mercado de jogos tem crescido e despertado enorme interesse para desenvolvedores utilizarem inteligências artificiais, porém, deve se preocupar com a qualidade em que essa ferramenta poderosa está sendo trabalhada. Atentar e pontuar características nesse desenvolvimento, ajudam a entender como usuário final experimentará esse produto, além de ser um ponto de grande interesse para aqueles que buscam entregar um produto de qualidade com um diferencial no mercado.

De acordo com Yamamoto (2002), conforme cresce e evolui a tecnologia, paralelamente a isso, no mercado dos jogos, as IAs se tornaram ferramentas cada vez mais presentes e atualizadas conforme a demanda. A primeira aparição dessa ferramenta aconteceu na década de 50, onde o jogo "OXO", tinha com o objetivo simples de duelar contra o usuário. Desde então, pode se analisar um avanço em novas técnicas para o desenvolvimento.

3.1 Técnicas de programações de IAs

Podemos destacar técnicas como, algoritmos determinísticos, que tem como o objetivo produzir com uma certa entrada de dados, sempre a mesma saída. Um problema pode ser visto quando colocamos em ênfase que essa entrada será comandada por um usuário, que, buscando ter uma experiência diferente, inserirá dados aleatórios que muitas vezes não é computado pelo algoritmo, diminuindo assim uma entrega diferente ao usuário, podendo-o levar a uma queda na expectativa, que muitas vezes resultam em um prejulgamento do desenvolvedor.

Outras técnicas como padrões de movimentos que inclui algoritmos de perseguição e evasão, pode possuir o mesmo problema, se não analisado e trabalhado antecipadamente pelo desenvolvedor, buscando caminhos diferentes que muitas vezes passam despercebidos pelos próprios quando estão em fase de produção dos jogos. Tendo em vista o grande número de jogos no mercado, além da preocupação de possuir uma ideia original ou um diferencial, o desenvolvedor precisa se preocupar com a qualidade em que o algoritmo entrará em contato com o usuário.

Kishimoto (2004), explica que em virtude da grande demanda desse mercado, novas técnicas são desenvolvidas com o objetivo de entregar uma IA mais similar ao comportamento humano, implementando assim algoritmos e motores dos jogos. Porém uma dificuldade é vista ao encontrarmos desenvolvedoras independentes e muitas vezes grandes empresas do setor, tratem essa abordagem de maneira superficial, entregando assim, um produto que não atende as expectativas do consumidor final, frustrando o mesmo que muitas vezes julgam de maneira antecipada o setor de jogos eletrônicos por conta de uma má experiência.

Pode se destacar o jogo FIFA, da desenvolvedora EA Sports, onde é o maior jogo do ramo futebolístico, tendo esse título de maneira honrosa, pois eles buscam a cada lançamento entregar uma experiência diferente ao usuário final. Tendo o foco no usuário e em como ele usufruirá esse produto, a EA Sports desenvolve o jogo utilizando diversas

técnicas de programação avançadas, com IAs de alto nível, visando a experiência do usuário. Além de possuir uma programação que cuida da parte visual do jogo como, a física do cabelo, das roupas, expressões faciais, entre outras coisas, a desenvolvedora também possui uma IA trabalhando na gestão futebolística, onde a IA analisa os movimentos do usuário, sua formação, estratégias de jogadas criadas com mais frequência, desafiando assim as habilidades do usuário fazendo com que ele jogue melhor e por mais tempo.

Outra técnica que ganha destaque são as máquinas de estados finitos, por conta da sua facilidade de implementação, essa técnica é bastante utilizada em jogos atuais. Sua praticidade se consiste em definições de diversos tipos de estados, onde cada estado representa uma ação do objeto em trabalho. Em um jogo considerado baixo nível de programação, ou seja, um programa simples, pode se usar máquinas de estados para definir controles de robôs que, em cada robô, possui diversos estados como, perseguir o jogador, evitar o jogador, mover aleatoriamente, parar por um momento. Tais estados são determinados por fatores como a distância desse objeto ao personagem e até mesmo o tempo.

Uma aplicação que usa esse tipo de técnica é o famoso jogo Half-Life, desenvolvido pela Valve, um jogo de ação no estilo "tiro em 1ª pessoa" com um objetivo principal traçado pela história que o guia. O jogo ganhou muita popularidade por conta da sua história e sua avançada implementação de IA. Pode-se analisar essas características quando observamos as ações dos inimigos, onde os mesmos foram implementados com máquinas de estados com listas que definem diversas ações. Cada estado define uma lista de atitudes que estarão disponíveis. Por exemplo, em um determinado momento os inimigos podem escolher fugir ou ir pra o combate, verificando a energia do jogador, para onde ele está mirando, quantos têm do seu próprio tipo e se eles possuem energias suficiente para o combate.

Técnica como essa distribui uma vasta lista de possibilidades de desenvolvimentos, tendo em vista o fator mais importante, a interação do usuário. Ao colocar funções vastas em um jogo, possibilita que o usuário não apenas interaja com essas funções, mas o leve para um caminho diferente do esperado. A fim de exemplo, pode-se pegar um jogo desenvolvido em um cenário de velho oeste, aonde o principal objetivo é andar de cavalo o mais longe possível nesse cenário. Ao colocar opções fora do objetivo principal, como por exemplo, poder interagir com bares de cidades do velho oeste, criaria uma quebra de expectativas positivas no usuário, pois seria entregue a ele, mais do que o esperado.

Máquinas de estados finitas, podem ser uma grande ferramenta, porém ao decorrer de um tempo, essa ferramenta desenvolvida em jogos passa a ser previsível para alguns jogadores, podendo assim, levá-lo a um estado negativo de experiência. Uma alternativa para esses problemas é utilizar máquinas de estados fuzzy, que diferente da máquina de estado finita, onde seus processos são restritos somente a uma situação em um determinado momento, na fuzzy, encontramos essa mistura de características de mais de uma situação ideal, fazendo assim um jogo mais fluido e o máximo longe de padrões robóticos nas ações dos objetos dentro dos jogos.

The SIMS, um jogo A-life, que simula aspectos da vida real, utiliza-se de técnicas de máquinas de estado fuzzy, onde as ações relacionadas a um item jogável, são armazenadas no próprio, permitindo uma interação completa entre vários Sims, nomes dos personagens que são criados oro jogadores. The SIMS é um jogo com infinitas possibilidades, onde seu principal objetivo é controlar casa com famílias e suas interações com o mun-



do. Cada personagem criado possui diversos atributos, como traços de personalidades, aparências, sexo, cor, idade, e todos os atributos interferem diretamente na forma que o usuário irá jogar.

Uma técnica muito utilizada em conjunta com outras já citadas é o Pathfing, que consiste basicamente em encontrar o caminho de um ponto específico, o p1, até o objetivo, p2. Seu uso possui sua importância pois é bastante usada para traçar rotas de inimigos, rotas de NPCs, rotas de carros, ou seja, basicamente se o objetivo buscado é traçar uma rota, a técnica mais indicada é esta. Em uma situação simples, onde não haverá obstáculos nessa rota, o caminho direto já se torna suficiente, porém se houver obstáculos, será preciso evitá-los.

Junto com essa técnica, havendo obstáculos, existem caminhos a se seguir. O primeiro desses caminhos é por tentativa e erro, que sua aplicação é ativada quando o objeto encontra um obstáculo, não tão grande e convexos, onde o objeto recua e tenta uma nova direção por um momento e depois retorna à direção original. O segundo caminho é seguindo o contorno do obstáculo, fazendo testes periódicos para verificar se ele ainda está interceptando.

Um exemplo clássico é o Midtown Madness 2, um jogo de corrida que ocorre em uma cidade, cujo objetivo principal é vencer corridas com obstáculos simulados como reais, tráfego de carros, pedestres, ruas, áreas abertas e cruzamentos. Além dessa ferramenta, outra ferramenta implementada é a de tomada de decisões, onde, no tráfego de carros, são constantemente verificados, se é para parar, não parar, de acordo com alertas e semáforos, a verificação constante da distância do carro a frente para evitar colisão. Ocorre de maneira similar nos pedestres, onde se movem pelas calçadas, desviando de obstáculos estáticos, e dinâmicos. Uma ação observada é o desvio que o pedestre faz quando o jogador chega perto com seu carro.

Porém, o caminho mais seguido é a do Waypoint Pathfinding, onde se utiliza de inúmeras rotas interligando todos os pontos principais em um mapa, aonde cada ponto, ou grafo, contém informações sobre como chegar até os outros pontos vizinhos. Tais técnicas formam e preenchem o desenvolvimento com suas peculiaridades, tendo como objetivo, além de resolver problemas de desenvolvimentos, criar algo que seja divertido, para o consumidor final, o jogador.

Outro exemplo para uso de rotas se encontra em jogos de corrida, aonde em uma pista, diversas rotas podem ser definidas de acordo com a posição do carro, ou seja, cada rota possui uma característica diferente, seguindo a rota e eventualmente mudando de rota, conforme muda a medida em curvas ou até mesmo quando existirem carros em sua frente.

Um estilo de jogo que se utiliza poderosamente também de implementações de IAs são os jogos no estilo de esportes, onde o principal objetivo é similar esportes reais que geralmente envolvem times. Grande exemplo disso são os jogos da série FIFA Soccer, com o objetivo de simular o futebol real.

Sua implementação consiste em trabalho de equipe onde a cooperação e a troca de informações entre os jogadores são essenciais para alcançar o objetivo final. A aplicação

desse estilo se consiste em definição de posicionamento dos jogadores no campo, máquinas de estados finitos, onde cada jogador possui características e atributos diferentes de acordo com sua posição, caminhos traçados de acordo com cada estratégia usada no jogo etc.

Como pode-se observar e analisar, ter domínio e diversificação de técnicas de IAs é um fator importante para desenvolvedores, além de permitir que cada um escolha a técnica que mais encaixa em seu projeto, ter um vasto conhecimento permite experimentar de outras técnicas abrindo assim possibilidades infinitas de criações em jogos digitais.

4. EXPERIÊNCIA DO USUÁRIO EM JOGOS ELETRÔNICOS

Tânia d’Arc (2021) conceitua de maneira simples que a experiência do usuário está ligada a interação que uma pessoa tem com um sistema, produto ou serviço, tirando suas percepções antes, durante e depois dessa interação. Visando a satisfação do usuário, as diversas formas em que um jogo pode se apresentar e entregar uma boa experiência, possuir uma boa estrutura desenvolvida se torna essencial. As desenvolvedoras possuem uma grande responsabilidade com essa entrega, pois o consumo do jogo só é possível se ele entregar uma boa experiência.

Émilie Calas e Marianne Javelot (2020) destaca cinco pilares da experiência do usuário, onde possuem o objetivo de proporcionar ao usuário final boas experiências. O funcionamento de um sistema possui um peso de importância para que esse resultado possa ser alcançado. Destacando não apenas a funcionalidade de IAs, mas a sua implementação, possuir esses pilares é de extremo valor para que os programadores possam conseguir entregar essa satisfação para seus usuários.

Resumidamente, Tânia d’Arc (2021) descreve esses pilares em três pontos importantes a serem analisados pelas empresas, visando que de maneira hierárquica, cada ponto possui uma importância única de acordo com as necessidades do consumidor. São eles; A funcionalidade, ponto mais importante, pois o sistema tem que ser capaz de realizar as funções nas quais foram desenvolvidas; A usabilidade, que tem como características importantes a serem analisadas como a facilidade do uso, acessibilidade, intuitividade e eficiência; E o desejo, onde o papel mais importante é possuir uma característica atrativa. O entendimento desses pontos é de suma importância para as desenvolvedoras que buscam implementar essa experiência do usuário, tendo em vista o principal objetivo: levar o consumidor a ter a melhor experiência com o seu produto, resultando não apenas em uma satisfação do usuário final, mas em uma divulgação positiva da empresa em um setor onde a avaliação é um ponto crucial.

Tendo em vista que a funcionalidade possui um papel fundamental no desenvolvimento dos jogos e que o mesmo possui interferência direta na experiência do usuário, buscar compreender e dominar as ferramentas de desenvolvimento se torna uma obrigação exigida dos desenvolvedores. Junto com isso, a usabilidade é um fator paralelo a se analisar no desenvolvimento, tendo o objetivo trazer uma experiência de nível alto para o usuário.



Outro fator importante que influencia para que o usuário tenha uma experiência relevante, é a dificuldade encontrada em jogos. Para Mirna Paula (2015), definir o peso da dificuldade em jogos possui um grande desafio, pois, por ter uma definição subjetiva, chegar a um resultado concreto varia de diversos fatos, tanto internos nos jogos, quanto externos no usuário.

Como diz Mirna Paula (2015,), "O ajuste de dificuldade não é tão simples quanto disponibilizar itens que recuperem a saúde/vida do jogador quando ele estiver enfrentando uma situação qualquer. Este é um problema que envolve estimar quando e como intervir, já que manter o jogador desafiado e interessado é uma tarefa complexa em contextos iterativos". O objetivo principal que se busca, é manter o jogador desafiado e interessado nessa tarefa, ou seja, busca-se a imersão do jogador, e para isso, ter um balanço dinâmico da dificuldade é crucial.

Para Mirna Paula (2015), um aspecto importante no desenvolvimento de jogos, e que ainda não é tão explorada é o balanceamento de dificuldade, que consiste em alterar comportamentos do jogo buscando evitar que o jogador tenha uma experiência frustrada com um jogo onde a dificuldade é alta ou até mesmo entediante com uma dificuldade baixa. É necessário levar em consideração esse balanceamento, pois usuários possuem habilidades diferentes, formas de resolver problemas de maneiras diferentes. Com isso a criação de um padrão nunca será suficiente, podendo assim se tornar um jogo com um extremo, sendo ele entediante ou frustrante. Com isso é necessário o desenvolvimento de jogos onde há um mapeamento das características do usuário, buscando dados e informações do seu comportamento em relação a atividades elaboradas durante sua jogabilidade.

É observado esse nível de dificuldade quando se leva em consideração aspectos dos jogos, como o Level Desing, a IA aplicada e parâmetros definido no jogo. O ajuste dessa dificuldade no Level Desing, consiste em fazer alterações físicas nos cenários dos jogos enquanto o jogo está sendo executado pelo jogador, como descreve Mirna Paula (2015). Este tipo de ajuste, ainda pouco explorado, já vem sendo aplicado em jogos no estilo de corrida, onde o a pista se adapta a forma como o jogador reage a obstáculos.

Essa aplicação de ajuste no meio da IA, segundo Mirna Paula (2015), consiste em desenvolver NPCs, que possuem características mais próximas a do jogador, criando assim uma genética com os melhores NPCs, porém tal técnica possuem falhas durante sua execução. Se em um determinado momento o jogador regrida com suas habilidades, o NPC não é capaz de regredir ao ponto de estar no mesmo nível que o jogador. Com isso, uma solução foi encontrada quando se coloca o ponto de aprendizagem no próprio NPC, fazendo assim com que ele aprenda com seus erros e evolua, tornando assim um jogo evolutivo, divertido e desafiador para o jogador.

Ajustar esse nível de dificuldade balanceando os parâmetros, segundo Mirna Paula (2015), consiste em realizar modificações que alterem na quantidade dos recursos disponibilizados pelo mapa, como itens de cura, vidas, armas, munições. Caso o jogo fique difícil, mais itens aparecem, se o jogo fica fácil, mais inimigos aparecem e é reduzido os recursos que aparecem.

5. CONSIDERAÇÕES FINAIS

Ao iniciar esse trabalho de pesquisa constatou-se que havia uma dúvida sobre a influência da inteligência artificial na experiência dos usuários de jogos eletrônicos, esta dúvida se iniciou primeiramente com caráter formativo do(a) aluno(a) para o mercado que é ágil e entender o seu funcionamento, logo, constata-se que o objetivo geral foi atendido por que efetivamente o trabalho conseguiu identificar a influência da inteligência artificial na experiência dos usuários de jogos eletrônicos, conceituando seus pontos positivos e negativos, com isso o objetivo foi atendido com sucesso.

O meu objetivo inicial era entender como a inteligência artificial era utilizada em jogos eletrônicos, ele foi atendido por que as próprias metodologias estudadas apresentam conceitos e pontos, que considero importante no desenvolvimento em empresas de grande porte ou em desenvolvedoras independentes, a fim de obedecer a demanda do mercado atual.

O segundo objetivo era identificar técnicas e ferramentas usadas na inteligência artificial, mostrando pontos negativos e positivos, visando a experiência que o usuário passaria, ele foi atendido, pois, os estudos abordados mostram como essa influência age nos usuários, tanto de maneira negativa quanto positiva, além de identificar e situar tipos de inteligências artificiais usada no mercado.

O último objetivo tinha como propósito, entender sobre a experiência do usuário e quais os meios que, de acordo com a pesquisa, se tratava o melhor caminho para a resolução de um problema causado pela influência de IAs desenvolvidas sem entender o caminho da experiência do usuário, tendo sido atendida, pois foi demonstrada pontos no quais são importantes para que esse caminho consiga êxito.

A pesquisa então partiu da hipótese de que a influência da inteligência artificial agia na experiência de usuários de jogos eletrônicos, sendo analisada essa influência tendo o foco na experiência do usuário final, mostrando métodos que influenciam negativamente e métodos que influencia positivamente nessa experiência do usuário.

O problema se tratava exatamente em entender qual a influência da inteligência artificial na experiência do usuário de jogos eletrônicos, ele foi atendido pois foram levantados pontos considerados importantes, tanto positivos quanto negativos no desenvolvimento dessas IAs que influenciam na experiência dos usuários, trazendo conceitos e metodologias.

Este trabalho foi feito a partir de livros, artigos, dissertações e sites da internet datados em até 21 anos, todos foram pesquisados no ano de 2021, neste trabalho também seria interessante ter questionários atuais feitos pelo(a) aluno(a) sobre o tema, se esse ponto fosse aberto, infelizmente, estamos no segundo ano da pandemia, e visitas ficam mais difíceis de serem feitas as empresas locais, mas, para os futuros acadêmicos recomendo que esse seria um ponto forte para embasar o trabalho de conclusão de curso pois apresentamos visões de profissionais da área sobre o tema.

Referências

- AIOT BRASIL 2021. **FIFA 21 aposta na inteligência artificial. 2020**. Disponível em: <https://aiotbrasil.com.br/tecnologia/as-novidades-do-fifa-21/> .Acesso em 17 nov. 2021.
- CALAS, Émilie, JAVELOT, Marianne, 2020. **Experiência do usuário: o que é? Veja 5 passos para melhorar!** Disponível em: <https://blog.crossknowledge.com/pt/experiencia-do-usuario/> .Acesso em 17 nov. 2021.
- COPPIN, Ben. **Inteligência Artificial**. 1ª Edição. Rio de Janeiro: LTC, 2004.
- D'ARC, Tânia. 2021. **Experiencia do usuário: o que é, como fazer e como otimizar**. Disponível em: <https://www.smarthint.co/experiencia-do-usuario/> .Acesso em 17 nov. 2021.
- GÁMEZ, E. H. C. **On the Core Elements of the Experience of Playing Video Games**.2009. 208 f. Tese de doutorado - UCL Interaction Centre Department of Computer Science, 2009.
- KISHIMOTO, A.: **Inteligência artificial em jogos eletrônicos**. 2004. Disponível em: https://www.academia.edu/2231411/Intelig%C3%Aancia_Artificial_em_Jogos_Eletr%C3%B4nicos . Acesso em: 25 abr. 2021.
- LACERDA, Mauricio. **Inteligência Artificial em Jogos**. Disponível em: https://www.researchgate.net/publication/267805759_Inteligencia_Artificial_em_Jogos . Acesso em 25 mai. 2022.
- LAMOTHE, André. **Tricks of the Windows Game Programming Gurus**. USA: Sams, 1999.
- LATTARO, Alex. 2016. **Aplicações práticas de inteligência artificial em games**. Disponível em: <https://imasters.com.br/desenvolvimento/aplicacoes-praticas-de-inteligencia-artificial-em-games> . Acesso em 17 nov. 2021
- RODRIGUES, Ricardo. **Da primeira à última geração: a evolução dos jogos eletrônicos**. 2021. Disponível em: <https://blog.ingrammicro.com.br/gaming/evolucao-dos-jogos-eletrnicos/> .Acesso em: 17 nov. 2021.
- SALTZMAN, Marc. **Game Design - Secrets of the Sages**. USA: Macmillan, 2000.
- SAVI, Rafael. VON WANGENHEIM, Christiane Gresse. ULBRICHT, Vania. VANZIN Tarcisio. Proposta de um Modelo de Avaliação de Jogos Educacionais. 2010. Disponível em: <http://seer.ufrgs.br/renote/article/view-File/18043/10630> .Acesso em: 25 abr. 2021.
- SCHWAB, Brian.: **AI Game Engine Programming**. Hingham: Charles River Media. 2004.
- SILVA, Mirna Paula, **Inteligência Artificial Adaptativa para Ajuste Dinâmico de Dificuldade em Jogos Digitais / Mirna Paula Silva**. — Belo Horizonte, 2015
- TOZOUR, P.: **The Evolution of Game AI from AI Game Programming Wisdom**. Hingham: Charles River Media. 2002.
- YAMAMOTO, F. S.: **Inteligência Artificial em Jogos Eletrônicos Interativos**. Universidade de São Paulo - EPUSP, 2002.

CAPÍTULO 5

SEGURANÇA DA INFORMAÇÃO

INFORMATION SECURITY

Alexsandro Pereira Azevedo¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

Este trabalho tem como objetivo de explicar acerca da segurança da informação, destacando os principais conceitos e teorias sobre o assunto. Partindo da carência na segurança de informações e dados pessoais, originou-se a dúvida de como solucionar tal problema, com normas metodológicas de prevenções de fácil entendimento para qualquer tipo de usuário. De acordo com registros dos autores pesquisados, observou-se que a falha na segurança se originou desde os primórdios da humanidade, com mais ênfase a partir do início do século XX, porém tem-se soluções e precauções nas quais o usuário pode utiliza-las de forma simplificada.

Palavras-chave: Segurança da Informação; Infraestrutura de TI; Criptografia; Ativos corporativos.

Abstract

This paper aims to explain about information security, highlighting the main concepts and theories on the subject. Starting from the lack of security of information and personal data, originated the doubt on how to solve such problem, with methodological prevention rules that are easy to understand for any type of user. According to records of the authors surveyed, it was observed that the security flaw originated from the dawn of humanity, with more emphasis from the beginning of the twentieth century, but there are solutions and precautions in which the user can use them. in a simplified way.

Key-words: Information Security; IT infrastructure; Cryptography; Corporate Assets.

1. INTRODUÇÃO

A segurança da informação visa garantir a integridade, confidencialidade e disponibilidade dos dados de um banco de dados, para que as informações existentes não sejam utilizadas por pessoas não autorizadas, que por consequência, resultando em danos irreparáveis ao verdadeiro detentor de tais informações. Com o avanço da internet das coisas, é fundamental falar em segurança da informação, com o surgimento de novos gadgets, equipamentos e plataformas online, onde são armazenadas as informações de usuários na rede, surgiu também ações maliciosas para interceptar e captar os dados dos usuários, com base nessas circunstâncias, este trabalho demonstrará possíveis soluções para tal problema.

Percebe-se que na sociedade contemporânea, ao mesmo tempo em que as informações são consideradas de suma importância para uma empresa, as mesmas estão sob constantes riscos. A sua perda constitui em prejuízo para a organização detentora da mesma, podendo até mesmo ser crucial para a sobrevivência da organização. A informação é algo que não se deteriora com o tempo, ela é reutilizável em outras ocasiões e tem seu valor determinado pelo usuário. A informação só é perdida quando não administrada adequadamente ou quando não é protegida corretamente, acarretando em consequências graves dependendo do grau de importância da mesma.

Qual a importância da segurança da informação para a sociedade contemporânea? É necessário destacar e apresentar políticas de segurança da informação para que as empresas não tenham prejuízos por perdas de informações internas, sejam elas sigilosas ou não, como por exemplo: senhas; dados importantes de funcionários; dados restritos; plano de negócios; etc.

Este trabalho de conclusão de curso tem como objetivo demonstrar conceitos e metodologias acerca de sistemas da informação. No primeiro capítulo “teorias de segurança da informação” demonstrando como assegurar as informações de dados, no capítulo 2 “Normas e padrões metodológicas de segurança da informação” demonstrando normas, padrões e metodologias aplicadas em segurança da informação e por fim no capítulo 3 “Segurança da informação no ambiente corporativo”.

A metodologia de pesquisa utilizada neste estudo caracteriza-se como uma revisão de literatura de caráter descritiva que vem abordar acerca da importância da segurança da informação. Portanto, esta pesquisa será realizada por meio de trabalhos publicados nos últimos 25 anos e irá abordar o seguinte descritor para a pesquisa: Segurança da informação.

2. TEORIAS DE SEGURANÇA DA INFORMAÇÃO

2.1 Apontar os conceitos de segurança da informação

Para ser utilizada, a informação necessita garantir três características fundamentais: a integridade, a disponibilidade e a confidencialidade, características que devem ser preservadas, pois são tidas como princípios da segurança da informação (DANTAS, 2011, p 11).

A segurança da informação (SI) 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 ISO/IEC 27002:2005).

Ao se falar em segurança da informação, deve-se levar em consideração essas qualidades da informação, pois toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança (DANTAS, 2011, p 11).

A tríade CIA (*Confidentiality, Integrity and Availability*) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger.

2.1.1 Confidencialidade

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas (NBR ISO/IEC 27002:2005).

Quando ocorre a quebra da confidencialidade da informação, conteúdos sigilosos da empresa estará em risco, tais como: dados bancários; informações sigilosas de funcionários, entre outros.

2.1.2 Integridade

A integridade é a garantia da exatidão da informação e dos métodos de processamento entre um transmissor e um receptor (NBR ISO/IEC 27002:2005).

De acordo com Dantas (2011, p. 11) "garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente." Toda empresa comunica-se interna e externamente o tempo todo, transmitindo dados em todas as direções, e a comunicação efetiva só acontece quando o emissor e o receptor da informação a interpretam da mesma maneira, e ocorre a quebra da integridade quando a informação é corrompida, alterada, roubada ou destruída.

da sem autorização. A informação deve ser mantida em sua condição original, ou seja, da mesma forma na qual foi concebida.

Existem meios para que a integridade de dados não sejam comprometidas acidentalmente ou intencionalmente, são chamadas restrições de integridade, que servem para garantir que os dados não sofram modificações por pessoas não autorizadas. São elas:

- Restrição de Chave: Impedir que uma chave primária seja repetida e/ou duplicada. Tendo o registro único, garantindo a proteção dos dados.
- Restrição de Domínio: Impede que a chave primária receba um valor nulo, garantindo que a chave primária de cada tabela seja única.
- Integridade de vazio: Complementa a restrição de domínio, mas neste caso, proíbe valores vazios.
- Integridade referencial: A chave estrangeira precisa coincidir com o mesmo nome da chave primária, não somente o mesmo nome do campo, mas também os valores de referência.

2.1.3 Disponibilidade

A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, sem perda de tráfego (NBR ISO/IEC 27002:2005).

Assim, foi mencionado que “disponibilidade, significa garantir que a informação possa ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções” (BENETTI, 2015). A informação necessariamente precisa estar disponível e que ocorre a quebra da disponibilidade quando a informação está indisponível para ser acessada pelos usuários, geralmente causando uma negação de serviço.

2.2 Criptografia

De acordo com Weber (1995, p. 3) “a finalidade básica de um criptosistema é cifrar uma mensagem através de um método de cifragem[...]” Quando os dados são cifrados, é aplicado um ou mais algoritmos para codificá-los de modo que os dados não tenham mais o formato original para que não possam ser lidos sem um algoritmo de descifragem.

Para Weber (1995, p. 2) “a criptografia contemporânea não é mais baseada em obscuridade, ou seja, não se utiliza mais a suposição de que qualquer sistema pode ser seguro na medida em que ninguém, exceto seus criadores, tem acesso à metodologia ou aos algoritmos utilizados internamente ao sistema.” Nenhum sistema estará sempre se-



guro, pois a cada momento surgem novas formas de quebrar a criptografia contida numa informação. É necessário estar sempre atualizando o algoritmo de criptografia, para que um atacante não tenha acesso as informações de um banco de dados.

Criptosistemas distintos possuem diferentes graus de segurança, dependendo da facilidade ou da dificuldade com que eles são atacados e quebrados. Um sistema é dito incondicionalmente seguro se ele é teoricamente inquebrável, ou seja, não interessa qual a quantidade de texto normal ou cifrado a disposição, nunca se tem informação suficiente para deduzir as chaves utilizadas ou decifrar um texto cifrado qualquer (WEBER, 1995).

Todos os métodos de criptografia desenvolvidos até agora são quebráveis, desde que haja recursos computacionais para quebrá-los, alguns necessitam de grande poder computacional para quebra-los por causa do grau de sua complexidade na qual foi desenvolvido. Segundo Weber (1995, p. 6):

Se o custo requerido para quebrar um sistema (ou decifrar uma mensagem) é maior que o valor da informação que será obtida, então para todos os fins práticos, o sistema é seguro [...] a criptologia atual está mais preocupada com os aspectos computacionais do que com o valor da informação, e assim os criptosistemas normalmente são classificados como computacionalmente seguros ou não [...].

Os métodos de criptografia estão se atentando mais ao poder computacional requerido para descriptografar do que com o próprio valor da informação que será protegida, mas deve-se salientar que o nível de poder computacional tende a crescer com os avanços na tecnologia computacional, necessitando um aprimoramento nas técnicas de descriptografia caso contrário, as informações dos dados serão comprometidas por um atacante.

2.2.1 Criptografia tradicional

Antes da era dos computadores eletrônicos, já existiam métodos de criptografia para fins de codificar mensagens como por exemplo as mensagens de balística. Estes métodos consistiam em realizar substituição de caracteres por outro ou trocando caracteres de posição, são eles: substituição e transposição.

Métodos de substituição: Cada caracter na mensagem é substituído por outro na mensagem, com objetivo de tornar o texto incompreensível, existem vários tipos de métodos de substituição, são eles:

- Substituição monoalfabética: cada caracter é substituído por outro, de acordo com uma tabela ou uma regra simples. A cifra mais antiga conhecida é a chamada Cifra de César, onde cada caracter é substituído por três caracteres adiante do alfabeto.
- Substituição monofônica: Consiste em operar como a substituição monoalfabética, mas agora cada caracter da mensagem original pode ser mapeado para um ou vários caracteres na mensagem substituindo-os por números.

- Substituição polialfabética: Este método consiste em várias cifras de César utilizadas em sequência, com valores de deslocamento diferentes e obtidos a partir de uma palavra-chave poderiam ser usadas 4 tabelas, usadas em alternância a cada quatro caracteres.
- Substituição por polígramos: É um método que utiliza grupo de caracteres em vez de apenas trabalhar com caracteres individuais.
- Método de transposição: Cada caracter permanece inalterado, mas a sua posição na mensagem é alterada de acordo com alguma regra definida. A diferenciação entre um texto cifrado por substituição e outro por transposição é feita utilizando-se análise de frequência dos caracteres. Se a frequência for a mesma da língua, trata-se de uma transposição. Se não, tem-se uma substituição.

3. NORMAS E PADRÕES METODOLÓGICAS DE SEGURANÇA DA INFORMAÇÃO

Segundo Martins e Santos (2005) “a preocupação com a segurança dos sistemas computacionais não é recente. O processo de definição de regras e padrões de segurança iniciou-se na década de 60 (com o impulso da Guerra Fria) [...]”. Desde as grandes guerra que se tem preocupação com a segurança dos sistemas operacionais, tendo maior impulso com o início da Guerra Fria, porque cada informação era considerada valiosa e seria um grande prejuízo caso o outro lado obtivesse tal informação.

A implantação de um SGSI é baseada numa série de padrões e normas internacionais, são elas: (TECSEC, 1985), (ISO 15408:1999), (ISO/IEC TR 13335:1998), (BS7799-2:2001), (ISO/IEC 17799:2001) e (IEC 61508:1998).

3.1 Padrão BS7799 (Norma ISO/IEC 17799)

Anteriormente conhecida como padrão BS7799 “O objetivo destas normas é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas empresas” (MARTINS; SANTOS, 2005). Esta norma ISSO/IEC 17799 fornece uma base comum para desenvolvimento efetivo de práticas voltadas à segurança organizacional, pois serve de base para as outras normas e desenvolvimento de SGSI.

- BS7799-1 - *Code of Practice for Information Security Management*: É a primeira parte da norma contendo a introdução e definições de uso da norma.
- BS7799-2 - *Specification for Information Security Management Systems*: É a segunda parte da norma que define a base necessária para a construção de um SGSI.

Um SGSI é um sistema de gestão análogo a um Sistema da Qualidade e como tal é passível de certificação. Esta certificação se dá a partir das evidências (documentos e práticas) do conjunto de controles implantados e que devem ser continuamente executados e devidamente registrados. Este modelo de gestão está baseado no ciclo com melhoria contínua PDCA (Plan-Do-Check-Act).

Segundo Martins e Santos (2005) “a norma ISO/IEC 17799 surgiu num momento em que as organizações de todo o mundo passaram a investir muito mais em segurança da informação, muitas vezes sem orientação. Devido à sua notoriedade, a norma ISO 17799 passou a ser referenciada como sinônimo de segurança da informação. [...]”. Inicialmente não havia uma regra de segurança da informação bem definida a ser seguida, a norma ISO/IEC 17799 é utilizada para prever, prevenir e proteger possíveis vulnerabilidades ou brechas que um sistema possua, sendo elas de forma escrita, digitais e etc. “A norma contempla ao todo 127 controles, porém nem sempre é necessária a adoção de todos estes mecanismos para se atingir o patamar de segurança desejado” (MARTINS; SANTOS, 2005).

Os tipos de falhas trabalhadas na norma ISO/IEC 17799 envolvem desde os dados da informação até a estrutura física de TI, como por exemplo: Vírus, sites sem certificação de segurança, e-mails com links maliciosos e spam, danos materiais a máquinas da estrutura de TI.

3.2 Norma ISO/IEC TR 13335:1998)

Esta é composta por cinco partes que envolve a área de TI, são elas: conceitos e modelos para segurança em TI, gerenciamento e planejamento da segurança TI, técnicas para o gerenciamento de segurança em TI, seleção de proteção e proteção para conexões externas.

3.2.1 Conceitos e modelos para segurança em TI

Tem visão geral de modelos e conceitos fundamentais utilizados na gestão de segurança de TI.

3.2.2 Gerenciamento e planejamento da segurança de TI

Esta trata-se do relacionamento da área de SI com as outras áreas de uma organização. Seu ponto principal é a sugestão da criação de um comitê que envolve diversas ou maioria das áreas da organização principalmente a responsável pelos seus ativos, “Este comitê deve reunir-se periodicamente para definir os níveis aceitáveis de risco, cobrar e acompanhar resultados e reavaliar o projeto de segurança da informação quando necessário” (MARTINS; SANTOS, 2005).

3.2.3 Técnicas para o gerenciamento de segurança em TI

“Ela pode ser utilizada em conjunto com a norma BS7799-2, que sugere quais os processos (e não apenas as técnicas, como na ISO 13335-3) devem ser implantados na condução da gestão de segurança” (MARTINS; SANTOS, 2005). Esta parte trata da gestão de risco e análise de risco.

3.2.4 Seleção de proteção

Constrói um catálogo de contramedidas e serve de guia para a tomada de decisão na seleção da mesma.

3.2.5 Proteção para conexões externas

É um complemento da parte quatro da norma, com acréscimo de fatores relevantes para a conexão de sistemas em redes.

3.3 Norma IEC 61508

A norma internacional (IEC 61508:1998) enfoca, através de uma abordagem genérica, as atividades do Ciclo de Vida de Segurança para os Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES) que são utilizados para desempenhar funções de segurança. Neste sentido, esta norma vem sendo elaborada com o objetivo de desenvolver um policiamento técnico consistente para todos os sistemas elétricos/eletrônicos relacionados com a segurança (MARTINS; SANTOS, 2005).

Para Martins e Santos (2005), a norma IEC 61508 tem como objetivos principais “tratar sistematicamente todas atividades do ciclo de vida de um sistema instrumentado de segurança; habilitar que os desenvolvimentos tecnológicos dos produtos se realizem em ambiente sistemático de segurança funcional; ressaltar as melhorias dos Programmable Electronic Safety (PES) nos aspectos de desempenho e de viabilidade econômica e; uniformizar conceitos e servir de base para elaboração de normas setoriais”.

Essa norma é subdividida em sete partes, são elas: Requisitos Gerais; Requisitos para Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES); Requisitos de Software e; Definições, dois guias de aplicações sendo um da parte um e o outro das partes dois e três, e a última parte contém uma bibliografia de técnicas e medidas de segurança.

3.4 Método Quantitativo

Neste tipo de análise, procura-se quantificar, ou seja, calcular os valores para cada um dos itens coletados durante as fases da avaliação do risco. Nesse cenário eram observados os valores reais de cada ativo existente nos processos de negócios da organização, em termos do custo de substituição e também ligados à perda de produtividade (BMED, 2013).

Utiliza-se esse método quando a organização possui registros de eventos ocorridos, pois não se deve utilizar esse método sem a disponibilidade de dados, e que eles sejam confiáveis.

3.5 Método Qualitativo

Este tipo de técnica de análise de risco procura utilizar critérios para estimar os impactos aos negócios, provocados pela exploração das vulnerabilidades dos ativos por parte de ameaças. Procura-se com esta técnica utilizar critérios e classificações que podem abranger ao mesmo tempo valores tangíveis (o que você consegue ver e tocar) e intangíveis (algo não físico, como o abalo da imagem de uma organização) (BMED, 2013).

Ele é utilizado quando não há disponibilidade e confiança no registro dos dados, quando os seus custos não estão disponíveis, quando é impossível de mensurar com outro método, e quando não existe a necessidade da precisão do método quantitativo, dentre outros fatores.

3.6 Análise de risco

Após efetuado um diagnóstico dos riscos existentes, é necessário definir junto à alta administração da empresa ou organização, quais níveis de riscos são aceitáveis e não aceitáveis. De acordo com Martins e Santos, existem 4 tipos de opções entre riscos aceitáveis e não aceitáveis, são eles:

- Reduzir o nível de risco: Através da aplicação de controles de segurança;
- Aceitar o risco: Considerar que ele existe, mas não aplicar qualquer controle;
- Transferir o risco: repassar a responsabilidade de segurança a um terceiro, como, por exemplo, um data center;
- Negar o risco: esta é a opção menos recomendada.

A análise de riscos pode ser tanto quantitativa (baseada em estatísticas) quanto qualitativa (baseada no nível de qualidade ou valiosidade de dados da informação).

“O relatório de análise de risco deve conter identificação e classificação de ativos e processos de negócio, análise de ameaças e vulnerabilidades, e análise e parametrização de riscos e definição de tratamento dos riscos” (MARTINS; SANTOS, 2005).

4. SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

De acordo com Letsugu (2013) “a Tecnologia da Informação está presente em diversas formas dentro de uma instituição, como, por exemplo, computadores, sistemas, programas de computador, antivírus, firewalls, entre outros.” A informação está presente em todo o ambiente corporativo, desde uma geladeira computadorizada á servidores.

De acordo com Letsugu (2013) “os ativos de uma empresa são todos os bens que a empresa possui no momento, tais como: mercadorias, caixa, duplicatas a receber, máquinas, dados, informações e até seus funcionários.” As informações de uma empresa são de grande importância, por isso é importante pensar na prevenção antes mesmo que haja algum problema com a mesma. Deve-se proteger as informações de uma empresa, para proteger os ativos da empresa e cumprir com a ética da empresa.

4.1 Ativos empresariais

Para a Contabilidade Básica, são considerados ativos os bens e os direitos de uma entidade, expressos em moeda e à disposição da administração; já sob uma ótica econômica e financeira, os *ativos são recursos controlados pela empresa e capazes de gerar benefícios futuros* (entradas de caixa ou redução de saídas de caixa). Assim, pode ser considerado um ativo, todo e qualquer elemento com ou sem natureza física, que seja controlado pela empresa e que a ela proporcione a possibilidade de obtenção de fluxos de caixa (PEREZ; FAMÁ, 2006).

Os ativos de uma empresa são os bens de uma empresa que podem ser convertidos em valor monetário, como por exemplo dinheiro em caixa e estoque de mercadoria.

Os ativos podem ser subdivididos em duas categorias, são elas: Ativos circulantes; Ativos não circulantes.

4.1.1 Ativos circulantes

São aqueles que possuem um número maior de liquidez e que podem ser convertidos em valor monetário mais rapidamente, tal qual afirma Frazão (2018).

Para ser caracterizado como ativo circulante, é necessário seguir os seguintes critérios: a conversão em meio monetário deve ser realizada até 12 meses após a data do balanço ou ao longo do ciclo operacional da empresa; tenha como propósito ser negociado;



e que seja caixa ou equivalente de caixa. (FRAZÃO, 2018).

São exemplos de ativos circulantes:

- Disponibilidade de dinheiro em caixa ou em bancos;
- Estoques de matérias prima, produto final e produto em produção;
- Pagamentos a receber de clientes;
- Impostos a recuperar quando disponível;
- Aplicações financeiras a curto prazo.

4.1.2 Ativos não circulantes

São aqueles de permanência duradoura na empresa, possuem liquidez menores que os ativos circulantes e é responsável pelo funcionamento da organização. Os ativos não circulantes podem ser divididos em 3(três) categorias:

- Investimentos: “Os Investimentos como subgrupo do ativo não circulante se classificam como participações e aplicações societárias permanentes. Eles têm como objetivo gerar rendimento para a empresa[...]” (FRAZÃO, 2018).
- Intangível: “Os ativos intangíveis, chamados por alguns de ativos invisíveis, por outros de ativos intelectuais, dentre tantas outras denominações[...]” (PEREZ; FAMÁ, 2006). Estes ativos são destinados à manutenção das atividades da empresa ou exercícios com essa mesma finalidade.
- Imobilizados: “São os bens e direitos de natureza permanente responsáveis pela manutenção das atividades normais de uma empresa. Eles são bens corpóreos, ou seja, bens tangíveis” (FRAZÃO, 2018). São exemplos de imobilizados: veículos, terrenos, móveis e etc.

4.2 Infraestrutura de TI

A crescente facilidade de acesso à Internet vem permitindo que, cada vez mais, empresas e pessoas tenham acesso a esse veículo informacional, resultando em uma distribuição mais democrática dos conhecimentos da humanidade, oportunizando mercados e negócios a quem tiver competência [...] A TI vem se mostrando como ferramenta indispensável à sobrevivência organizacional, na medida em que imprime maior velocidade aos processos internos e permite aos gestores um conhecimento/relacionamento amplo com seu ambiente de influência [...] (JUNIOR; FREITAS; LUCIANO, 2005).

A infraestrutura de TI é composta por recursos físicos e virtuais que suportam armazenamento, processamento e análise de dados

A adoção de TI possibilita às pessoas fazer mais em menor espaço de tempo, de modo que a eficiência resulte em economia de tempo que, por sua vez, pode ser reinvestida na eficácia pessoal (TAPSCOTT, 1997, p. 86). No entanto, pode haver resistência interna à mudanças, já que diferentes habilidades tornam-se relevantes na qualificação (ou não) dos indivíduos para as tarefas, levando a um desequilíbrio na estrutura social existente [...] (JUNIOR; FREITAS; LUCIANO, 2005).

Uma infraestrutura de TI padrão pode consistir nos seguintes componentes de hardware: servidores, máquinas computadores, data centers, switches, roteadores e etc.

4.2.1 Servidor

Um servidor nada mais é do que um sistema de computação centralizado, em que através dele, são fornecidos serviços à uma rede de computadores. Desta maneira, todos os pacotes destinados à internet ou recebidos pela internet passam pelo servidor. O servidor tem o papel de armazenar arquivos digitais, sendo de extrema importância no cotidiano de uma empresa de tecnologia, geralmente os mais procurados são aqueles para hospedagens de sites, podendo ser desde criação e armazenamento de e-mails, armazenamento de arquivos, acesso a internet entre outros. Os computadores que acessam os serviços de um servidor são chamados de clientes, abastecendo outras redes para que assim, todos possuem a garantia de uso estipulada (GUALBERTO, 2017).

4.2.2 Data center

“Um data center é uma estrutura que tem papel importantíssimo para que diversos serviços atuais sejam bem utilizados e para garantir a continuidade de funcionamento de sistemas que processam dados diversos” (LOCAWEB, 2014).

De acordo com Locaweb (2014):

Basicamente, um data center se trata de um local destinado a concentrar os equipamentos que uma empresa ou organização utilizam para o processamento e armazenamento de dados, o que, dependendo do tamanho do empreendimento, pode acolher milhares de servidores, outros bancos de dados informatizados e componentes auxiliares, como storages e ativos de rede. Nesse sentido, a tradução para o português como Centro de Processamento de Dados (LOCAWEB, 2014).

Um data center é um conjunto de servidores que são utilizados para um grande volume de processamento e armazenamento de dados de uma organização, “Esses equipamentos são montados com o objetivo de processar de maneira adequada grande quantidade de informações, ininterrupta e confiavelmente, para que a organização que usufrui



desse sistema não tenha desvios ou queda na operacionalidade de seus serviços” (LO-CAWEB, 2014).

4.2.3 Switch

De acordo com Processtec (2018) “O switch funciona como um elemento que controla a comunicação entre os dispositivos conectados a rede. Os switches segmentam a rede, possibilitando que o fluxo de informações entre os dispositivos seja mais eficiente.” Um *switch* é um equipamento que segmentam a conexão de rede, e também fazem a comunicação local entre equipamentos que estão ligados nele, estendendo a comunicação de várias máquinas a uma determinada rede na qual o *switch* está conectado “Um switch é basicamente um equipamento para estender os pontos de rede, conectando todos os aparelhos em uma só rede, conseguindo também, transmitir vários pacotes de dados ao mesmo tempo” (PROCESSTEC, 2018).

4.2.4 Roteador

De acordo com Alecrim (2019):

Um roteador é um equipamento que tem a função básica de receber e direcionar pacotes de dados dentro de uma rede ou para outras redes. Esse tipo de dispositivo é mais avançado do que o switch. Além de executar as funções deste, os roteadores têm como diferencial a capacidade de determinar qual a melhor rota para um pacote de dados chegar ao seu destino.

Um roteador é um equipamento que possui funções semelhantes ao *switch*, mas com o diferencial que o roteador é capaz de determinar a melhor rota que esteja em menor uso ou congestionamento para que um pacote de dados possa chegar ao seu destino final, seja ele outro roteador, *switch* ou um computador.

Por conta dessa característica, roteadores são indicados para interligar redes. Isso pode ser feito nas mais diferentes configurações. Por exemplo: uma empresa que ocupa um prédio de três andares e tem uma rede em cada um deles pode usar um roteador para interligá-las e, ao mesmo tempo, conectá-las à internet (ALECRIM, 2019).

4.2.5 Firewall

De acordo com Machado “Os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados” (2012). Os firewalls podem ser tanto softwares quanto hardwares, que filtram todo o fluxo de dados entre um emissor e um receptor, “Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na

rede mas também a confidencialidade deles” (MACHADO, 2012).

Em um modo mais restritivo, um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede. O problema é que esta condição isola este computador ou esta rede, então pode-se criar uma regra para que, por exemplo, todo aplicativo aguarde autorização do usuário ou administrador para ter seu acesso liberado (ALECRIM, 2013).

Firewall como software: Para Machado:

Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final (MACHADO, 2012).

Um firewall já vem pré-instalado junto ao sistema operacional e ativo por padrão desde o acionamento do sistema pela primeira vez. Os firewalls utilizam um conjunto de regras e permissões para a filtragem de dados da rede até o computador.

Firewall como hardware: De acordo com Alecrim:

A vantagem de um firewall de hardware é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional (ALECRIM, 2013).

Os firewalls como hardware são desenvolvidos especificamente para fim de filtragem de dados na rede, capaz de lidar com um alto volume de dados, e possuem maior garantia de segurança na rede por não terem as mesmas falhas que são encontradas em firewalls de software.

4.2.6 Antivírus

Para Vinicius (2019) “Antivírus é um programa utilitário capaz de identificar códigos maliciosos em Sistemas eletrônicos, atuando na proteção contra softwares mal intencionados, que são chamados de vírus”. Os antivírus são softwares desenvolvidos para lidar com softwares maliciosos, chamados de vírus ou malwares, Para Vinicius (2019) “o Antivírus protege o sistema de um computador fazendo uma varredura em todos os dispositivos de armazenamento[...] lendo cada arquivo para saber se ele possui código malicioso ou mal intencionado”. O antivírus faz uma varredura para a detecção de malwares em todos os componentes de armazenamento do sistema, desde a varredura de dispositivo de armazenamento do computador ao dispositivo de armazenamento externo ao ser plugado no computador.

“A maior parte dos softwares contra vírus são programas que se atualizam automati-

camente através de um servidor para aprender a defender o sistema contra novos vírus” (VINICIUS, 2019). É fundamental manter o banco de dados do antivírus atualizado, para assim garantir maior segurança contra novos malwares.

5. CONSIDERAÇÕES FINAIS

De acordo com citações de autores que foram abordadas durante o trabalho, chegou-se a uma conclusão de medidas preventivas que devem ser tomadas acerca de Segurança da Informação, porém, devido a limitações de pesquisa científica e por tempo limitado, poderia ser feito estudo de caso envolvendo o tema proposto.

No primeiro capítulo foi abordado conceitos de segurança da informação, tais como Confidencialidade, Integridade, Disponibilidade e a Criptografia, tais tópicos são os de suma importância para um problema quando se trata de Segurança da Informação.

No segundo capítulo teve como ênfase normas e padrões metodológicos definidos para o gerenciamento da Segurança da Informação, notou-se uma grande importância dos tópicos, não somente para a segurança de ativos corporativos, mas também toda a cadeia de dados pessoais.

Foi demonstrado no terceiro capítulo conceitos e significados quanto ao meio corporativo, que são eles: Os ativos corporativos, a infraestrutura de TI e medidas preventivas de segurança na rede, foi abordado também o quão os ativos tanto corporativos ou pessoais são importantes.

Referências

ALECRIM, Emerson. **Diferenças entre roteador, switch, modem e hub** 2019 disponível em <<https://www.infowester.com/hubswitchrouter.php>> (Acessado em 24 de Outubro de 2019).

ALECRIM, Emerson. **O que é um firewall? Conceitos, tipos e arquiteturas** 2013 disponível em <<https://www.infowester.com/firewall.php>> (Acessado em 05 de Novembro de 2019).

BENETTI, Ticiano. **Segurança da informação – confidencialidade. Integridade e disponibilidade(-CID)** disponível em: <<https://www.professionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>> (Acessado em 15 de maio de 2019).

BMED, Fabio. **Análise quantitativa e qualitativa em segurança da informação** disponível em: <<https://fabiobmed.com.br/2013/06/06/analise-quantitativa-e-qualitativa-em-seguranca-da-informacao/>> (acessado em 11 de maio de 2019).

DANTAS, Marcus. **Segurança da informação: uma abordagem focada em gestão de riscos**, Olinda, Livro Rápido, 2011.

FRAZÃO, Márcia. **O que são ativos de uma empresa: tipos de ativos na contabilidade** 2018 disponível em <<https://investorcp.com/gestao-ativo-imobilizado/o-que-sao-ativos-de-uma-empresa/>> (Acessado em 22 de Outubro de 2019).

GALEALE, Napoleão Verarde; GONÇALES, Edison Luiz; GALEALE, Bernardo Perri. **Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras** disponí-

vel em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362017000300075&lang=pt> (Acessado em 12 de maio de 2019).

GUALBERTO, Marcelo. **O que é um servidor? Quais são suas características?** 2017 disponível em <<http://www.taticasolutions.com.br/?p=2542>> (Acessado em 23 de Outubro de 2019).

JUNIOR, Silvio Santos; FREITAS, Henrique; LUCIANO, Edimara Mezzomo. **Dificuldades para o uso da tecnologia da informação** 2005 disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1676-56482005000200005&lang=pt> (Acessado em 23 de Outubro de 2019).

LETSUGU, Matheus do Val. **Segurança da informação no ambiente corporativo** disponível em: <<https://www.professionaisti.com.br/2013/09/seguranca-da-informacao-no-ambiente-corporativo/>> (Acessado em 15 de maio de 2019).

LIBÓRIO, João; PEREIRA, Pedro. **Encriptação de Dados** disponível em: <<https://sites.google.com/site/encriptacao/criptologia/era-classica/cifra-de-transposicao>> (Acessado em 12 de Outubro de 2019).

LOCAWEB. **Você sabe o que é e como funciona um data center?** 2014 disponível em <<https://blog.locaweb.com.br/geral/voce-sabe-o-que-e-e-como-funciona-um-data-center/>> (Acessado em 23 de Outubro de 2019).

MACHADO, Jonathan. **O que é firewall?** 2012 disponível em <<https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm>> (Acessado em 05 de Novembro de 2019).

MARTINS, Alaíde; SANTOS, Celso. **Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação** 2005 disponível em <http://www.scielo.br/scielo.php?pid=S1807-17752005000200002&script=sci_abstract&lng=pt> (Acessado em 20 de Outubro de 2019).

PEREZ, Marcelo; FAMÁ, Rubens. **Ativos intangíveis e o desempenho empresarial** 2006 disponível em <http://www.scielo.br/scielo.php?pid=s1519-70772006000100002&script=sci_arttext> (Acessado em 22 de Outubro de 2019).

PROCESSTEC. **Dificuldade para transmitir informações nos PCs da sua rede?** 2018 disponível em <<https://www.processtec.com.br/artigos/o-que-e-switch>> (Acessado em 24 de Outubro de 2019).

SCHROEDER, Gustavo. **Restrições de Integridade** 2015 disponível em <<https://gustavoschroeder.wordpress.com/2015/12/03/restricoes-de-integridade/>> (Acessado em 12 de Outubro de 2019).

VINICIUS, Marcus. **O que é antivírus?** 2019 disponível em <<https://seletronic.com.br/o-que-e-antivirus/>> (Acessado em 05 de Novembro de 2019).

WEBER, Raul. **Criptografia Contemporânea**, UFRGS, 1995 disponível em: <<http://www.inf.ufsc.br/~mauro/curso/redes/cripto.doc>> (Acessado em 7 de Outubro de 2019).

CAPÍTULO 6

COMPUTAÇÃO FORENSE NO COMBATE AOS CRIMES CIBERNÉTICOS

FORENSIC COMPUTER IN THE FIGHT AGAINST CYBERNETIC CRIME

Victor de Souza Pereira¹

Catterina Dal Bianco²

Ernane Frasão Barbosa³

1 Ciência da Computação, Faculdade Pitágoras, São Luís - MA

2 Engenharia Elétrica, Universidade Federal do Maranhão (UFMA), São-Luís-MA

3 Ciência da Computação, Universidade Federal do Maranhão (UFMA), São Luís-MA

Resumo

A computação forense está associada a práticas ilegais, pois são aplicadas na internet, onde dados e privacidade são invadidos através de crimes cibernéticos, usando toda e qualquer ferramenta que possa estar ligada a rede de internet, de forma cotidiana. Neste sentido o objetivo geral do trabalho buscar apresentar de forma coesa importância da computação forense para soluções de crimes cibernéticos, bem como objetivos específicos discutir o desenvolvimento da ciência forense para atualidade; apresentar a computação forense na atuação de crimes cibernéticos e apresentar a importância da adesão e conhecimentos da ciência forense como ferramenta para combate ao crime digital. Tendo como metodologia revisão bibliográfica, com publicações de outros autores para auxiliar na produção deste trabalho. A computação forense é considerada ferramenta eficaz ao combate de todo e qualquer crime vinculado à rede de internet, pois mesmo que os dados sejam perdidos esta consegue recuperar e assim solucionar crimes cibernéticos.

Palavras-chave: Internet. Crimes Cibernéticos. Computação Forense. Crime Digital. Ciência Forense.

Abstract

Forensic computing is associated with illegal practices, as they are applied to the internet, where data and privacy are invaded through cybercrime, using any tool that can be connected to the internet network, on a daily basis. The general objective of this paper is to present the importance of computer forensics in the solution of cybercrime, and the specific objectives are to discuss the development of forensic science today, to present computer forensics in the performance of cybercrime and present the importance of adherence and knowledge of forensic science as a tool to combat digital crime. The methodology used is a bibliographic review, with publications by other authors to assist in the production of this work. Forensic computing is considered an effective tool to combat all and any crime linked to the Internet network, because even if the data is lost, it can recover and thus solve cybercrimes.

Keywords: Internet. Cybercrime. Computer forensics. Digital crime. Forensic science.

1. INTRODUÇÃO

Atividades e práticas ilegais, são aplicadas todos os dias na internet, dados e privacidade são invadidas, através de crimes cibernéticos. Utilizam de computadores, redes e dispositivos eletrônicos que estejam vinculados a internet. E esta prática de crimes tem crescido, e para que estes delitos sejam solucionados ou anemizados, surgir a computação forense, onde por meios da análise de dados seja do sistema ou computador, ou quaisquer dispositivos que esteja interligado e seja alvo de crimes cibernéticos, vem para solucionar este tipo de crime, assim juntando identificação, coleta, preservação, análise e relatório, funcionando de forma eficaz para a investigação. Tendo como, importância da computação forense no combate aos crimes cibernéticos, demonstrar que crimes podem ser solucionados e assim, afastando possíveis criminosos.

A ciência forense se torna fundamental para apreensão de crimes cibernéticos, onde esta ferramenta será de extrema importância para fraudes que são cometidas a todos os indivíduos que são expostos diariamente na internet. Esta possui características nas quais que juntas possibilitaram parecer favorável sobre determinada evidência. Fazendo-se essencial a importância da ciência forense para auxiliar de forma positiva nas evidências tecnologias relacionadas a pessoa envolvida. Torna-se relevante pesquisar mais sobre o quanto a ciência forense contribui de forma positiva na busca de dados que possam auxiliar na busca de evidências crimes cibernéticos. Podendo assim, ser uma grande ferramenta para atuação direta de peritos da área no qual ajudara em solução de casos, evitando assim novos crimes do mesmo criminoso.

O desenvolvimento da internet abre meio e soluções eficazes para resolução de problemas e situações, mas, no tempo que se torna favorável, abre portas para o aumento de acesso, isto no intuito de ações criminosas e que afetam e trazem danos a indivíduos ou patrimônios, essas estão expostas diretamente na internet, no qual objetivo é extrair dinheiro de forma fácil, considerado crime cibernético. Neste contexto qual a importância da computação forense como ferramenta perspicaz para barra e minimizar casos de crimes cibernéticos?

Tendo como objetivo geral a importância da computação forense para soluções de crimes cibernéticos. E ainda com objetivos específicos discutir o desenvolvimento da ciência forense para atualidade; apresentar a computação forense na atuação de crimes cibernéticos e apresentar a importância da adesão e conhecimentos da ciência forense como ferramenta para combate ao crime digital;

Este trabalho utilizou-se de revisão bibliográfica para dá início ao projeto, onde será abordado de forma sucinta e clara com ajuda das publicações em livros, artigos e trabalhos acadêmicos, considerando de suma importância o estudo sobre computação forense no combate aos crimes cibernéticos, além das suas contribuições para o desenvolvimento tecnológico. Foram selecionados em sites de busca, como Google acadêmico e alguns resumos que são disponibilizados em bancos de dados e texto que puderam se disponível na internet e/ou fonte original. Com o comprometimento em cita todo e qualquer texto que não fosse de autoria própria, assim respeitando as normas da ABNT e os dados buscados foram exclusivamente para finalidade científica acadêmica.

2. COMPUTAÇÃO FORENSE ATUALMENTE

A computação forense é dada como arte de descobrir e ou até mesmo recuperar informações de determinado crime, assim tornando-o admissíveis em tribunal (YASINCAC; MANZANO, 2001). E de acordo com Dan Farmer (2012), a perícia computacional forense, é a captura e também, análise de evidências nas quais será possível verificar mesmo estando distorcido ou tendencioso, reestruturar dados nos quais foram modificados no passado em um determinado sistema ou em dados importantes. Assim, tem se a computação forense como importância na computação para busca de fatos reais (SOUZA, 2016).

E assim a computação forense irá investigar e solucionar crimes, através de informações digitais dos dispositivos, tais como notebooks, tablets e afins. E com o crescente desenvolvimento das tecnologias, os crimes através da internet se tornam cada vez mais comuns, sabendo que esta é uma área onde contém bastante desenvolvimento o que tornam essências nas investigações.

Mas, sabe-se que a computação não está somente relacionada aos crimes digitais, porém é decisivo para provas e evidências de outros crimes que fazem parte do dia a dia. Neste sentido é dado como importante papel para identificar qualquer ato ilegal que esteja ligado a áreas de informática, identificando e fazendo uso de evidências que contribuíram para ser utilizadas como confirmação de um crime (DARYUS, 2020).

A computação forense é um conjunto de técnicas que coleta, recupera, analisa e preserva evidências digitais a fim de solucionar crimes. Computadores, notebooks, tablets, celulares e GPS são alguns dos dispositivos analisados à fim de obter informações para a resolução de casos. Qualquer crime que envolver, direta ou indiretamente, aparelhos que armazenam dados, como computadores ou celulares. Crimes cibernéticos - como fraudes bancárias e roubo de identidade - são alguns exemplos, mas a computação forense não trabalha apenas diretamente com crimes praticados no mundo virtual. A análise de informações digitais também tem papel fundamental na resolução de crimes praticados no mundo físico, como, por exemplo, recuperando mensagens ou outras informações já apagadas de um celular e que podem ser vitais para a resolução de um caso. Além disso, o profissional especializado nessa área também é capaz de descobrir se uma evidência foi adulterada ou não. No caso de filmagens de câmera de segurança, por exemplo, a data ou hora mostrados nas imagens poderiam ser alteradas em favor de algum dos envolvidos no processo, sendo importante a análise de um profissional para que a prova seja concreta e confiável (MARTINE, 2016).

Ainda, para os autores Eleutério e Machado (2011), a computação Forense é a ciência na qual pode preservar e documentar vestígios de qualquer dispositivo digital, bem como computadores, PDAs, câmeras digitais, telefones celulares e vários outros dispositivos de armazenamento de memória e ainda de acordo estes autores a computação forense é organizada como: coleta, exame, análise e relatório, como mostra na figura 01.



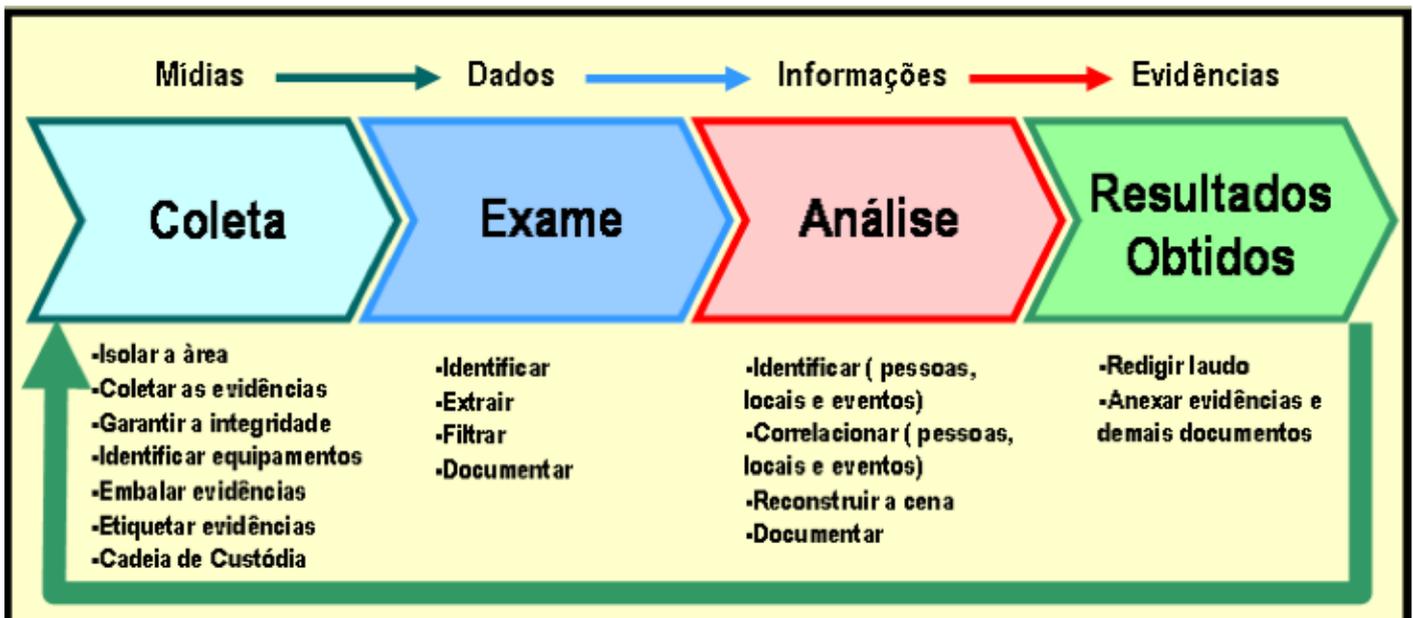


Figura 01: Etapas Do Processo De Computação Forense
 Fonte: adaptado, Kent et al., 2016

Na figura 01, demonstra os passos da computação forense, onde inicia pela coleta onde essa tem como objetivo de isolar, etiquetar, registrar e coletar dados físicos, propondo a integridade das provas. Em seguida o exame, onde estes farão um filtro das informações mais relevantes. Segue com a análise, utilizando o que resultou dos exames para assim analisar e ter respostas úteis. E por fim o relatório, onde irá possibilitar a relevância do caso, onde também terá um laudo pericial no qual deve ter a conclusão imparcial de forma clara e concisa, além de ser claro ao ponto de ser interpretado por uma pessoa comum de conhecimento intermediário (SOUZA, 2016).

E os profissionais no qual trabalham com a computação forense são os técnicos e analistas de redes, pois tem a base necessária para aprofundar-se nos assuntos referentes a esta computação. Estes são responsáveis pela coleta, reconstrução, análise e além de preservar as evidências. Estes profissionais são capazes de recuperar dados que já foram excluídos do ferramental digital, mesmo que já tenha sido formatado e ou utilizado por terceiros.

E pode ser também usado investigação de dados através de GPS do dispositivo móvel (celular), para assim localizar possíveis suspeitos ou vítimas no momento do crime. Percebe-se que a computação forense atua em diversos campos de investigação legal e proteção de sistemas, trabalhando como um CSI, considerada uma das áreas mais interessantes e procuradas das áreas computacionais (MARTINE, 2016).

Atualmente os avanços tecnológicos têm crescido de forma acelerada. O que possibilita a exposições a fraudes digitais e as tentativas de roubos e ou vantagem por meios ilícitos. Pois, sabe-se que a maior parte de golpes, estão relacionada a estas ferramentas tecnológicas, o que torna cada vez maior a possibilidade destes ataques. Entretanto, junto a esses avanços, áreas da computação forense tem-se desenvolvido e tornado seus profissionais capacitados e qualificados.

Assim, métodos e técnicas foram construídos para detectar esse tipo de golpes através dessas ferramentas relacionadas e conectadas a internet. O homem, está exposto e

ameaçado de forma constante a esse perigo, que é real. Mas, profissionais estão atuando e inovando, e se tornando profissionais ao se aperfeiçoar nesta área, comprovando que existe um equilíbrio entre os crimes e os profissionais dispostos e capacitados para intervir esses atos. Mas, infelizmente ainda existe a necessidade de profissionais atuando nesta área, mesmo com o avanço tecnológico. Considerasse a maior desvantagem já que os ilícitos eletrônicos têm se agravado constantemente, porém mesmo com essa desvantagem, ainda sim, pode contar com este suporte (DARYUS, 2020).

Conforme o Brooks (2014), a computação forense é combinada junto com elementos do direito e da computação, isto com o objetivo de coletar e analisar dados de sistemas computacionais, redes de computadores, comunicações sem fio e sistemas de armazenamento digitais de tal forma que esses dados sejam válidos na justiça.

A computação forense, está ligada fortemente com preservação e coleta dos dados, integridade e cadeia de custódia, análise e apresentação de resultados, e um dos mais importantes aspectos jurídicos.

Atualmente, a computação forense se torna muito importante nesta persecução penal, já que qualquer um pode deixar registros no mundo digital, é a partir deste seguimento que a computação forense age firmemente. E no segundo, os computadores são peças fundamentais para o cometimento dos crimes e sem esta ferramenta, os crimes não existiriam. Assim como

Wilson Leite da Silva Filho (2021) explica sobre esses ataques:

Ataques a sites, programas maliciosos para roubo de senhas, programas que seqüestram os dados do usuário (ransomware), entre outros, são exemplos desse tipo de crime. Muitos fatos criminosos de repercussão e correlacionados com a computação forense têm surgido na mídia. Abordaremos alguns, como o objetivo de, além de informar, sensibilizar o leitor em relação à dimensão que este tipo de delito tem tomado.

A computação forense, como já dito, vem como meios e métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital com validade probatória em juízo. Neste sentido, é necessário que deve ser tomado maior atenção na coleta destes dados e para a preservação deles, ou seja, isolar do local, evitar quaisquer acessos remotos. Utilizar funções de *hash* para que garanta a integridade dos dados entre outros. E a computação forense está em uma gama enorme de informações sobre os crimes que ocorre diretamente ou indiretamente pela internet nos tempos atuais, e esta ferramenta serve para auxiliar no ramo cibernético contra crimes e situações na rede.

3. ATUAÇÃO DA COMPUTAÇÃO FORENSE PARA CRIMES CIBERNÉTICOS

A computação forense é considerada uma arte, na qual, descobre e recupera algumas informações relacionando a um crime, tornando-os admissíveis (YASINCAC, MANZANO,



2001). E ainda, de acordo Dan Farmer (2012), trata de captura e análise de determinadas evidências, ressaltando que as mesmas o quanto antes, para que estejam livres de estarem distorcidas ou até mesmo tendenciosos, de modo que, pode ser possíveis reconstruir dados ou uns ocorridos no sistema no passado.

E neste contexto a computação forense, que irá preservar documentos como evidências, isto é, de um dispositivo digital ou que estejam relacionados à internet e esses processos se dão por 4 etapas: Coleta, Exame, Análise e Relatório.

E para que sua atuação seja eficaz nesse processo, a outros seguimentos como algumas ferramentas e técnicas utilizadas na etapa de coleta. Os dados disponíveis no dispositivo e até mesmo, os voláteis, nos quais são fontes de evidências digitais, é fundamental que estes estejam coletados e preservados corretamente que não possibilite sua alteração. E essa preservação e coleta facilitaram a busca de elementos de forma concreta e sólida, o que torna uma base para dar continuidade aos demais processos da perícia para os crimes cibernéticos (ELEUTÉRIO; MACHADO, 2001).

E ainda, para auxiliar usam-se as técnicas de imagem e espelhamento, onde os exames da computação forenses devem ser efetuados por réplicas idênticas dos originais, isso se dar, através de materiais originais, capturados e submetidos aos exames forenses. Desta maneira, uma cópia fiel e idêntica dos dados, mantendo a integridade do material apreendido (ELEUTÉRIO; MACHADO, 2011).

E estas técnicas são de duplicação e ou cópia, feita na fase da coleta consequentemente a preservação correta do material que foi apreendido.

E para ajudar tem se ainda, ferramentas que são utilizadas no bloqueio de escrita e na duplicação da computação forense, nos quais auxiliaram na preservação dos dados no processo da realização da imagem ou do espelhamento. Destacando-se os duplicadores e bloqueadores de escrita. E para este tipo de serviço é usado o *EspionForensics* e o *forensic Bridge Tableau*, o que são para este processo de bloqueio de escrita em discos, e o *Software ICS writeProtectCard Reader* é para bloqueio de escrita em cartões de memória. E para quem utiliza os duplicadores forense: rapidez na duplicação de dados; suporte de interfaces de discos; sem necessidade de computador (ELEUTÉRIO; MACHADO, 2011).

Mas, este processo não é obrigatório na etapa de coleta de dados. Porém, ao utilizar desta ferramenta facilitara o processo de duplicação de discos, pois garante assim a integridade.

Assim como Eleutério e Machado (2011) afirmam:

O programa Norton Ghost da empresa Symantec é uma opção ao uso de duplicadores forenses e bloqueadores. O software ForensicToolKit (FTK) e o software encase são soluções proprietárias compatíveis com o Windows. Ambas possuem diversas funcionalidades que possibilitam a realização de diversas técnicas para perícia forense computacional. Já como opções para Linux, o autor destaca a utilidade de alguns softwares para a etapa de preservação e coleta: DC3DD e Guymager, e destacam também os sistemas Linux CAINE e FDTK-Ubuntu para mesma finalidade.

E segundo Lillard et al. (2010), alguns ferramentais e ou dispositivos para coleta de dados, pode ser dividida em dois grandes grupos, isto de acordo com a volatilidade dos dados: Grupo Post-mortem, este com coleta sobre fontes não voláteis e seus principais dispositivos são: CDs, DVDs, cartões de memória, mídias de armazenamento, discos rígidos (HD) e tem o grupo em vida este são em fontes voláteis. E mesmo que a coleta post-mortem seja as mais usadas para exames periciais, salva alguns casos é fundamental a coleta live "A coleta do tipo live, quando realizada em redes de computadores, geralmente ocorre à captura de dados que trafegam pela entrada ou pela saída de tráfego de um computador ou de um ponto da rede".

Essa é a principal função dos softwares de Network Forensic Analysis Tools (NFAT), ou seja, a captura e análise de tráfego de rede, neste caso, voltado para parte forense. Nessa categoria de software, o programa TCPDUMP é o sniffer de rede mais conhecido e utilizado hoje em dia. Esse programa possui uma interface amigável e uma biblioteca libpcap, a qual possui infraestrutura flexível para captura de pacotes em redes de computadores (GALVÃO, 2013).

Outro exemplo dessa categoria de software, o Wireshark é um famoso analisador de protocolo de rede e ainda possui a funcionalidade de captura de pacotes de redes. Ele coloca a placa de rede em modo promíscuo, possibilitando a um maior alcance da captura de pacotes, além das funcionalidades de exportar pacotes para uma posterior análise. O software Wireshark é Open Source e disponível para diversas plataformas (SOUSA, 2016).

E ainda depois que fechar o processo de coleta, tem o processo de extrair esses dados ou seja as informações mais importantes, para seja analisada. Pois, é nessa etapa que será extraído e assim ver o que poderá ser importante para investigação, podendo ser encontradas evidências inacessíveis, a que podem está protegida com senhas e ou criptografia.

E a recuperação destes dados é usado com o Data Carving, isso dos que já foram apagados, usando assinaturas conhecidas (por exemplo, cabeçalhos que contêm a identificação do tipo de arquivo) e ainda podem sem usados. Alguns softwares como Photorec e Ontrack Recovery podem realizar a recuperação de arquivos apagados de forma automática (ELEUTÉRIO; MACHADO, 2001). Além, que em alguns momentos necessita de programas e arquivos que precisam de de senhas para sejam extraídos e tem se: Engenharia reversa, a engenharia social, ataques de força bruta.

Onde a engenharia reserva é o processo de desmontar e analisar, analisando e construindo o modelo em um nível alto para que assim o programa alvo possa ser estruturado e entendido (PINHEIRO, 2013). O que facilitar o funcionamento do programa e sua autenticação, na parte protegida do software e assim, na informação desejada pela perícia. Já a engenharia social é de ataque, onde alguém usa a persuasão, com a finalidade de obter informações que são usadas no acesso não autorizado aos computadores e/ou informações (SOCIAL-ENGINEER, 2015).

E no seu ambiente é onde os arquivos são protegidos por senha e os usuários serão disponíveis da equipe que os investiga e o responsável pode ter acesso nos processos e senha, o que facilitara o trabalho pericial. Por outro lado, o de força bruta consiste em utilizar dicionários de senha, senha por senha, a fim de localizar a possível senha dentro

do dicionário utilizado.

Os avanços tecnológicos têm crescido e ao mesmo tempo, a população se torna mais exposta a grandes fraudes digitais, furtos, e até tentativas de chantagem para extorquir dinheiros por meios ilícitos. Pois, cada vez, se tornam propício para este tipo de golpes.

O desenvolvimento de áreas, bem como a computação forense e seus profissionais, tem tido olhares diferentes, devidos os grandes crimes em rede, pois através dos conhecimentos é possível sanar possíveis fraudes, além de construir novos meios para detectar esse tipo de coisa. E é nítido o perigo e ameaçados quanto este tipo de crimes. Mas por outro lado, há profissionais que continuam inovando e aperfeiçoando na área, por isso a grande importância de investir em conhecimento da ciência forense. Mas, deve ter aperfeiçoamento na área, mostrando o equilíbrio e possibilitando que ainda sim, não se estar a mercê, de tais crimes.

4. CONSIDERAÇÕES FINAIS

Diante do presente trabalho, é perceptível a importância da computação forense. E atualmente, esta ferramenta é bem mais usada e reconhecida, já que anteriormente não se falava tanto, somente pelos estudiosos da área. Em meio a tecnologias avançadas, aos mais diversos crimes, a computação forense tem cada dia mais visibilidade através da aplicabilidade e da sua procura dos mais diversos crimes na rede de internet.

Com o crescente avanço da tecnologia os crimes conectados à rede de internet têm crescido de forma avassaladora, isto com invasão de dados digitais, bem como furto de informações pessoais, prejudicando assim uma parte das pessoas. E a ciência forense, vem para combater e recuperar dados que foram invadidos, auxiliando na busca de segurança dos usuários que estão expostos.

Mas, mesmo que com o avanço das tecnologias e que exista os dispositivos mais diversos e modernos, ainda sim os criminosos da rede, conseguiria driblar a segurança e invadir sistemas praticando fraudes, ameaças, roubo de senhas e outras informações restritas, espionagem industrial, crimes contra a honra, entre outros ilícitos. Conclui-se assim, a importância do estudo da ciência forense para o combate desse tipo situações, e o incentivo a pesquisa e aprofundamento deste campo, para combate deste tipo de crimes.

Referências

BROOKS, CHARLES L. **CHFI Computer HackingForensicInvestigatorCertificationAllin-OneExam-Guide**; 2014

DARYUS. **Computação forense: o que é e como funciona?** Disponível em: <<https://blog.daryus.com.br/computacao-forense-o-que-e-e-como-funciona-2/>>. Acessado em 27 de mar. 2022

ELEUTÉRIO, P. M. S.; MACHADO, M. P. Desvendando a computação forense. São Paulo: Novatec, 2011.

FARMER, Dan; VENEMA, Wietse. **Perícia forense computacional, teoria e pratica aplicada**; Tradução

Edson Furmankiewicz, Carlos Schafranski, Docware Traduções Técnicas; Revisão Técnica Pedro Luís Próspero Sanchez. São Paulo: Person Prentice Hall, 2007.

GALVÃO, R. K. M. **Introdução à análise forense em redes de computadores**: São Paulo: Novatec, 2013.

LILLARD, T. et al. **Digital forensics for network, internet and cloud computing**: Burlington: Syngress, 2010.

MARTINI, Ramiro. **Computação forense: o que é e como funciona**. Disponível em: <<https://www.bague-te.com.br/colunas/ramiro-martini/16/05/2016/computacao-forense-o-que-e-e-como-funciona>>. Acessado em: 30 de mar. 2022

PINHEIRO, D. O. Um estudo experimental das ferramentas de engenharia reversa aplicadas às vulnerabilidades do software. 42 f. Monografia, UFCE, Quixadá, 2013

SILVA FILHO, Wilson Leite da. **Crimes cibernéticos e computação forense**. Disponível em: <<http://sb-seg2016.ic.uff.br/pt/files/MC2-SBSeg16.pdfv>>. Acessado em: 28 de mar. 2022

SOUSA, Adriano Gomes. **Etapas do processo de computação forense: uma revisão**. Acta de ciência e saúde, número 05, volume 02. 2016.

YASINCAC, A.; MANZANO, Y. **Policies to enhance computer and Network Forensics**. IEEE. 2001

CAPÍTULO 7

ANÁLISE DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

*IMPLEMENTATION ANALYSIS OF GENERAL LAW ON PERSONAL DATA
PROTECTION IN BUSINESS DATABASES*

Deric Martins Trindade Gonçalves¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD) se caracteriza pela privação dos dados pessoais com intuito de ajudar na privacidade e no manuseio dessas informações, trabalhando assim a concretização das informações pessoais seguramente. A LGPD assegura uma série de benefícios para dados pessoais de clientes visto que a mesma remete punições à quem descumpre. Portanto, o trabalho conta como as instituições lidam com a imensa quantidade de dados ali contidos nos bancos de dados e a projeção de melhorias e rapidez nos sistemas, visando a qualidade e a proteção dos dados na qual é essencial, mas não descartando a organização dos mesmos e também tem a finalidade de demonstrar como os bancos de dados institucionais se comportam mediante a Lei Geral de Proteção de Dados Pessoais (LGPD) para analisar, de modo geral, a importância da confidencialidade dos dados no meio das mesmas paralelamente a grandes empresas. Baseada por documentos, pesquisas, relatórios e artigos relacionados ao tema, que mostra dificuldades enfrentadas no processo de aplicação e consequentemente a adaptação.

Palavras chave: Segurança de dados, Privacidade, Gestão de banco de dados

Abstract

The General Law on Personal Data Protection (LGPD) is characterized by the deprivation of personal data in order to help in the privacy and handling of this information, thus working to secure personal information. The LGPD ensures a series of benefits for customer personal data as it sends punishments to those who fail to comply. Therefore, the work tells how the institutions deal with the immense amount of data contained therein in the databases and the projection of improvements and speed in the systems, aiming at the quality and protection of the data in which it is essential, but not discarding the organization also aims to demonstrate how institutional databases behave according to the General Law on Personal Data Protection (LGPD) to analyze, in general, the importance of data confidentiality in their midst in parallel with large companies. Based on documents, research, reports and articles related to the topic, which shows difficulties faced in the application process and consequently the adaptation.

Keywords: Data Security, Privacy, Database management



1. INTRODUÇÃO

O mundo atual é composto por diversas tecnologias que são aprimoradas ano após ano e com isso, considerando o avanço tecnológico, a Internet das Coisas, os serviços em nuvem e o próprio *machine learning*, contribuíram também para a produção de mais dados. Nesse sentido, as pessoas permanecem conectadas a internet, trocando informações, com algumas delas disponíveis e expostas.

De fato, a facilidade de acesso à internet auxilia muito a vida da população, visto que pela mesma, é possível realizar diversas ações, desde compras, pagamento de contas, cadastros sem mesmo ir até a local físico. Entretanto, com a facilidade vem o questionamento: “meus dados emitidos estão realmente seguros?” essa e outras dúvidas diariamente são promovidas.

Constantemente ocorrem vazamentos de dados de grandes empresas e quando são divulgados, as preocupações com os prejuízos e incertezas perante a segurança desses dados voltam à tona. Com base no Regulamento Geral sobre a Proteção de Dados (GDPR), regulamento europeu que visa a proteção dos dados pessoais, a Lei Geral de Proteção de Dados (LGPD) foi fundamentada e tem como seu principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade com o livre desenvolvimento da personalidade da pessoa natural.

Com a Lei Geral de Proteção de Dados, as empresas tendem a ser mais cuidadosas e conseqüentemente se cria uma nova forma de lidar com a segurança desses dados pessoais, visto que as mesmas devem garantir a proteção das informações. Mediante a isso, a Lei Geral de Proteção de Dados de modo direto e penal, busca minar essas fragilidades que foram descritas ao longo da pesquisa.

Revisando todas as precariedades de segurança de dados, este trabalho visa contribuir para melhor interpretação da Lei que, embora sancionada há alguns anos, ainda há uma dificuldade de compreensão visto que ainda entra em constante modificação, descreve também os tipos de informações, os bancos de dados, além de entender as dificuldades e caminhos para a implantação e as penalidades de infração.

O primeiro capítulo explora o que seria a LGPD, como ela funciona, como são tratados os dados e quais são os direitos dos titulares. O segundo capítulo disserta sobre as características dos principais bancos de dados utilizados, juntamente com os mais frequentes ataques que ocorrem nos bancos de dados empresariais, afim de exemplificar os danos e prejuízos causados. O terceiro capítulo visa mostrar como a LGPD é aplicada, seus caminhos de implementação na empresa, suas sanções e prevenções para essas penalidades.

O tipo de pesquisa realizado neste trabalho foi uma revisão literária, onde o objetivo desta pesquisa é sintetizar a análise a aplicação da LGPD no contexto empresarial, afim de exemplificar como a Lei auxilia na proteção, como forma de aprofundamento tanto na parte da LGPD como nas informações sobre banco de dados e seus demais ataques, além de exemplificar que a Lei demonstra garantir um melhor desempenho para as empresas e mais segurança para os titulares dos dados. Este trabalho tem como base livros, disser-

tações e artigos científicos procurados e selecionados. O período dos artigos pesquisados foram os trabalhos publicados nos últimos 7 anos. As palavras chaves utilizadas na busca serão Lei Geral de Proteção de Dados, banco de dados, privacidade, fragilidade e segurança.

2. A LEI GERAL DE PROTEÇÃO DE DADOS

Em geral, a LGPD foi idealizada com base no Regulamento Geral sobre a Proteção de Dados (GPDR), lei europeia que também consiste na proteção de dados pessoais, aplicada em toda união europeia. As instituições estão se adaptando-a, visto que mesmo sancionada em 2018, ela entrou em vigor apenas em 2020, sendo modificada durante esse período.

A LGPD engloba todos aqueles que realizarem um tratamento de dados, não importando o meio, o país de sua sede ou do país onde estejam localizados os dados, desde que os tratamentos sejam realizados em território nacional (BRASIL, 2018).

Na prática, a LGPD solicita das empresas a confirmação de que está sendo cumprida legalmente. Os responsáveis pelos dados pessoais devem obrigatoriamente fornecer este documento, denominado Relatório de Impacto de Proteção de Dados. No documento, deve constar demais informações mediantes ao ciclo de vida de manuseio dos dados pessoais e uma designação do fundamento que fornece tal tratamento.

Como o enfoque da Lei seria possuir e manusear os dados pessoais de uma pessoa física com segurança, o Art. 2 da Lei nº 13.709 tem como fundamentos:

- I - o respeito com a privacidade;
- II - a autodeterminação informativa;
- III - a liberdade para se expressar, para informar e comunicar;
- IV - a privação de dados sensíveis, de sua honra e de imagem;
- V - no que diz desenvolver economicamente e tecnológico e a inovação;
- VI - a livre iniciativa, concorrência e a proteção do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

As empresas promovem a asseguaração de dados no proceder de sua aquisição, diante disso entra uma outra questão por parte da LGPD cuja função é entender o que seria um titular e os tipos de dados regulados.

2.1 Titular

É qualquer pessoa natural que possua dados, portanto, uma pessoa identificável.



2.1.1 Dados x Informação

A promoção do questionamento de que os dados e informações ainda é eminente, afinal, tem o mesmo significado? ou são definições distintas? Em geral, eles são resumidos da seguinte forma:

- Dado: Todos os fatos que podem ser armazenados;

Exemplo: Tom de pele, altura, idade, sexo;

- Informação: A diferente perspectiva sobre os dados;

Exemplo: Quantidade de pessoas com aquele tom de pele, quantos tem a mesma altura, quantos do mesmo sexo.

Sintetizando, os dados são constituídos de fatos prontos, geralmente representado por dados físicos. O agrupamento desses dados, constitui-se as informações. A informação é a construção de todos esses dados de modo a fazer sentido, a possuir um valor, em uso da quantidade. Transformar dados em informação é um processo, ou um conjunto de tarefas logicamente relacionadas realizada para alcançar um resultado definido.

2.1.2 Dados pessoais

O dado pessoal identifica qualquer pessoa física com informações gerais como CPF, RG, endereço, número de telefone. Esses dados geralmente são obtidos pelas empresas para facilitação de identificação da pessoa, porém mesmo com essas características gerais, a encarregada tem total responsabilidade pela privacidade dos dados.

2.1.3 Dados sensíveis

Os dados pessoais sensíveis são de grande importância para a proteção de dados, visto que expõe informações íntimas de pessoas como seu gênero, cor racial religião e posição política, filiação a sindicato ou a organização de caráter religioso (PINHEIRO, 2018, p. 19).

2.1.4 Dados anônimos

Os dados anônimos são definidos como aquele dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (BRASIL, 2018).

A anonimização de dados oculta os dados sensíveis, faz justamente que os dados

sejam anônimos. Estes dados não são de identificar o titular dos mesmos, pois são encriptados antes da coleta para uso.

É essencial sempre que possível, uma organização, pública ou privada, realize a anonimização de dados pessoais, pois isso aperfeiçoa a segurança da informação na organização e gera, assim, mais confiança em seus serviços e para seus públicos (SERPRO).

2.2 Agentes de tratamento

O tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, descarte, dentre outras. Os agentes de tratamento encarregados do manuseio desses dados, conforme diz a Lei, são controladores, operadores e encarregados.

2.2.1 Controlador

De acordo com o art. 5º da Lei nº 13.709, inciso VI propõe a seguinte definição para o controlador:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Já para Pinheiro (2018, p. 20) “o controlador que recebe os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal”.

O art. 9º da Lei determina que o titular tem o direito de acesso às informações de contato do controlador, dentre elas a identificação do controlador, o endereço, e as informações de contato propriamente ditas.

2.2.2 Operador

De acordo com o art. 5º da Lei nº 13.709, inciso VII propõe a seguinte definição para o operador:

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Pelo operador, a LGPD propõe o princípio de transparência, que determina a comunicação clara e precisa e de fácil acesso em relação ao tratamento desses dados e os agentes. A Lei também estabelece, no inciso VI do artigo 9º, a necessidade de disponibilizar

informações dos agentes, afinal como operador deve fornecer suas informações ao titular como sua identificação e endereço.

2.2.3 Encarregado

De acordo com o art. 5º da Lei nº 13.709, inciso VIII propõe a seguinte definição para o encarregado:

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Pinheiro (2018, p. 75) diz que “a imputação da necessidade de um encarregado principal por parte do controlador em face das atividades e ações relativas ao tratamento de dados busca garantir que as informações fiquem centralizadas e que o controlador se certifique de que a aplicação das normas receberá efetiva validação”.

Dessa forma, a LGPD estabelece, em seu artigo 41, que o controlador deverá indicar um encarregado pelo tratamento de dados e divulgar publicamente a identidade e as informações de contato do encarregado, como a identificação e as informações de contato.

2.3 Direito dos titulares

Com esse trabalho de informações coletadas e geridas, basta saber quais são os direitos dos titulares desses dados. De acordo com o art. 18 da Lei, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento. O titular tem o direito de solicitar à empresa a quais os objetivos da coleta. Essa confirmação pode ser simplificada ou pode ser em formato de declaração completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a sua finalidade (GUEDES, 2020).

A **Figura 1** abaixo exemplifica de forma simplificada todos os incisos desse artigo:



Figura 1: Ilustração dos direitos dos titulares
Fonte: digitalks (2020).

Embora a o art. 18 assegure que as empresas forneçam detalhes sobre o que de fato acontece com os dados desses titulares, a mesma reitera que os dados anonimizados não tem o mesmo tratamento dos dados pessoais (PINHEIRO, 2018).

2.4 Os princípios gerais da lei

Os princípios da Lei, tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas (BRASIL, 2021).

As empresas devem informar ao titular dos dados como é feito e fornecido a privacidade de forma que transpareça confiança e confiabilidade.

Em geral, a Lei constitui-se de princípios para o tratamento de dados pessoais que devem ser respeitados pelas empresas, Nunes (2019) cita que existem 10 princípios, são eles:

- Finalidade: o tratamento de cada informação pessoal deve ser feito com fins específicos, ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais;
- Necessidade: as empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular;

- Livre acesso: qualquer pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito e a qualquer momento;
- Qualidade dos dados: garantir aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas de forma clara e consciente;
- Segurança : toda responsabilidade da segurança dos dados cabe as empresas portadoras dos mesmos, sendo assim, buscar a proteção com todos os meios possíveis;
- Prevenção: Adoção de medidas para prevenção de ocorrências de danos em virtude do tratamento de dados;
- Não discriminação: os dados pessoais em hipótese alguma podem ser usados para promover abusos ou discriminação contra os seus titulares;
- Responsabilização e prestação de contas: Demonstração pelo agente de tratamento, adoção de medidas preventivas e capazes de comprovar o cumprimento das normas de proteção dos dados.

3. BANCO DE DADOS, FRAGILIDADE E ATAQUES

3.1 Formação dos bancos de dados

Um banco de dados é tudo aquilo que se põe armazenando informações em um único lugar, sejam elas organizadas ou desorganizadas. Forma em tudo que possui uma base de dados que armazenam diversas informações, comumente em computadores e geralmente formada por linhas, colunas e tabelas para facilitação da leitura, manuseio e organização dos dados.

Existem diversos tipos de banco de dados e cada um com uma funcionalidade diferente, varia de como vão ser trabalhadas as funções. O banco de dados relacional é um exemplo, embora clássica, ainda seria um dos mais utilizados pela sua capacidade de processamento e confiabilidade por parte da Linguagem de Consulta Estruturada (SQL).

Os bancos de dados relacionais necessitam de um gerenciamento de dados, para isso existe o Sistema Gerenciamento de Banco de Dados (SGBD), cuja função é manusear a fim de facilitar por comandos, através da linguagem SQL, o gerenciamento e organização dos dados.

A modelagem de dados representa a descrição formal da estrutura de um SGBD. "A evolução tecnológica permitiu que diferentes alternativas para a organização da estrutura de SGBDs fossem testadas e aprimoradas" (CAYRES, 2015, p. 4). Alguns modelos de dados mais vistos em bancos empresariais, dentre eles, Cayres (2015) cita que existem diversos modelos de SGBD.

3.1.1 Modelo Hierárquico

O modelo hierárquico trabalha com discos que possibilitam a exploração de sua estrutura de endereçamento físico, ou seja, os dados são estruturados em hierarquias. Elas trabalham com registros, onde cada registro é uma coleção de atributos cada uma contendo uma informação. O banco de dados da hierarquia acima dos outros é o registro-pai, os outros abaixo são chamados de registros-filhos.

3.1.2 Modelo de redes

Revolucionando o modelo hierárquico, o modelo de rede permite que um registro-filho possa se ligar com mais de um registro-pai, fazendo assim com que as conexões sejam mais complexas. O modelo de redes se diferencia pelo uso de grafos, ao contrário do hierárquico que usa árvores.

3.1.3 Modelo Orientado a Objetos

Os bancos de dados orientado a objetos armazenam suas informações em forma de objetos, ou seja, são diferentes de banco de dados anteriores, pois só é manipulada por métodos definidos pela classe que o objeto se aloca. Ainda muita utilizado, o modelo orientado a objeto.

3.1.4 Modelo NoSQL

Sendo um dos principais modelos utilizado pelas empresas, o modelo NoSQL tem como principal desafio a organização do processamento e manipulação do Big Data (conjuntos de dados que crescem continuamente e precisam ser processados e armazenados). Em geral, o NoSQL promove inúmeras soluções inovadoras para armazenamento, essas inicialmente criadas para criar soluções para problemas gerados por aplicações que crescem horizontalmente, que fornecem mecanismos de inserção de novos dados.

3.2 Ataques cibernéticos

A linguagem SQL é a mais utilizada em banco de dados empresariais, com exceção dos bancos de dados não relacionais (noSQL), é a linguagem mais utilizada pelo banco de dados relacionais, pelos motivos da sua simplicidade e facilidade de uso. Contudo, atenção redobrada na hora da manutenção desses dados, pois qualquer falha é facilmente explorada por indivíduos maliciosos.



Os ataques aos bancos de dados são explorados por falhas de segurança que frequentemente acabam em vazamentos, que geram incertezas sobre a segurança de armazenamento de dados pessoais. O *Facebook*, por exemplo, expôs dados de 267 milhões de usuários, que continham IDs, números de telefone e nomes reais dos mesmos. Em 2018, um desses vazamentos atingiu 30 milhões de usuários, enquanto um do início de 2019 fez com que dados de 419 milhões de pessoas fossem expostos (LIMA; ALMEIDA; MAROSO, 2020).

Atualmente, embora existam inúmeros meios segurança, os riscos de exposição de dados são enormes. Como mostra a **Figura 2** abaixo, os ataques a empresas geram prejuízos, visto que há uma perda de mais de 6 trilhões de dólares por conta de vazamentos, fraudes, roubo de identidades dentre outras.



Figura 2: Demonstração de ataques e prejuízos empresariais.

Fonte: dfndr (2021).

Segundo Lima, Almeida e Maroso (2020, p. 122) os canais de riscos para as instituições são:

- Um ataque por invasão de um cibercriminoso: ou seja, o cracker utiliza-se de seus métodos de engenharia social e através deles entra no sistema da empresa.
- Fornecedores: o ataque acontece através de algum fornecedor ou terceirizado da empresa e, por mais que a empresa esteja protegida, não é possível ter o controle de como está a gestão de risco nos parceiros, fornecedores ou terceirizados.
- Redes sociais: quando o colaborador acessa a rede social de um computador ou celular e clica em conteúdos maliciosos, conectando-se involuntariamente a um vírus e infecta a rede passando o software malicioso para a empresa inteira.
- Funcionários: as pessoas são os principais alvos de estratégias de invasores, os quais se utilizam das mais variadas motivações, fazendo o indivíduo cair na sua engenharia social,

3.2.1 Ataques comuns

Embora a falha humana ainda seja uma das causas de vazamento de dados, existem vários meios que criminosos podem efetuar para obter informações ou atrapalhar empresas, partindo de práticas comuns, como ataques de sobrecarga, vírus e a própria engenharia social. Dentre todas as elas, os ataques mais comuns estão:

- *Phishing*: a prática mais conhecida pelas empresas, o *phishing*, seria uma armadilha que criminosos cibernéticos usam para obtenção de dados de forma ilícita de uma pessoa, seja por e-mails, sites falsos ou cadastros falsos.
- *SQL Injection*: o *SQL Injection* é outro tipo de ataque frequente entre as empresas, que se resume em um meio de alteração do código SQL de determinada aplicação, gerada por uma falha dos próprios desenvolvedores.
- *Ransomware*: tipo de vírus que mantém seus dados como refém, forçando ao detentor oferecer uma troca pelo resgate, geralmente se paga uma quantia estipulada pelo invasor.
- DDoS: traduzido por Ataque de Negação de Serviços, o DDoS prejudica as empresas invadindo servidores e interrompendo ou sobrecarregando conexões diretas, criando lentidão e frustração de clientes e empregados (SGORLON, 2021).

3.3 Revisão de segurança

Com o objetivo de evitar o ataque por meio de vírus, recomenda-se que as empresas utilizem filtros em seus bancos de dados, que basicamente seria uma camada que verifica as informações e uma autenticação para prosseguir (KOBBS, 2017).

Paralelo a isso, as empresas não costumam ter a prática de backup de seus dados, sendo assim um dos problemas mais graves em questão, pois uma possível invasão e exclusão de todo o banco de dados seria solucionada pelo backup.

Embora o backup a todo momento tenha um alto custo, toda prevenção mediante a perda dos dados é crucial. Uma análise de vulnerabilidade reduziria ou até mesmo eliminaria as brechas existentes, pois sua função principal é identificar quais caminhos estão expostos a ameaças que são geradas por diversos motivos (KOBBS, 2017).

Várias formas de prevenção são executadas diariamente, dentre elas o uso do firewall, que hoje em dia é um elemento indispensável para controlar acessos indesejados a rede. Além da atualização e configuração constante dos serviços conectados a internet, fora o monitoramento constante das redes.

Existem caminhos para minar a evitar ataques, dentre elas a migração para nuvem, pelo fato de provedores desse tipo de solução, manterem as práticas de segurança bem rigorosas e proporcionarem uma infraestrutura de serviço mais completa (SGORLON, 2021).



4. RETRATAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

De início, é preciso organização, saber quais dados se devem coletar e sua relevância para categorização, saber quem têm acesso, como estes dados estão sendo adquiridos, onde estão sendo armazenados, documentar, qual a razão, o tempo de uso e as quais as práticas de segurança.

Para Pinheiro, (2018, p. 34) “a complexidade da implementação desse tipo de regulamentação se dá pelo fato de que os negócios estão globalizados, e o fluxo de dados está internacionalizado ainda mais com os recursos digitais e a internet”. Logo, há necessidade de se aplicar uma abordagem de direito comparado e de direito internacional.

Já para Benedito (2021, p. 8) “o processo de adequação à LGPD está ligado à revisão dos processos do negócio. Partindo do princípio de que um processo de negócio compreende o conjunto de um ou mais procedimentos ou atividades relacionadas, as quais, coletivamente, realizam um objetivo de negócio no contexto de uma estrutura organizacional”.

Uma vez definidos os primeiros dados e as necessidades, os impactos da implantação da LGPD demonstra uma evolução direta, necessitando uma política de proteção e segurança de dados de forma clara, objetiva e com uma linguagem acessível para compressão do cliente, uma base de dados segura totalmente protegida e para distinguir os princípios básicos da Lei, a Autoridade Nacional de Proteção de Dados (ANPD) entra em ação como demonstrado na **Figura 3** abaixo.

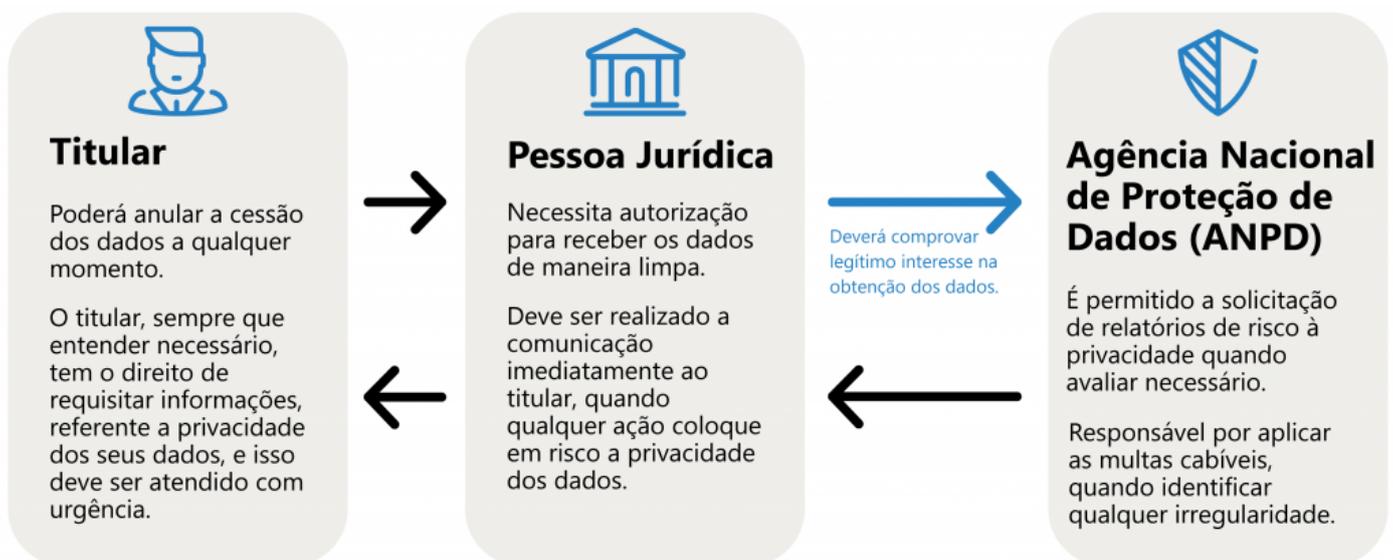


Figura 3: Exemplo de como funciona a ANPD
Fonte: Taugor (2019)

A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil. Ela garante a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos, sem o perigo de vazamentos (BRASIL, 2020). Não será exigido que pessoas físicas ou jurídicas que realizam tratamento de dados, transfiram para a ANPD seus bancos de dados. Cabe à mesma fiscalizar e aplicar sanções quando o tratamento de dados ocorrer em desconformidade com a legislação de proteção de dados, mediante processo administrativo, com contraditório e ampla defesa (BRASIL, 2020).

Fernandes (2019) diz que os efeitos e punições de vazamentos variam de acordo com a proporção do incidente e tipo de dados que foram vazados. Diversos são os efeitos negativos que podem atingir as empresas envolvidas em possíveis vazamentos e, por esse motivo, é imprescindível proteger sua empresa contra esse tipo de incidente.

Mediante a isso, a LGPD prevê sanções para quem não tiver cumprimento da Lei. De acordo com o art 52. da Lei Nº 13.709 são essas as penalidades:

- I - advertência, com possível indicação de prazo para correção;
- II – pequena multa por até 2% do faturamento da pessoa jurídica de direito privado, de um grupo ou conglomerado no Brasil no seu último exercício, excluindo tributos, no total de 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 - publicação da infração depois de 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 seis meses;
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Todas as sanções são aplicadas mediante a LGPD aplicada na empresa situada.

4.1 Retratação de vazamentos

Em suspeitas de vazamento dos dados pessoais, a LGPD determina que seja repassada para ANPD e que comunique a todos os titulares de forma geral. A comunicação a ANPD deve ser de imediata e deve ser retratada as informações:

- Quais tipos de dados foram afetados?;
- As informações sobre os titulares envolvidos;
- Todos os riscos que podem ter;
- E a indicação das medidas de segurança que foram utilizadas para a proteção dos dados.

4.2 Prevenções

Para que haja preparo contra possíveis vazamentos de dados, é essencial a adoção de determinados mecanismos como:

- É de grande importância fazer o mapeamento de dados pessoais, para que tenha consentimento de onde esses dados estão sendo armazenados, por onde entram e saem, se há dados sensíveis a ser tratados;
- O treinamento de funcionários da empresa para uma gestão organizada e responsável desses dados além da implementação de normas de confiabilidade;
- Formação do encarregado pelo tratamento de dados pessoais (DPO), que seria o responsável pelo canal de comunicação entre a empresa e os titulares dos dados juntamente a ANPD;
- Formação de um ambiente seguro para esses dados de modo geral, implantando sistemas de firewall para evitar possíveis invasões, além da utilização da criptografia de dados;
- Implementação de uma política de segurança capaz de organizar processos internos que diminua riscos de possíveis vazamentos (FERNANDES, 2019).

4.3 Mapeamento de dados

O mapeamento de dados é de grande auxílio para entender por onde e como os dados são transmitidos desde o princípio, de quando foi coletado pela empresa até o seu desuso e assim torna fácil a identificação de quem são esses dados, desde clientes a parceiros.

Com as informações adquiridas no processo de mapeamento, é possível entender o tamanho e quantidade de dados da empresa, gera também relatórios, de políticas, gestão, procedimentos e controle de proteção desses dados. Um mapeamento de dados deve ser elaborado em conjunto por diversos setores das empresas com ajuda técnica e jurídica para possíveis vulnerabilidades encontradas (BRANDÃO, 2020).

4.4 Avaliação de riscos

Com a realização da avaliação de riscos, a empresa pode garantir que sejam implementados níveis apropriados de medidas técnicas e organizacionais para proteção dos dados pessoais e evitar que riscos ocorram.

É fundamental que a avaliação de riscos seja realizada apenas depois que os processos foram mapeados através do mapeamento de dados, onde é possível identificar

as características do processo em relação aos dados pessoais envolvidos (quais dados estão sendo tratados, fluxo de vida dos dados, responsáveis, armazenamento, destino, descarte). Somente assim será possível analisar os principais riscos que envolvem os processos. Cada processo que envolva dados pessoais, deve ser avaliado de forma individualizada, mesmo que alguns riscos sejam inerentes a vários processos.

4.5 Sistemas de Informação (SI)

Em geral, a informação é um dos ativos de uma empresa de enorme e valor, levando em conta, o trabalho do SI visa a proteção dessas informações, além de preservar a privacidade por meio de hardware, software e redes que coletam dados e transformam em informações.

Para Cayres (2015, p. 23), um Sistema de Informação (SI) é um conjunto de elementos ou componentes inter-relacionados que coleta (entrada), manipula (processo), armazena e dissemina dados (saída) de informações, além de fornecer um mecanismo de realimentação (ação corretiva) para garantir a realização de um determinado objetivo.

4.6 Ciclo de vida dos dados

Quando há sua obtenção pelas empresas, os dados percorrem por determinados caminhos partindo da coleta, é onde o seu ciclo se inicia. Com esses dados coletados, ocorre o processamento e logo após a sua análise, partindo para o próximo passo que seria o compartilhamento e em seguida o armazenamento, para que ocorra a reutilização ou possivelmente o descarte/eliminação. A **Figura 4** demonstra detalhadamente as fases do ciclo, além de comparar como era antes da LGPD e depois da LGPD.

CICLO DE VIDA DOS DADOS		
FASE DO CICLO	ANTES DA LGPD	COM A LGPD
Coleta	Os dados pessoais são coletados indiscriminadamente.	Os dados pessoais coletados devem obedecer ao princípio da necessidade e da finalidade.
Processamento	Os dados podem ser processados sem um tratamento específico.	O processamento de dados só poderá ser realizado se o tratamento estiver enquadrado no Art. 7º da LGPD.
Análise	A análise de dados é feita para entender o mercado, conhecer o perfil das pessoas e definir estratégias para oferecer bens e serviços para o público-alvo.	A análise de dados deve levar em consideração a finalidade da coleta. Devem ser obedecidos os princípios de tratamento, com propósito legítimo, específico e explícito.
Compartilhamento	Os dados pessoais são compartilhados sem a necessidade do consentimento de seus titulares.	O compartilhamento de dados deve ser consentido pelos seus titulares.
Armazenamento	Os dados pessoais são armazenados e mantidos por tempo indeterminado.	Os dados pessoais devem ser armazenados e mantidos por prazos definidos, ou seja, até que finalidade seja alcançada ou deixem de ser necessários ou pertinentes ao alcance da finalidade.
Reutilização	Os dados pessoais são reutilizados sem a necessidade de consentimento de seus titulares.	Um novo consentimento deve ser solicitado sempre que houver mudança de finalidade.
Eliminação	Os dados pessoais são mantidos sem a obrigatoriedade de serem eliminados.	Os dados pessoais devem ser eliminados após o término de seu tratamento.

Figura 4: Ciclo de vida dos dados sem e com a LGPD
Fonte: (Positum, 2020)

Nota-se que após a aplicação da LGPD, todos os processos se tornaram mais seguros em todas as fases do ciclo, reforçando ainda mais a importância da Lei para que tenha mais segurança na hora do manuseio desses dados.

Determinados dados pessoais podem ser utilizados para outras finalidades além daquelas relacionadas ao serviço. Informações sobre os dispositivos como modelo do hardware, tipo de sistema operacional, navegador utilizado para o acesso, localização, dentre outros, podem ser utilizados para melhoria contínua dos serviços e aprimoramento da experiência do usuário. Desde que anonimizados, esses dados também podem ser utilizados para fins de pesquisa por órgãos de pesquisa, podem ser utilizados de maneira agregada para divulgação de informações por meio de meios de comunicação, e em publicações científicas e educacionais. Assim, qualquer tratamento posterior dos dados pessoais para outras finalidades deve ser comunicado ao titular do dado.

4.7 Transferência internacional de dados

De acordo com o art. 33º a transferência internacional de dados somente é permitida nos casos em que países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei ou quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei na forma de cláusulas contratuais específicas, padrões, normas contratuais e selos, certificados, códigos de conduta regularmente obtidos.

Diversos serviços podem envolver transferência de dados por vários países, a exemplo disso é a comunicação de órgãos públicos entre países, como serviços de inteligência e jurídico. Nesses casos, é de grande importância assegurar o titular que seus dados serão transferidos internacionalmente, informar a finalidade, quais são os países que estão relacionados, além do grau de proteção e privacidade.

5. CONSIDERAÇÕES FINAIS

Ao longo do trabalho, nota-se que a Lei Geral de Proteção de Dados precisava ser implementada no Brasil, visto que o país estava atrás comparado aos países europeus, que já possuíam o Regulamento Geral de Proteção de Dados. A Lei garante mais proteção aos titulares, pois as empresas tendem a se adequar mais e mais com as implementações, além das penalidades que muitas delas não tendem a querer.

A proposta deste trabalho foi um estudo e uma síntese de como a Lei Geral de Proteção de Dados fornece uma segurança para os bancos de dados empresariais, além de explorar como funcionam e quais são suas vulnerabilidades. O trabalho também tem enfoque em exemplificar os principais pontos de cada tópico, avaliando e fornecendo possíveis soluções para as vulnerabilidades existentes nos bancos de dados, visando a LGPD.

A análise dos tópicos tinha o objetivo de exploração e atualização de alguns pontos que ainda estavam em seu projeto inicial. Contudo, o trabalho foi concluído com poucas ressalvas menos importantes, visando apenas o assunto principal para estudo e entendimento do que seria e de como funcionam todos os itens citados ao longo do trabalho.

Referências

ANPD, **Perguntas Frequentes – ANPD**. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/novembro/201103-faq-anpd-2.pdf>. Acesso em: 22 mai. 2022.

BENEDITO, Matheus Braga. **LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE SOBRE OS DIREITOS DOS TITULARES E OS DEVERES DAS ORGANIZAÇÕES PERANTE A LEI**. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Federal de Campina Grande, Paraíba, 2021. Disponível em: <http://dspace.sti.ufcg.edu.br:8080/xmlui/bitstream/handle/riufcg/19884/MATHEUS%20BRAGA%20BENEDITO%20-%20TCC%20CI%20c3%8aNCIA%20DA%20COMPUTA%20c3%87%20c3%83O%202021.pdf?sequence=1&isAllowed=y>. Acesso em: 20 mai. 2022.

BRANDAO, Graziela. **O que é o mapeamento de dados?** Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/>. Acesso em: 22 mai. 2022.

BRASIL, **Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf. Acesso em: 02 jun. 2022.

BRASIL, **Lei nº 13.709**, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Palácio do Planalto, 2018: Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 04 nov. 2021.

CARVALHO, Vinícius, **MySQL: Comece com o principal banco de dados open source do mercado**, São Paulo: Casa do Código, 2015, 169 p.



CAYRES, Paulo Henrique. **Modelagem de Dados**, Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2015, 186 p.

DFNDR. **Falhas de segurança digital**: Conheça as 7 falhas mais comuns em PMEs. Disponível em: < <https://www.psafe.com/blog/falhas-de-seguranca-digital/> > Acesso em: 4 nov. 2021.

DIGITALKS, **LGPD E MARKETING**: GUIA PRÁTICO PARA O PROFISSIONAL DE MARKETING DIGITAL. Disponível em: <https://digitalks.com.br/artigos/lgpd-e-marketing-guia-pratico-para-o-profissional-de-marketing-digital/> Acesso em: 19 mai. 2022.

FERNANDES, Ana Valéria. **EFEITOS DO VAZAMENTO DE DADOS SEGUNDO A LGPD**. Disponível em: <https://4s.adv.br/blog/efeitos-do-vazamento-de-dados-segundo-lgpd/>. Acesso em: 25 mai. 2022.

KOBS, Vanderlei Darlei. **Segurança de redes**: mitigação e análise de vulnerabilidades. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdade Antonio Meneghetti – AMF, Restinga Seca, Rio Grande do Sul, 2017. Disponível em: <http://repositorio.faculdadeam.edu.br/xmlui/bitstream/handle/123456789/37/TCC%20Vanderlei%20Darlei%20Kobs%20-%20SISTEMAS%20DE%20INFORMA%20-%202017.2.pdf?sequence=1&isAllowed=y>. Acesso em: 20 mai. 2022.

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD - Lei Geral de Proteção de Dados**: sua empresa está preparada? 1 ed. E-book, 235 p.

NUNES, Natália Martins. **10 Princípios da LGPD para o tratamento de dados pessoais**. Disponível em: <https://ndmadvogados.com.br/artigos/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais> Acesso em: 20 mai. 2022.

POHLMANN, Sérgio Antônio. **LGPD Ninja**: Entendendo e implementando a Lei Geral de Proteção de Dados na Empresa. 1 ed. Nova Friburgo: Fross, 2019, 403 p.

SERPRO, **O que são dados anonimizados, segundo a LGPD**. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd> Acesso em: 19 mai. 2022.

SGORLON, Armindo. **Os 5 tipos de ataques cibernéticos mais sofridos por empresas**. Disponível em <https://sga.com.br/tipos-de-ataques-ciberneticos/> . Acesso em: 19 mai. 2022.

XPOSITUM. **Ciclo de Vida dos Dados e LGPD** Disponível em: <https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>. Acesso em: 22 mai. 2022.

CAPÍTULO 8

INTELIGENCIA ARTIFICIAL: MACHINE LEARNING APLICADO ÀS REDES SOCIAIS

*ARTIFICIAL INTELLIGENCE: MACHINE LEARNING APPLIED TO SOCIAL
NETWORKS*

Wagner Elias Oliveira Rabelo¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

A Inteligência artificial tem como finalidade oferecer melhor tomadas de decisões junto ao aprendizado de máquina para contribuir com a tecnologia de modo, através de demonstrativos, algoritmos, recursos, apps, programas entre outros diagnósticos, que servem para tomada de decisões, e assim ajudar a alcançar os seus objetivos e melhorar o desempenho computacional. Sendo assim, o presente estudo teórico tem como objetivo compreender como a inteligência artificial e aprendizado de máquina são aplicadas as redes sociais, a partir de uma revisão bibliográfica de publicações mais recentes sobre o tema. Partindo da análise dos trabalhos e assuntos mais debatidos sobre IA, foram identificados que essa ferramenta se tornou essencial para aperfeiçoamentos de algoritmos, pois contribui para que esses estudos possam se manter ascensão no mercado. Como principal contribuição, este estudo apresenta um conceito novo associado às perspectivas mais recentes na área, com base na literatura clássica, capaz de entregar uma definição clara e que auxilia no desenvolvimento teórico-empírico do conhecimento em inteligência artificial e aprendizado de máquina. Conclui-se que o uso de algoritmos aplicados em inteligência tem um amplo saldo sobre o poder de processamento computacional comparados com anos anteriores.

Palavras-chave: Inteligência. Artificial. Aprendizado. Máquina. Profundo. Redes Sociais. Redes Neurais. Algoritmo.

Abstract

Artificial intelligence aims to offer better decision-making together with machine learning to contribute to technology in a way, through statements, algorithms, resources, apps, programs and other diagnoses, which serve for decision making, and thus help to achieve its goals and improve computational performance. Therefore, the present theoretical study aims to understand how artificial intelligence and machine learning are applied to social networks, based on a literature review of more recent publications on the subject. Based on the analysis of the most debated works and subjects on AI, it was identified that this tool has become essential for algorithm improvements, as it contributes to these studies being able to maintain their rise in the market. As a main contribution, this study presents a new concept associated with the most recent perspectives in the area, based on the classic literature, capable of delivering a clear definition and that helps in the theoretical-empirical development of knowledge in artificial intelligence and machine learning. It is concluded that the use of algorithms applied in intelligence has a large balance on the computational processing power compared to previous years.

Keywords: Intelligence. Artificial. Apprenticeship. Machine. Deep. Social media. Neural networks. Algorithm

1. INTRODUÇÃO

Hoje, a mídia social é onipresente. Com o advento da internet e dos smartphones, tornou-se uma maneira fácil de se manter conectado com amigos, familiares e colegas. A facilidade de conexão com pessoas e empresas através das mídias sociais a tornou uma das favoritas entre os usuários. Os usuários passam um tempo enorme em plataformas de mídia social como Twitter, Facebook e WhatsApp. As pessoas usam esses sites para se conectar com amigos e familiares, compartilhar atualizações sobre suas vidas e participar de discussões on-line com outras pessoas.

Não é surpresa, então, que as empresas tenham começado a incorporar a IA (Inteligência Artificial) e a mídia social juntas. Este artigo irá explorar a conexão entre IA, mídia social e engajamento on-line. À medida que continuamos a nos esforçar para compreender o mundo complexo ao nosso redor e desenvolver tecnologia para manter o ritmo, os algoritmos e a inteligência artificial (IA) estão desempenhando um papel cada vez mais proeminente. A transformação digital, com sua ênfase na personalização, só aumentou isto e deu origem à IA um foco de atenção.

A IA estar pronta para ter um impacto maciço na forma como administramos as mídias sociais e como interagimos com o mundo on-line.

Não é de se estranhar o tempo que usuário passa junto as suas redes sociais. O objetivo delas é exatamente esse, fazer com que fiquem cada vez mais tempo conectados nos mesmos. Facebook, WhatsApp, Instagram, YouTube, Twitter, utilizam de algoritmos de inteligência artificial para literalmente prender a pessoa na frente do celular, com isso coletando o máximo de informações pessoais possíveis com base nos seus gostos, fazendo com que permaneça mais tempo conectado. Esta pesquisa bibliográfica pretende demonstrar e alertar a população no geral sobre o uso compulsivo, discriminado das mídias.

É possível amenizar o tempo e controlar o uso contínuo das redes sociais? O objetivo desse artigo é fornecer informações confiáveis que possam auxiliar no uso moderado da principal ferramenta do mundo moderno, para o uso moderado o computador portátil que se carrega dentro do bolso, sendo assim cada vez mais conectado. A maioria dos usuários desconhecem a necessidade de investigar os impactos negativos que o uso exacerbado das tecnologias, cada vez mais desenfreado, pode causar à população. Bem como seu potencial de dependência na vida das pessoas, especialmente neste momento de pandemia em que a comunicação se dá por meios virtuais de tecnologias de inteligência artificial.

Diante disso, tem-se por objetivo geral compreender como passamos tanto tempo presos refém das redes sociais. Já como objetivos específicos, foram estabelecidos: Conceituar inteligência Artificial; Como Machine Learning é aplicada às redes sociais: Apontar o futuro das IA relacionada as mídias sociais.

O presente trabalho trata-se de um estudo bibliográfico que se propõe discorrer sobre a Inteligência Artificiais aplicas às redes sociais de modo geral, através de uma revisão de literatura descritiva e qualitativa. Os dados para fundamentação do tema proposto serão coletados em publicações oficiais como periódicos, artigos científicos e livros mais



recentes coletados em bases de dados com o objetivo de identificar as bases constitutivas sobre o tema principal, e assim propor um conceito unificador.

2. CONCEITO DE INTELIGÊNCIA ARTIFICIAL

O estudo da inteligência teve início há mais de 2.000 anos. Com filósofos tentando compreender como funciona os processos de visão, aprendizado, lembranças e raciocínio. No entanto, foi somente por volta dos anos 50 que se originou a área de Inteligência Artificial (IA), quando cientistas começaram a utilizar computadores no desenvolvimento de programas com o objetivo de resolver problemas do cotidiano.

A Inteligência Artificial é uma das ciências mais recentes, teve início após a Segunda Guerra Mundial e, atualmente, abrange uma enorme variedade de subcampos, desde áreas de uso geral, como aprendizado e percepção, até tarefas específicas como jogos de xadrez, demonstração de teoremas matemáticos, criação de poesia e diagnóstico de doenças. A inteligência artificial sistematiza e automatiza tarefas intelectuais e, portanto, é potencialmente relevante para qualquer esfera da atividade intelectual humana. Nesse sentido, ela é um campo universal (RUSSELL; NORVIG, 2004).

Quando se fala de Inteligência Artificial, é difícil defini-la, mas ao longo do tempo ela seguiu quatro linhas de pensamento:

I. Sistemas que pesam como seres humanos:

“O novo e interessante esforço para fazer os computadores pensarem... máquinas com mentes, no sentido total e literal” (HAUGELAND, 1985).

II. Sistemas que atuam como seres humanos:

“A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas.” (KURZWEIL, 1990).

III. Sistemas que pensam racionalmente:

“O estudo das faculdades mentais pelo seu uso de modelos computacionais” (CHARNIAK; MCDERMOTT, 1985).

IV. Sistemas que atuam racionalmente:

“A Inteligência Computacional é o estudo do projeto de agentes inteligentes” (POOLE et al., 1998).

No geral, as linhas de pensamento I e III referem-se ao processo de pensamento e raciocínio, enquanto as II e IV ao comportamento. Além disso, as linhas de pensamento I e II medem o sucesso em termos de fidelidade ao desempenho humano, enquanto na III e IV medem o sucesso comparando-o a um conceito ideal que de inteligência, que se

chamará de racionalidade. Um sistema é racional se “faz tudo certo”, com os dados que tem (RUSSELL; NORVIG, 2004).

Historicamente, todas as quatro dimensões para o estudo da inteligência artificial têm sido seguida. Como se poderia esperar existe uma tensão entre abordagens centradas em torno de seres humanos e abordagens centradas em torno da racionalidade. Uma abordagem centrada nos seres humanos deve ser de ciência empírica, envolvendo hipóteses e confirmação experimental. Uma abordagem racionalista envolve uma combinação de matemática e engenharia (Ide, 2004).

Para Stairs e Reynolds (2006), o processamento de linguagem natural permite ao computador reconhecer comandos de voz em uma linguagem natural. 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). Este processamento de linguagem natural pode ser usado para recuperar informações sem digitar comandos ou procurar palavras-chave. Pode-se falar em um microfone conectado ao computador e o computador converte a fala em arquivos de textos ou comandos. Os sistemas simples conseguem associar uma palavra digitada a uma palavra falada pelo microfone, sistemas mais avançados não precisam gravar as palavras (STAIRS; REYNOLDS, 2006).

A IA ainda é tabu dependendo do assunto abordado, ainda não se sabe se o homem vai ser capaz de criar a real inteligência artificial, ou ao menos desvendar os princípios do cérebro humano que é a base sua criação. Hoje, o que se sabe é que seus conceitos desenvolvidos ao longo de anos têm trazido grandes benefícios para humanidade e que de um modo geral ela sempre vai inovar e evoluir gradativamente (STAIRS; REYNOLDS, 2006).

Nos últimos anos, houve uma revolução no trabalho em Inteligência Artificial, tanto no conteúdo quanto na metodologia. Agora, é mais comum usar as teorias existentes como bases, em vez de propor teorias inteiramente novas, fundamentar as afirmações em teoremas rigorosos ou na evidência experimental rígida, em vez de utilizar como base a intuição e destacar a relevância de aplicações reais em vez de exemplo de brinquedos (RUSSELL; NORVIG, 2004).

IA é uma ramificação da Computação, fazendo com q computadores pesem ou se comportem de maneira inteligente. A IA também está ligada com a psicologia, biologia, lógica matemática, linguística, engenharia, filosofia, entre outras áreas científicas, conforme mostra a Figura 1.



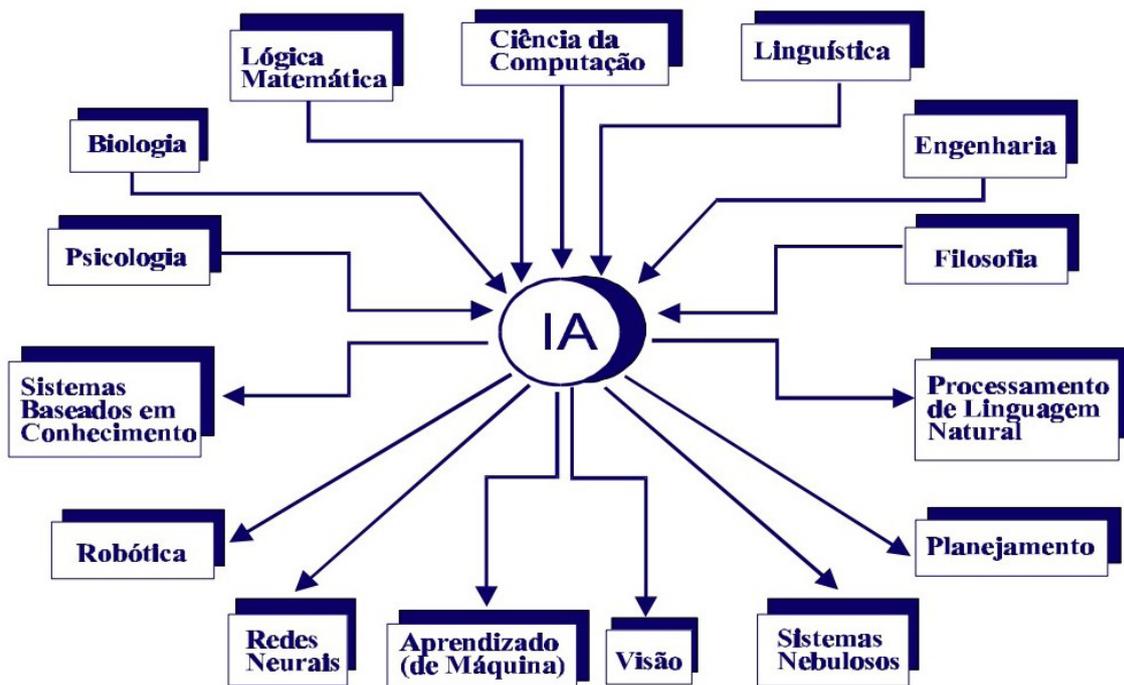


Figura 1 – Área relacionada com IA
 Fonte: Monard, Baranaukas (2000).

Desde então, a IA vem se destacando em diversas áreas de pesquisa: Sistemas Baseados em Conhecimento, Robótica, Redes Neurais, Aprendizado de Máquina, Visão, Lógica Nebulosa, Planejamento, Processamento e Interpretação de Linguagem Natural, Reconhecimento de Padrões. Tendo como objetivo desenvolver ao computador habilidades para desempenhar funções antes feita somente por humanos.

Pode-se dizer que o primeiro grande trabalho reconhecido como IA foi realizado por Warrem Macculloch e Walter Pitts (1943). De acordo com Russell e Norvig (2004), eles se basearam em três fontes: “o conhecimento da fisiologia básica e da função dos neurônios do cérebro, uma análise formal da lógica proposicional criada por Russell e Whitehead e a teoria da computação de Turing”. Esses pesquisadores sugeriram um modelo de neurônios artificiais, no qual, cada neurônio era caracterizado por “ligado” ou “desligado”, desse modo, o estado de um neurônio era analisado como, “equivalente em termos concretos a uma proposição que definia seu estímulo adequado” (RUSSELL; NORVIG, 2004).

Este período foi marcado por grandes entusiasmos e expectativas, mas poucos progressos, John McCarthy, Hyman Minsky, Claude Shannon e Nathaniel Rochester foram os principais idealizadores da época. Eles organizaram um seminário de dois meses em Dartmouth, em 1956, onde havia mais seis participantes: Trenchard More (Princeton), Arthur Samuel (IBM), Allen Newell e Herbet Simon (CMU), Ray Solomonoff e Oliver Selfridge do (MIT). Os destaques desse encontro foram: Allen Newell e Herbet Simon, com o programa de raciocínio Logic Theorist (LT). O seminário não trouxe muitas novidades no campo da IA, contudo, apresentou os personagens mais importantes da história. “Nos vinte anos seguintes, o campo seria dominado por essas pessoas e por seus alunos e colegas do MIT, da CMU, de Stanford e da IBM” (RUSSELL; NORVIG, 2004).

O primeiro sistema especialista comercial bem-sucedido, o R1, iniciou sua operação

na Digital Equipment Corporation (DEC). O programa contribuiu para configurar pedidos de novos sistemas de computador; em 1986, ele já fazia a empresa faturar cerca de 40 milhões de dólares por ano. Em 1988, o grupo de IA da DEC já possuía 40 sistemas especialistas entregues, com outros sendo produzidos (CHARNIAK; MCDERMOTT, 1985).

O cientista britânico, Alan Turing, o pai da computação moderna, afirmou que um computador pode ser chamado de inteligente se ele puder enganar um ser humano ao fazê-lo acreditar que ele (o computador) é um humano. Quando criou o teste de Turing (1950), afirmou que para que o computador fosse capaz de passar no teste ele deveria possuir as seguintes capacidades: processamento de linguagem natural, aprendizado de máquina, representação do conhecimento e raciocínio automatizado (RUSSELL; NORVIG, 2013). O Processamento Natural de Linguagem (PNL) é um conjunto de técnicas variadas da computação para o processamento de textos, sejam eles orais ou escritos, com a finalidade de obter um processamento de linguagem para uma variedade de tarefas e aplicativos (LIDDY, 2001), conforme Figura 2.

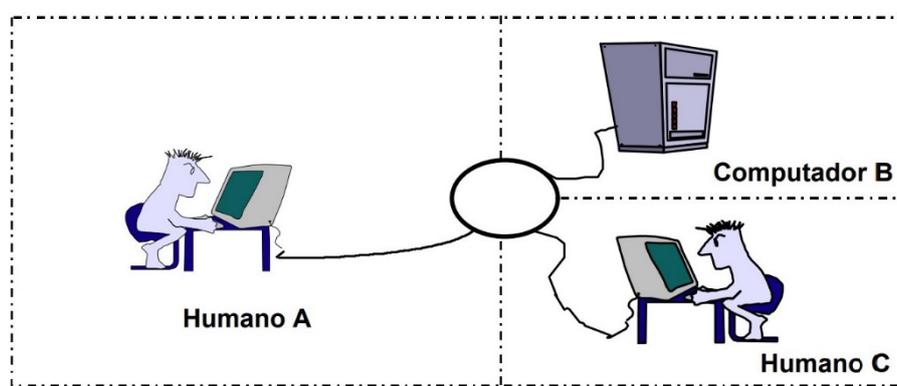


Figura 2 – Teste de Turing
Fonte: Monard, Baranaukas (2000).

O teste proposto por Alan Turing em 1950 fornece uma definição de inteligência de forma operacional. Turing definiu o comportamento inteligente como sendo a habilidade de obter desempenho humano em todas as tarefas cognitivas que fosse suficiente para enganar um inquiridor humano. De maneira mais simples, o teste proposto consiste em que um computador seja interrogado por um ser humano através de um terminal. O computador passa no teste se o inquiridor não puder dizer se do outro lado se encontra um computador ou um ser humano.

3. COMO MACHINE LEARNING É APLICADA ÀS REDES SOCIAIS

Aprendizado de Máquina (AM) – *Machine Learning* é uma área de IA cujo q tem como objetivo o desenvolvimento de técnicas computacionais sobre o aprendizado humano, bem como a construção de algoritmos capaz de adquirir conhecimento de forma automática. Um algoritmo de aprendizado é um programa de computador que toma decisões baseado em experiências preestabelecidas, acumuladas através da solução bem-sucedida dos problemas propostos anteriormente. Os diversos sistemas de AM possuem características comuns que possibilitam sua classificação quanto a linguagem formal, modo, paradigma e forma de aprendizado. Algumas dessas características, serão introduzidos neste capítulo.

O sucesso atual é “mera” implementação do modelo estatístico *deep learning* (aprendizado profundo, DL), inserido no subcampo da IA denominado de *machine learning* (aprendizado de máquina, ML). Em 1959, Arthur Lee Samuel, pioneiro norte-americano no campo de jogos de computador e IA, enquanto funcionário da IBM, cunhou o termo *machine learning*, inaugurando um subcampo da IA cuja finalidade é prover os computadores da capacidade de aprender sem serem programados. Evoluindo a partir do estudo do reconhecimento de padrões e da teoria de aprendizagem computacional na IA, o ML explora o estudo e a construção de algoritmos que, seguindo instruções, fazem previsões ou tomam decisões baseadas em dados – modelos elaborados a partir de entradas de amostras. O aprendizado de máquina é empregado em uma variedade de tarefas de computação, nas quais programar os algoritmos é difícil ou inviável. Trata-se de um processo de solução de um problema específico por meio da construção algorítmica de um modelo estatístico baseado em um conjunto de dados (BURKOV, 2019).

Machine Learning é uma subárea em que usuários, no uso de algoritmos realizam o treinamento de sistema informático, e que posteriormente realizará classificações. No treinamento é aplicada análise de dados. Os dados são representados por atributos, instâncias e classes. Os atributos são as características dos dados. Por sua vez, as instâncias são conhecidas como registros, e compostos por atributos, sendo que um dos atributos da instância visa caracterizar a instância, ou seja, a classe a que pertence a instância (WITTEN, 2002).

Atualmente é uma área interdisciplinar e abrange diversos subcampos principalmente AM e redes neurais. Tem como objetivo a criação e desenvolvimento de técnicas computacionais e a construção de softwares que sejam capazes de aprender de maneira independente. Redes Neurais é um desdobramento da área da inteligência artificial e podem ser definidas como uma máquina desenvolvida para replicar a maneira como o cérebro humano realiza determinada tarefa. Esta rede pode ser implementada através de componentes eletrônicos ou através de um algoritmo de programação (HAYKIN, 2001).

Os sites de redes sociais digitais estão se tornando mais populares a cada dia, como o Facebook, Twitter e LinkedIn. Entre todos esses sites, o Twitter é um dos mais pesquisados devido sua enorme interação entre os usuários da rede. Ultimamente, o aumento exponencial de spam tem se tornado um problema crescente no Twitter bem como outros sites de redes sociais digitais (BAKSHY, 2011).

A contar de 2012 o *deep learning* tornou-se onipresente, recebendo expressivos investimentos das gigantes de tecnologia. Diz respeito à previsão, com base em dados. “Atualmente, quando acessamos um dispositivo computacional, em qualquer de seus formatos, provavelmente estamos acessando concomitantemente um processo de *deep learning*” (KAUFMAN, 2019).

Por várias décadas, a abordagem dominante no campo da IA foi baseada em programas lógicos de computação, marginalizando a visão baseada no aprendizado de máquina. O atual crescimento exponencial dos dados, contudo, inviabiliza o uso da programação (regras definidas a priori). A Amazon não pode codificar os gostos do conjunto de seus clientes em um programa de computador, assim como o Facebook desconhece como escrever um programa para identificar as melhores atualizações no Feed de Notícias. A Netflix pode ter cem mil títulos de DVD em estoque, mas se os clientes não souberem como encontrar suas preferências de nada adianta. A grande quantidade de dados não é o

único fator restritivo, o conhecimento tácito é igualmente um limitador (KAUFMAN, 2019)

As redes neurais são funções matemáticas inspiradas nas biológicas, formadas por neurônios artificiais que se interligam entre si. A figura traduz uma arquitetura padrão, em que os círculos representam os neurônios artificiais e as setas os pesos – Figura 3.

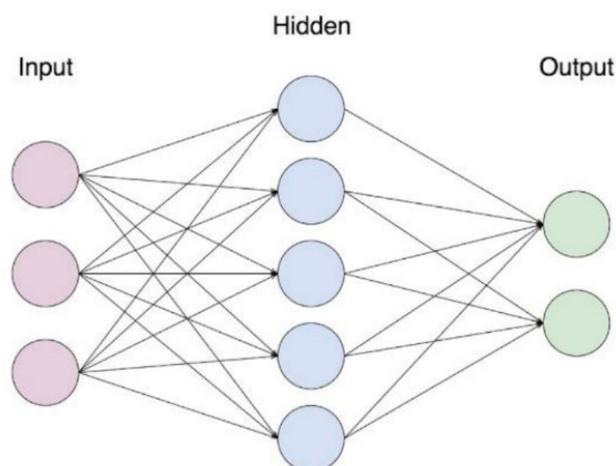


Figura 3 – Redes Neurais
Fonte: Wiedere (2016).

O objetivo de um algoritmo de aprendizado supervisionado é usar o conjunto de dados para produzir um modelo que tenha um vetor de atributos x como entrada e gerar informações que permitem deduzir o label desse vetor de atributos (BURKOV, 2019).

Na Figura 4, a imagem 2A é o output (imagem a ser reconhecida). As imagens subsequentes, representam o resultado das camadas intermediárias (*hidden layers*), cuja precisão depende do número de neurônios: a figura C tem 200 neurônios, por exemplo, e a figura 4D tem 2.000 neurônios.

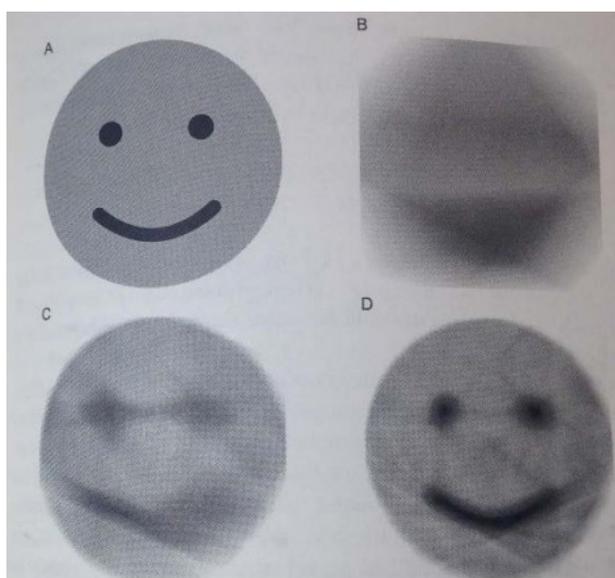


Figura 4 – Reconhecimento de imagem
Fonte: Gerish (2018)

A rede geralmente tem entre 10 e 30 camadas empilhadas de redes neurais. Em um reconhecimento de imagem, a primeira camada procura cantos e bordas; as camadas intermediárias interpretam as características básicas para procurar padrões formas

ou componentes em geral; e as outras camadas envolvem interpretações completas. Na identificação de fotos nas redes sociais, a máquina percebe padrões e “aprende” a identificar rostos nos posts. O reconhecimento de voz (Siri, Alexa, Google Now), que junto com a visão computacional está entre as aplicações mais bem-sucedidas, já permite a comunicação entre humanos e máquinas – Figura 5

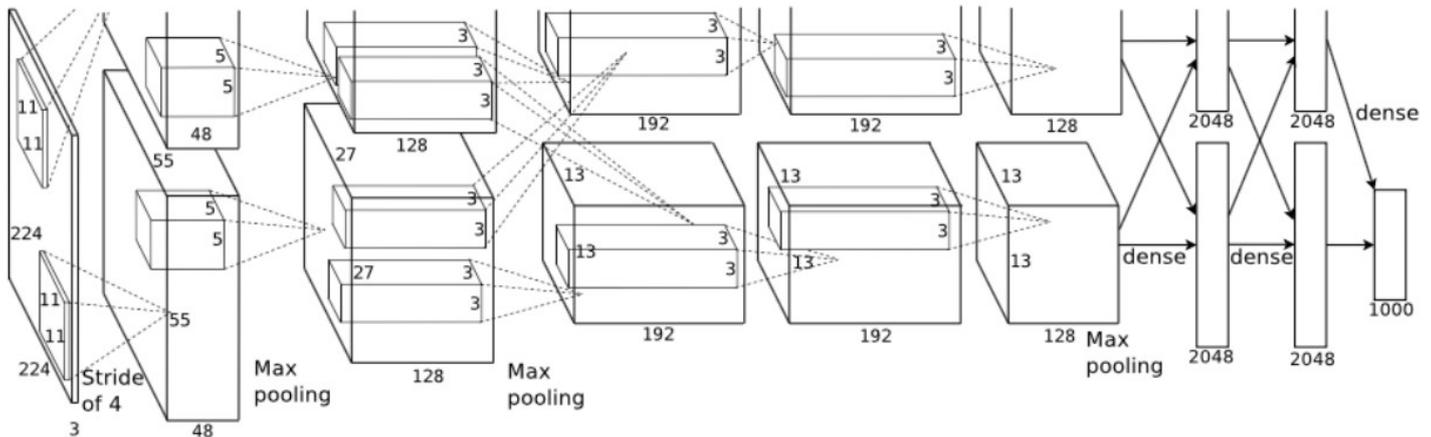


Figura 5 – Rede Neural Convolutacional
 Fonte: Krizhevsky, Sutskever e Hinton (2012).

4. FUTURO DA INTELIGÊNCIA ARTIFICIAL

O *dilema das redes* é um exemplo de denúncia à perda do controle das pessoas sobre o uso das redes sociais. O documentário apresenta ao público membros de gigantescas corporações como Facebook, Instagram, Twitter, Pinterest, entre outras mídias sociais que gostariam de manter em segredo, ou seja, à informação de que o cliente, não é o cliente real, mas sim, as empresas, os conglomerados midiáticos e os governos. Assim como aconteceu nas eleições para presidência do EUA em 2016. Estes grupos financiam anúncios direcionados nas redes sociais para que seja divulgados seus produtos e ideias. As informações são expostas por executivos das principais mídias sociais usadas por milhares de pessoas todos os dias, como ex-funcionários do Facebook, do Twitter e do Instagram, os quais ajudaram a criar algoritmos baseados em IA que são usadas hoje de forma automática e que mudaram definitivamente a maneira como as pessoas abordam os meios virtuais e fora deles.

Dentre as questões mais impactantes é trazida por Asa Raskin, inventor da rolagem automática do *feed* de notícias, revela que as empresas que anunciam na plataforma são os verdadeiros clientes, enquanto os usuários físicos são o produto, ou melhor, seus dados. Em seguida, a fala do ex-engenheiro ético da Google, Tristan Harris, reforça a afirmação de Raskin: “Se você não estiver pagando pelo produto, então você é o produto”. A ideia de transformação das pessoas em mercadoria é igualmente discutida por Bauman em muitos de seus textos, especialmente porque se vive num período no qual o movimento do mundo e as relações humanas giram em torno do consumo e da efemeridade (BAUMAN, 2008; 2011).

Entende-se que, quanto mais tempo o usuário passa conectado, mais informações são colhidas ao seu respeito, seus gostos, hábitos, interesses e características de bens de consumo. Estas informações são compiladas por IA que traçam um mapa a partir do

comportamento do usuário, por meio das curtidas e comentários, ao passo que analisam o tempo de exposição a leitura, a vídeos ou imagens. Após mapeados, são armazenados em servidores na nuvem e servem de base para oferecer produtos e serviços que mais se adequam ao gosto de cada pessoa.

Imaginem que estão entrando numa sala, uma sala de controle com um grupo de pessoas, centenas delas debruçadas sobre uma mesa de controle, e que essa sala irá modelar os pensamentos e sentimentos de um bilhão de pessoas.

Pode parecer ficção científica, mas isso realmente existe nos dias de hoje. Sei disso porque eu fazia parte de uma dessas salas de controle. O que não falamos é como um grupo de pessoas, que trabalham em um grupo de empresas de tecnologia, controlam, por meio de suas decisões, o que um bilhão de pessoas pensam hoje. Quando pegamos o telefone, e elas projetam o funcionamento disso ou o conteúdo das notificações, estão sendo programados pequenos blocos de tempo em nossa mente. Se vemos uma notificação, ela programa pensamentos que talvez não quiséssemos ter. Se abrimos essa notificação, ela programa que passemos um pouco mais de tempo envolvidos em uma situação na qual talvez não quiséssemos ser envolvidos. Quando falamos de tecnologia, tendemos a falar sobre ela como uma oportunidade visionária, que poderia seguir qualquer caminho. A tecnologia não está evoluindo ao acaso. Há um objetivo secreto guiando o caminho de toda a tecnologia que criamos. Esse objetivo é a disputa pela nossa atenção.

Todo novo site, eleições, política, jogos, até mesmo os aplicativos de meditação, tem que competir por uma coisa: nossa atenção. Isso ocorre com frequência. A melhor maneira de conseguir a atenção das pessoas é saber como funciona a mente delas. Um exemplo simples é o YouTube. Ele quer aumentar ao máximo o tempo que passamos nele. O que fazem então? Exibem o próximo vídeo automaticamente. Digamos que funciona muito bem. Estão conseguindo um pouco mais do tempo das pessoas. A Netflix observa isso e diz: "Isso reduz minha participação no mercado. Irei exibir automaticamente o próximo episódio". O Facebook diz então: "Isso reduz toda a minha participação no mercado, então tenho que exibir todos os vídeos antes mesmo que você clique pra assistir".

Portanto, a internet não está evoluindo ao acaso. A razão pela qual ela parece estar nos envolvendo dessa maneira é a disputa pela atenção. Sabemos aonde isso vai chegar. A tecnologia não é neutra, e torna-se esta disputa ao nível mais baixo do cérebro de quem pode ir mais baixo para ganhá-la. um exemplo do "Snapchat".

Caso não saibam, o Snapchat é o principal meio de comunicação dos adolescentes americanos. Utilizam mensagens de texto para se comunicar, é o Snapchat para os adolescentes. E cerca de 100 milhões deles o utilizam. Foi inventado um recurso chamado "Snapstreaks", que mostra a quantidade de dias seguidos em que duas pessoas se comunicaram. Em outras palavras, deram a duas pessoas algo que elas não queriam perder. Se você é adolescente, e tem 150 dias seguidos, não quer perder isso.

Pensem nos pequenos blocos de tempo programados na mente das crianças. Não é teoria: quando as crianças saem de férias, descobriu-se que elas dão suas senhas a até cinco amigos para manter o Snapstreaks delas ativo, mesmo quando não conseguem. Elas têm 30 desses, e precisam tirar fotos nem que seja de paredes e tetos só para passar o dia. Não é como se tivessem conversas reais.



Mas o que não dizem é que, na década de 70, quando falávamos ao telefone, não havia uma centena de engenheiros do outro lado que sabiam exatamente como funcionava nossa mente e nos organizavam no conceito da psicologia chamado de “duplo vínculo”. Se estiverem se sentindo um pouco indignados com isso, notem que esse sentimento simplesmente atinge vocês. A indignação também é uma ótima forma de chamar a atenção. Não escolhemos ficar indignados, é algo que acontece conosco.

O feed de notícias do Facebook, independentemente de nossa vontade, realmente se beneficia quando há indignação, porque ela não apenas programa em nós uma reação emocional no tempo e espaço. Também queremos compartilhar essa indignação com os outros. Queremos clicar em “compartilhar” e dizer: “Você acredita no que eles disseram? “A indignação funciona muito bem para chamar a atenção. Se o Facebook tivesse que escolher entre mostrar publicações tranquilas ou polêmicas, ele mostraria as polêmicas, não por ter sido uma escolha consciente de alguém, mas porque funcionaria melhor para chamar a atenção. A sala de controle do feed de notícias não é responsável por nós. Só é responsável por aumentar ao máximo a atenção. Também é responsável devido ao modelo de negócios da publicidade, para qualquer um que possa pagar mais, entrar na sala de controle e dizer: “Quero programar esses pensamentos na mente daquele grupo ali”. Pode-se mirar com precisão uma mentira diretamente às pessoas mais suscetíveis. Como isso é lucrativo, só tende a piorar.

5. CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo a partir de uma revisão de literatura compreender sobre algoritmos de aprendizado de máquina aplicado as mídias sociais, onde estão presente no cotidiano online bastante competitivo. Diante isso, mostrar um consenso sobre os principais conceitos em relação a esse tema.

Como consequência foi possível entender como as pessoas empresas necessitam controlar o tempo de uso nas redes para terem um melhor gerenciamento de seu tempo, pois acabam não tendo uma adequada gestão das redes sociais, e assim acabam passando muito tempo diante da tela do smartphone. Com um melhor gerenciamento do conteúdo que é visto, é possível ter melhores tomadas de decisões e auxílio para o desempenho pessoal.

Após a análise das principais teorias sobre a inteligência artificial, pode se concluir que ela possui ferramentas essenciais que auxiliam na tomada de decisão, no modo geral, contribuem para o aperfeiçoamento de algoritmos de aprendizagem de máquina, e ajudam desde a elaboração de simples aplicativos até redes sociais conhecidas mundialmente, sendo uma fonte valiosa de informação para as empresas. Como principal resultado, foi apresentado as principais ferramentas de inteligência artificial e como são fundamentais no uso de dispositivos com internet, através de dados que foram essenciais para o levantamento desses resultados.

Conclui-se também a importância que tem os usuários em conhecer melhor o aprendizado de máquina, para que não a veja somente como um simples algoritmo, mas sim como peça fundamental para o desenvolvimento de apps, e assim ter a possibilidade de

evitar ou antecipar possíveis problemas com o uso indevido e, pois, temos uma ótima ferramenta na palma da mão repleta de informações além disso, com o estudo foi possível validar os objetivos aqui estabelecidos.

Portanto, em relação às futuras investigações sobre inteligência artificial aplicada as redes sociais, recomenda-se analisar esse assunto em diferentes ramos de atuação organizacional, assim como em diferentes conceitos, explorar a sua relação com a demais áreas da tecnologia e os seus impactos com a sociedade no geral, pois a inteligência artificial é um manancial de informações que servem para a sobrevivência e desenvolvimento de novas tecnologias.

Por fim, tendo esclarecido aprendizado de máquina aplicada as redes sociais, considera-se este estudo uma base de dados que será de grande contribuição para construção de novos estudos exploratórios sobre o assunto.

Referências

- ABDEL-AAL, R.E.; AL-GARNI, Z. Forecasting Monthly Electric Energy Consumption in eastern Saudi Arabia using Univariate Time-Series Analysis. **Energy**, v. 22, n.11, p.1059-1069, 1997.
- ABRAHAM, B.; LEDOLTER, J. **Statistical Methods for Forecasting**. New York: John Wiley & Sons, 1983.
- BAKSHY, Eytan et al. **Everyone's an influencer: quantifying influence on twitter**. In: **Proceedings of the fourth ACM international conference on Web search and data mining**. 2011.
- BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Jorge Zahar, 2001
- BURKOV, Andriy. **The hundred-page machine learning book**. Publisher: Andriy Burkov, 2019.
- CHARNIAK, Eugene; MCDERMOTT, Drew. **Introduction to Artificial Intelligence** (Addison Wesley, Reading, MA, 1984), 1985.
- GERRISH, Ed; WATKINS, Shannon Lea. The relationship between urban forests and income: A meta-analysis. **Landscape and Urban Planning**, v. 170, p. 293-308, 2018.
- HAUGELAND, John. **Artificial Intelligence: The Very Idea**. Massachusetts. 1985.
- HAYKIN, S. **Redes Neurais: Princípios e Prática**, Bookman. (2001)
- KAUFMAN, Dora. **A inteligência artificial irá suplantará 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.
- KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E. Imagenet classification with deep convolutional neural networks. **Advances in neural information processing systems**, v. 25, 2012.
- KURZWEIL, Ray et al. **The age of intelligent machines**. 1990.
- KURZWEIL, Ray et al. **The age of intelligent machines**. Cambridge: MIT press, 1990.
- LIDDY, Elizabeth D. **Natural language processing**. 2001.
- MAKRIDAKIS, S.; WHEELWRIGHT, S.; HYNDMAN, R.J. **Forecasting Methods and Applications**. 3. ed. New York: John Wiley & Sons, 1998.
- MONARD, Maria Carolina; BARANAUSKAS, José Augusto. **Aplicações de inteligência artificial: uma vi-**

são geral. Anais, 2000.

O DILEMA DAS REDES. Direção: Jeff Orlowski. Produção de Larissa Rhodes: Netflix, 2020 Documentário disponível em: <<https://www.netflix.com>>.

PELLEGRINI, F.R.; FOGLIATTO, F. Estudo comparativo entre modelos de Winters e de Box-Jenkins para a previsão de demanda sazonal. **Revista Produto & Produção**, v. 4, número especial, p.72-85, 2000.

POOLE, D.; MACKWORTH, A. K.; GOEBEL, R. **Computational Intelligence: A Logical Approach.** Oxford: Oxford University, 1998.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência artificial.** 2004.

RUSSELL, Stuart. **Human compatible:** Artificial intelligence and the problem of control. Penguin, 2019.

RUSSELL, Stuart; BOHANNON, John. Artificial intelligence. Fears of an AI pioneer. **Science** (New York, NY), v. 349, n. 6245, p. 252-252, 2015.

WITTEN, Ian H.; FRANK, Eibe. Data mining: practical machine learning tools and techniques with Java implementations. **Acm Sigmod Record**, v. 31, n. 1, 2002.

CAPÍTULO 9

INTELIGÊNCIA ARTIFICIAL EM EVOLUÇÃO INDUSTRIAL

ARTIFICIAL INTELLIGENCE IN INDUSTRIAL EVOLUTION

Luis Eduardo Silva de Sousa¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

A Inteligência Artificial tem sido muito aplicada nos últimos anos e tem auxiliado as várias posições sociais, nesta esfera temos a aplicação desta tecnologia no avanço industrial, visando o desenvolvimento e rapidez de produção em larga escala com a eliminação de falhas. Com o progresso dos estudos das Redes Neurais torna-se possível o desenvolvimento de novas utilidades para a Inteligência Artificial, com o emprego do aprendizado de máquina para aperfeiçoar a indústria em vários departamentos. Com a compreensão das Redes Neurais e do aprendizado de máquina é observável a indispensabilidade da Inteligência Artificial na movimentação da indústria. Por meio de artigos de vários pesquisadores tanto na área da computação como também na história, pode-se observar os avanços dessa tecnologia ao decorrer do tempo e os diversos métodos com que ela se dá, tais como, os proveitos para o avanço do mercado global. A aplicação da Inteligência Artificial na indústria é indispensável, tanto para o consumidor final como para o mecanismo global.

Palavras-chave: Inteligência Artificial. Indústria. Aprendizado.

Abstract

Artificial Intelligence has been widely applied in recent years and has helped the various social positions, in this sphere we have the application of this technology in industrial advancement, aiming at the development and speed of large-scale production with the elimination of flaws. With the advancement of studies on Neural Networks, it becomes possible to develop new uses for Artificial Intelligence, with the use of machine learning to improve the industry in several departments. With the understanding of Neural Networks and machine learning, the indispensability of Artificial Intelligence in moving the industry is observable. Through articles by several researchers both in the field of computing and in history, it is possible to observe the advances of this technology over time and the different methods with which it occurs, as well as the benefits for the advancement of the global market. The application of Artificial Intelligence in the industry is indispensable, both for the final consumer and for the global mechanism.

Keywords: Artificial Intelligence. Industry. Apprenticeship.

1. INTRODUÇÃO

A inteligência artificial é um estudo avançado na área da ciência da computação, cujo objetivo é aprender o comportamento humano e suas habilidades dentro de uma determinada situação. Desta forma evitando possíveis erros cometidos pelo homem e assim aumentar a velocidade de produção em uma indústria.

A revolução Industrial foi um procedimento com muitas transformações tanto econômicas quanto sociais, que teve seu ponto de partida no século XVIII. Por tanto esse procedimento fez a transição das ferramentas simples para grandes máquinas e assim a substituição da energia humana para energia a vapor.

A inteligência artificial na indústria 4.0 tem como objetivo permitir o aprendizado de forma avançada em robôs, conseqüentemente iram desenvolver suas habilidades e desta forma a indústria consegue produzir com mais velocidade e com menos falhas em seus processos.

No decorrer desta jornada, teremos o prazer de desfrutar do conhecimento a respeito da Machine Learning e rede neural artificial que nos últimos anos vem ganhando bastante atenção de diversas empresas que estão dispostas a alavancar seus futuros investimentos e de ponta partida, atendendo cada vez melhor seus clientes, entregando aquilo que eles realmente estão procurando com uma maior velocidade.

Por qual razão pesquisar a respeito da inteligência artificial em evolução industrial? Quais são os tipos existentes até o momento de inteligência artificial? O que é *Machine Learning* e como ela contribui no desenvolvimento industrial? Quais são os impactos da I.A no mercado de trabalho?

Com o conhecimento do que é a I.A e Machine Learning e como elas podem somar na indústria, dará uma maior importância para essas novas ferramentas de trabalho e com o envolvimento da comunidade científica, poderá trazer uma maior visibilidade para à área e junto disso, novos investimentos para próximas pesquisas e assim obter novas descobertas e junto disso trazer novos benefícios para o mercado e a sociedade.

Para esta Revisão Literária será necessário o manuseio de alguns livros PDF's, artigos e revistas acadêmicas publicados na internet com relação a Ciência da Computação, Inteligência Artificial e Aprendizado de Máquina, Redes neurais que iram possibilita que este trabalho tome forma para ser procedente.

O período dos artigos pesquisados serão trabalhos publicados nos últimos 16 anos e as palavras chaves utilizadas, em sua maioria, serão: "Inteligência Artificial, Aprendizado de Máquina, Ciência da Computação, Redes neurais, Industria, Revolução Industrial".

2. APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL EM GERAL

Segundo Russell e Norvig (2004) As definições de inteligência artificial variam ao longo de duas dimensões principais.

- A que se baseiam em pensamentos e raciocínio onde o objetivo é desenvolver sistemas que pensam como seres humanos ou que pensam racionalmente.
- A que se baseia em comportamento onde o objetivo é desenvolver sistemas que atuam como seres humanos ou que atuam racionalmente.

De acordo com as dimensões mencionadas, aqui estão quatro definições de inteligência artificial (I.A), onde duas delas estão mais relacionadas a primeira dimensão e as demais na segunda.

- Bellman (1956) afirma que "Automatização de atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado..."
- Segundo Charniak e McDermott (1985) "O estudo das faculdades mentais pelo uso de modelos computacionais."
- Rich e Knight (1992) "O estudo sobre como fazer computadores realizarem coisas nas quais, no momento, as pessoas sejam melhores."
- Luger (2004) "A Inteligência Artificial pode ser definida como o ramo da Ciência da Computação que se ocupa da automação do comportamento inteligente."

De acordo com o estudo de pesquisadores a I.A, tem como objetivo seguir parâmetros de comportamentos e habilidades humanas, por isso é fundamental o estudo avançado em sistemas computacionais para entendermos como a mente humana é desenvolvida. Com o entendimento avançado da mente humana, teremos capacidade de tentar replicar isso em um algoritmo e ensiná-lo a efetuar trabalhos e junto disso, adquirir novas habilidades com maior velocidade e com menos falhar ou até mesmo não tendo mais o cansaço de efetuar tal trabalho.

No ano de 1969, a universidade de Stanford criou o programa DENDRAL que tinha como função, desenvolver soluções capazes de descobrir estruturas moleculares orgânicas a partir da espectrometria. Então foi formada uma equipe com três indivíduos com amplo conhecimento em filosofia, ciência da computação e genética. Esses foram Edward Feigenbaum, Buchanan, Joshua Lederberg e assim o DENDRAL foi muito importante para os seguintes desenvolvimentos de programas inteligentes, pois ele foi o primeiro sistema de conhecimento intensivo que teve sucesso.

2.1 Convergência entre I.A e evolução industrial

Com a automatização da produção, criação das primeiras máquinas, energia proveniente do carvão e também do ferro, evolução na agricultura com uso de novos componentes de adubação, vigentes tipos de plantações em objeção a forma da agricultura usada desde a idade média, que tinha como costume, interromper a plantação em uma determinada parte da terra durante um certo tempo para assim a terra recuperar suas características naturais.

Importante lembrar da grande formação da força de trabalho, essas são algumas características das transformações técnicas e econômicas que aconteceram no final do século XVIII na Inglaterra, então foi dado o nome de revolução industrial.

Segundo Duarte (2017) o mundo como conhecemos hoje foi formado por três revoluções industriais. A Primeira Revolução industrial teve início na Inglaterra no final do século XVIII, entre os anos de 1760 a 1830. O principal marco dessa revolução foi a introdução das máquinas a vapor, que deram início à produção mecânica, estendendo as suas atividades aos setores da indústria têxtil, agricultura e transportes, com destaque maior o carvão mineral, caracterizado como o principal combustível para o abastecimento dessas máquinas.

De acordo com Duarte (2017) a Segunda Revolução Industrial, por sua vez, teve início no ano de 1870. Nesse período, houve a adoção da eletricidade, a qual passou a ser parte fundamental da produção em massa. As máquinas que antes utilizavam energia a vapor foram substituídas por máquinas movidas a energia elétrica. Tal revolução deu origem às lâmpadas incandescentes para iluminação de indústrias e residências, possibilitando o trabalho no período noturno, o que, conseqüentemente, aumentou a jornada de trabalho e a produção.

Conforme Almeida (2005) já a Terceira Revolução Industrial começou na década de 1960, com marco histórico pelo crescente uso da tecnologia da informação em meio às atividades na produção industrial, com o desenvolvimento da computação. O surgimento de novos produtos marcou a época, a exemplo da criação da Internet, dos computadores, telefone celular, softwares, sistema de GPS, tecnologia automotiva e robótica, as quais antes não eram empregadas nas atividades produtivas.

Com o forte avanço da tecnologia presente na terceira revolução industrial, com todos esses desenvolvimentos surgiu assim a quarta revolução industrial mais conhecida como "Indústria 4.0", já se destacando muito no mundo atual, tendo como principal objetivo a inclusão da tecnologia de internet na própria indústria. O mundo está passando por uma grande evolução em termos de trabalho, comunicação e pesquisas e tratando-se de inovação, temos a presença forte da IoT (Internet das coisas), I.A (Inteligência artificial) e robótica.

A Quarta Revolução Industrial não é definida por um conjunto de tecnologias emergentes em si mesmas, mas a transição em direção a novos sistemas que foram construídos sobre a infraestrutura da revolução digital (anterior). A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o



sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos (SCHWAB, 2016, p 20).

A inteligência artificial já está presente na sociedade e vem trazendo com ela muitas transformações tanto no mercado de trabalho, economia e claro social. Sendo uma ferramenta capaz de automatizar atividades com uma maior agilidade, assim impulsionando a economia e dando uma maior produtividade com a exclusão de erros cognitivos ou o próprio cansaço proveniente de movimentos repetitivos. Importante lembrar da sua grande importância na preservação da vida humano, fazendo trabalhos que seriam perigosos para o homem.

A indústria 4.0 engloba uma grande quantidade de tecnologias avançadas com muitas habilidades em vários setores. Muito dessas habilidades só se tornaram possíveis por meio da RNA. Uma rede neural artificial é um sistema criado com base em estudos do funcionamento do cérebro humano. Essa rede neural tem o objetivo refletir nas máquinas a maneira como os seres humanos aprendem. Por meio delas as máquinas ganham a habilidade de entender e aprender padrões, que leva a se adaptar a mudanças e desta forma aprender a buscar respostas e soluções para um determinado problema.

Importante ressaltar que uma RNA tem duas formas de adaptação sendo elas aprendizagem supervisionada e aprendizagem não-supervisionada. Uma RNA com aprendizagem supervisionada é basicamente um modelo que aprende a partir de resultados pré-definidos aplicando valores passados da variável Target para assim aprender quais podem ser seus resultados de saída. Os mesmos valores de saída servem como supervisão e assim possíveis previsões que permite um ajuste das previsões com base em seus erros sendo assim se torna um aprendizado supervisionado, pois o modelo tem uma referência do que está certo e do que está errado. Logo uma RNA não supervisionada tem como tarefa, tentar entender as informações por conta própria. Este tipo de aprendizado é onde os grupos de dados são classificados para que tenha uma resposta pela qual a máquina pode determinar sua precisão.

2.2 A potencialidade da indústria 4.0

Percebe-se que no século XXI, entre várias transições. O mundo presencia o surgimento da digitalização, conhecida também como transformação digital, reconhecida pela presença de computadores, tablets e também smartphones, conexão com internet com amplo acesso e uma potência forte das mídias de comunicação. Nessa circunstância, o mercado tem se preparado para a nova geração de muitos consumidores digitais e portanto são criadas novas estratégias de marketing, a partir de análise de grandes quantidades de informações "big data" e também um foco em analisar redes sociais.

A Indústria 4.0 fundamenta-se na agregação da tecnologia de informação e comunicação que por sua vez permitem alcançar novos estágios de produtividade, flexibilidade, qualidade e gestão, concedendo o nascimento de novos planos e modelos de negócio para a indústria, com isso levando a ser considerada como a quarta revolução industrial ou

quarto paradigma de produção industrial.



Figura 1- Sistema Ciber Físico
Fonte: www.eaware.com.br

Um sistema CPS é um sistema formado por elementos computacionais com a função de coordenar entidades físicas. O sistema ciber físico tem o objetivo a interação entre os elementos computacionais e elementos físicos.

3. MACHINE LEARNING E INTELIGÊNCIA ARTIFICIAL

Machine Learning é a capacidade que um determinado sistema possui de aprender e fazer ações por meio de diversas tentativas ou até mesmo por meio da própria experiência. Segundo Coppin (2010), aprendizado está diretamente ligado com a inteligência, pois realmente se um sistema é capaz de aprender a exercer determinada tarefa mereça então ser chamado de inteligente.

Um processo de aprendizagem inclui a aquisição de novas formas de conhecimento: o desenvolvimento motor e a habilidade cognitiva (através de instruções ou prática), a organização do novo conhecimento (representações efetivas) e as descobertas de novos fatos e teorias através da observação e experimentação. Desde o início da era dos computadores, tem sido realizadas pesquisas para implantar algumas destas capacidades em computadores. Resolver este problema tem sido o maior desafio para os pesquisadores de inteligência artificial (IA). O estudo e a modelagem de processos de aprendizagem em computadores e suas múltiplas manifestações constituem o objetivo principal do estudo de aprendizado de máquinas. (SANTOS, 2005, p10).

O aprendizado de máquina, trabalha com diversos tipos de métodos, entre eles o método supervisionado, não supervisionado e aprendizado por esforço. O método por esforço o algoritmo aprende com erros mediante a diversas tentativas (tentativa e erro). Ou seja, *Machine Learning* é um meio que os sistemas e algoritmos verificam informações e automatizam o protótipo de análise através de dados, portanto os computadores encontram soluções para determinados problemas sem serem diretamente designados para isso.

Uma subárea da *Machine Learning* é conhecida como aprendizagem profunda ou Deep Learning, conhecida também de Redes Neurais Artificiais que fazem uso de algoritmos com o objetivo de igualar aos processos realizados pela mente humana.

A DL faz uso de camadas de neurônios artificiais para realizar análises dos dados com o propósito de assimilar a linguagem humana. Depois da matematização do neurônio biológico o neurônio artificial atua similar ao neurônio biológico, as informações são transmitidas por meio das camadas de entrada, processamento e saída.

Um processo que aplica técnicas de *Machine Learning* é o processamento de linguagem natural, utilizando padrões em um volume de divisões de dados puros para reconhecer a linguagem natural. Em outras palavras o uso desse processamento de linguagem natural é para análise de sentimentos de usuários. Em especial o mercado vem aplicando esse artifício para analisar e encontrar padrões em publicações em todas as redes sociais com a finalidade de saber o que os clientes pensam a respeito da marca ou produtos conseguindo assim ver o nível de procura e aceitação do produto no mercado.

3.1 Redes neurais artificiais

Redes Neurais Artificiais são modelos matemáticos manifestados computacionalmente e com base direta no cérebro humano, por tanto nas redes neurais biológicas ou redes neurais cerebrais e por meio desse modelo de simetria as redes neurais biológicas, as RNAs são capazes de aprender mediante a experiências do mesmo modo que um ser humano. Podemos assim começar a entender o funcionamento de um neurônio biológico apresentado na figura 2 para mais tarde ter um melhor entendimento do funcionamento do neurônio artificial.

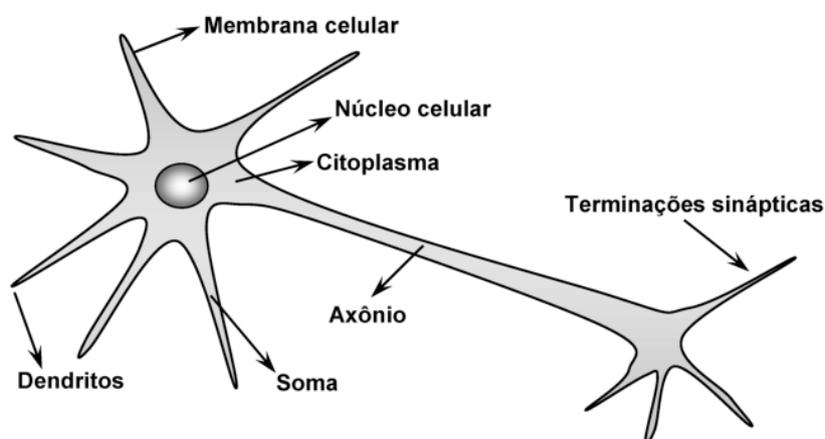


Figura 2- Neurônio biológico
Fonte: www.researchgate.net

McCulloch e Pitts em 1943, foram responsáveis pelo ponto inicial em pesquisas avançadas e no entendimento das redes neurais artificiais. O elemento essencial da RNA é um neurônio que usa uma função de transferência para determinar a saída de alguma possível entrada.

Para Falqueto (2018) o algoritmo de RNA é um sistema físico que pode adquirir, armazenar e utilizar conhecimentos experimentais, e pode alcançar um ótimo desempenho por causa do grande número de conexões entre os neurônios da rede.

As RNAs atuam da seguinte forma, todo dado ou informação passa por uma linha de conexão e em cada linha dessa apresenta um peso de processamento. Cada elemento de

processamento do neurônio usa as informações predeterminadas para gerar o processamento do dado no qual é distribuído para todos os elementos de processamento da RNA, dessa maneira o processamento da informação é compartilhado para toda a rede que se transforma em um processamento com uma maior rapidez de toda e qualquer informação.

Com o entendimento da correlação do neurônio biológico com o neurônio artificial, vamos por tanto compreender o funcionamento do neurônio artificial e aprender seu modelo matemático, como podemos ver na figura 3.

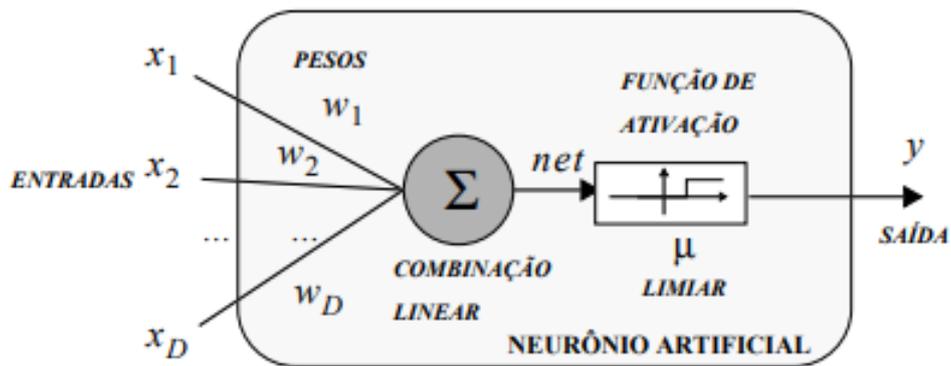


Figura 3- Modelo matemático de um neurônio de McCulloch e Pitts
 Fonte: l1nq.com/elwT0

1. Para todo sinal P temos as entradas X_1, X_2, \dots, X_p ;
2. Os pesos são dados por W_1, W_2, \dots, W_p e um limitador t ;
3. Os sinais entram como (0, 1) já os pesos assumem valores reais;

$$\text{Atividade} = \text{peso}_1 \times \text{entrada}_1 + \text{peso}_2 \times \text{entrada}_2 \dots \text{peso}_w \times \text{entrada}_w$$

Para a saída temos y e se dá da seguinte maneira:

1. Saída = 1, se Atividade \geq limitador ou
2. Saída = 0 se Atividade $<$ limitador.

A grande maioria das RNAs dispõem de uma regra de treinamento, no qual os pesos, que validam a influência de cada unidade simboliza para o sistema, são dessa forma ajustados e configurados com regras específicas correspondentes a um padrão preestabelecido para atuação em cada sistema neural.

Uma outra maneira de retratar uma saída do modelo de McCulloch e Pitts é por meio da função de ativação. Há diversos tipos de função de ativação. Função linear, função de escala e função sigmoide, que criam, na devida ordem, saída linear contínua, saída binária e uma saída não-linear contínua, de acordo com a **figura 4**.

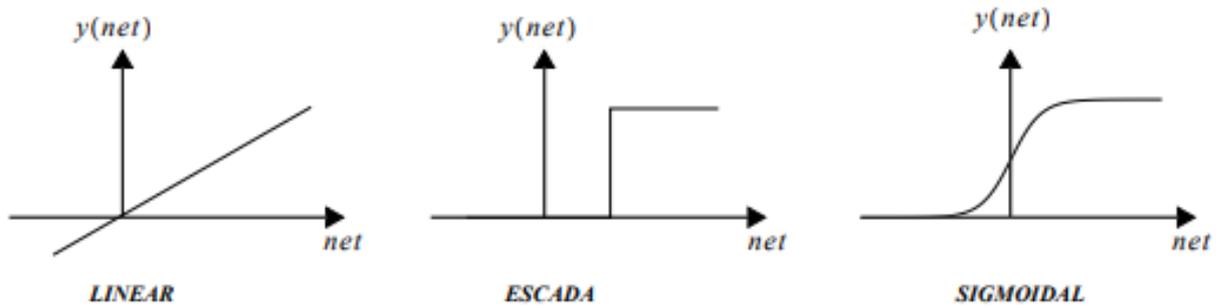


Figura 4- Funções de ativação
 Fonte: l1nq.com/elwT0

Trataremos somente a função sigmoide, em virtude a sua maior complexidade em comparação as outras. A função sigmoide é dada por:

- $g(z) = 1/1+e^{-z}$

As suas propriedades são:

- É uma função não linear, ou seja, tem formato de "S";
- Continua e diferencial no conjunto dos números Reais;
- Possui uma derivada simples e que é representada pela sua própria função $g'(z) = g(z)(1 - g(z))$.

4. APRENDIZADO DE MÁQUINA NA INDÚSTRIA E SEUS EFEITOS

As indústrias estão em uma busca interrupta por inovações para ganharem vantagens competitivas em relação a seus concorrentes do mercado. Conforme explicam Mateus e Mendonça (2020), essa busca por inovações inclui a aplicação de modelos de ML, os quais têm ajudado as empresas a melhorar seu desempenho a e crescer apesar do ambiente fortemente competitivo.

Gomes (2010) busca descrever que organizações que adotaram o uso da Inteligência Artificial (IA) notam que há um potencial benéfico, independente do segmento em que estão inseridos. Isso se dá ao fato de que a utilização da IA vai além da automação mecânica, abrangendo processos cognitivos, que são capazes de gerar aprendizado. Assim, um sistema de IA além de executar atividades repetitivas, numerosas e manuais, também fica responsável por demandas de análise e tomada de decisão.

Cossetti (2019) *Machine Learning*, envolve métodos de avaliação de dados que automatiza padrões analíticos em desenvolvimento, *Deep Learning* (DL), que realça a utilização de redes neurais artificiais com várias camadas de abstração, com maior aplicação no reconhecimento de padrões, e o Processamento de Linguagem Natural, que busca estudar maneiras de reproduzir processos de desenvolvimento ligados ao funcionamento

da linguagem humana.

Numerosos segmentos da indústria têm aplicado técnicas de ML para ajudar na tomada de decisão. Por exemplo, aplicações são achadas nas áreas de extração, de transformação, energética, alimentícia, construção civil, dentre muitas diversas. A machine learning se tornou uma importante aplicação no mercado para soluções de problemas em diversas áreas da indústria.

Importante reforçar o grande valor da ML na computação financeira, para análise de crédito e algoritmos para comercialização, também em processamentos de imagens e visão computacional para assim ser aplicado reconhecimento facial, detecção de movimentos e detecção de objetos e assim contribuindo para a segurança da humanidade. Presente ainda na biologia computacional, com a capacidade de detectar tumores, desenvolvimento de medicamentos e até mesmo em sequenciamento genético. E por último temos a área automotiva, aeroespacial e manufatura, com a aplicação da ML para possíveis manutenções preditivas.

Algoritmos de ML descobrem padrões nos dados e assim geram ações que ajudam a tomar melhores decisões e fazer previsões mais precisas. Os algoritmos contribuem em diagnósticos médicos, mercado de ações, previsão da carga de energia, entre muitos outros. Machine Learning ela está por trás de sites e muitos aplicativos com o objetivo de fazer sugestões e recomendações de produtos tais como filmes, músicas, moveis e muito mais. Tudo por análise do comportamento de seus clientes.

Podemos citar uma aplicação de ML na indústria sendo ela o próprio Google, fazendo a utilização de históricos de usuários para assim sugerir produtos com base em suas pesquisas na internet. No momento em que você faz uma pesquisa de algo que você nunca pesquisou antes, como por exemplo "jogar bola", o Google começa a indicar lojas que vendem acessórios relacionados ao tema que você pesquisou luvas, bolas, tênis e assim usando seu histórico para oferecer produtos. Portanto essa ML proporciona um ciclo infinito que movimenta as indústrias e ao mesmo tempo movimentando bilhões de dólares.

Importante frisar o estudo de outras formas de aplicações do ML na indústria.

- Controle de qualidade

O controle de qualidade é um enorme desafio para as indústrias. Assim a Machine Learning pode ajudar nesse trabalho, pode-se utilizar para elaborar algoritmos que possa distinguir peças de qualidade e peças com qualidade inferior, usando uma visão computadorizada.

- Manutenção

Uma grande vantagem do ML é a capacidade de prever a carência de manutenção de acordo com a necessidade da produção. Esse monitoramento auxilia na prevenção de falhas e também ajuda a elaborar manutenções de equipamentos. Dessa forma a indústria tem melhores resultados e os prejuízos reduzem bastante.



- Cadeia de Suprimentos

Tem como uma de suas tarefas com mais eficiência na indústria é o aperfeiçoamento da cadeia de suprimentos. Por tanto, fornecedores e compradores são capazes de colaborar de maneira que venha diminuir possíveis falhas de estoque, melhorar a previsão das previsões e datas de entrega de um determinado produto.

- Estoque

O gerenciamento de compra e a previsão de demanda, os modelos da cadeia de suprimentos, tem uma maior eficácia. Assim, o nível de segurança em relação a estoque pode ser ajustado para que fique bem mais próximo possível do que é realmente necessário, sem aumentos de gastos e sem danificar processos na tentativa de manter um grande estoque.

- Segurança

O contínuo monitoramento de rede corporativa autoriza entender como os equipamentos e as informações são aplicados pelas empresas a Machine Learning, quando identifica o comportamento habitual, pode identificar uma possível ameaça.

- Tomada de decisão

Esse modo de antecipação tem mais chances de levar a ação favorável para a corporação. E isso deixa bem claro a vasta gama de projetos nessa área, muitas novas tecnologias e com uma vasta demanda por novos profissionais.

4.1 Características do Aprendizado de Máquina

O termo Machine Learning (ML) comumente traduzido para o português como “aprendizado de máquina”, é um termo que foi mencionado pela primeira vez por um pioneiro em jogos de computador e inteligência artificial, Arthur Lee Samuel, especificando a ciência que utiliza os computadores para trabalhar autonomamente sem uma programação explícita (SYAM; SHARMA, 2018).

Os modelos computacionais modernos, em sua grande maioria, têm a capacidade de aprender são aplicados para resolver aqueles problemas que a programação comum não tem capacidade de solucionar.

O aprendizado por máquina possui três características importantes para ser entendida, foi estudado acima, uma breve introdução sobre estas características, vejamos agora um detalhamento mais aprofundado.

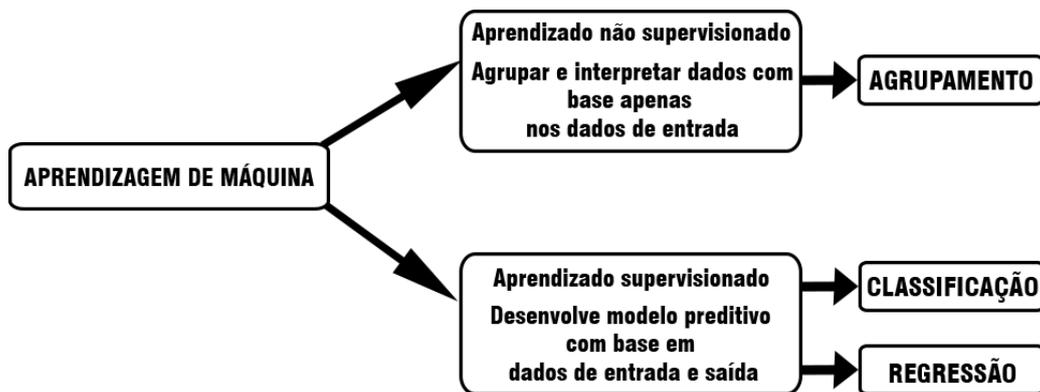


Figura 5- Modelo aprendizado modelo não-supervisionado e supervisionado

- **Aprendizado Supervisionado:** Machine Learning supervisionado elabora modelos que criam previsões com base em evidências, no entanto com algumas incertezas. Os algoritmos julgam dados (inputs) com respostas conhecidas (outputs) e dessa forma treinam modelos que irão gerar previsões razoáveis para novos inputs. Por esse motivo deve ser usado quando conjuntos de dados com resultados conhecidos estão livres. Muito usado para imagens médicas, reconhecimento de voz e pontuação de crédito.
- **Aprendizado Não-supervisionado:** ao contrário do exemplo acima o aprendizado não-supervisionado não usa dados classificados, com a intenção de melhor representar as informações. Esse aprendizado usa os dados testes não-classificados, assim reage aos dados com a paridade de cada um deles tendo como base em falta ou presença de cada um destes dados ou através de novos dados.
- **Aprendizado através de reforço:** máquinas que funciona por meio do aprendizado de reforço, trabalham com recompensa em estágios diferentes do problema. A cada reforço aplicado a máquina mira cada vez mais em receber essas recompensas com a finalidade de obter a recompensa final, a conclusão de algum problema.

5. CONSIDERAÇÕES FINAIS

Este trabalho se propôs, elaborar uma pesquisa que ajude a entender a importância da tecnologia no meio industrial que assim facilitar o entendimento da IA, neste caso, focou-se nas explicações da evolução industrial e no entendimento da indústria 4.0 que vem aplicando o uso da Inteligência artificial e aprendizado de máquina.

Vimos, portanto, como se deu as evoluções das tecnologias relacionadas à inteligência artificial e à aprendizagem de máquina. Com o propósito de mostrar as necessidades desta importante tecnologia para a evolução da indústria para os consumidores desse grande mercado universal e com o importante auxílio de pesquisadores da área.

Por meio de estudos feitos pelos pesquisadores McCulloch e Pitts, foi capaz de criar a pioneira rede neural tendo como objetivo de produzir uma máquina que pudesse aprender com uma grande semelhança à mente humana. Foi o início de um grande salto para a

inteligência artificial, compreendendo o funcionamento de um neurônio biológico e desta forma aplicando modelos matemáticos para a criação do neurônio artificial.

Portanto a inteligência artificial e à aprendizagem de máquina presentes na indústria se tornaram importantes aliados para uma maior velocidade de produção e com menos falhas assim proporcionando um grande desenvolvimento universal em diversas áreas.

Referências

ARAUJO, Fabia Melo de. **A inteligência artificial e os seus impactos no mundo do trabalho**. 2020. Tese de Doutorado.

BOMFIM, Marlon Alves. **Aplicação de técnicas de aprendizado de máquina para determinar a velocidade de produção em máquinas coextrusoras**. 2021. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

DA SILVA, Brigiane Machado; VANDERLINDE, Marcos. Inteligência artificial, aprendizado de máquina. **Revista Eletrônica Científica Inovação e Tecnologia**, Universidade Tecnológica Federal do Paraná, Câmpus Medianeira, Medianeira, Paraná, Brasil

GOLDSCHMIDT, Ronaldo Ribeiro. **Inteligência Computacional Fundação de Apoio à Escola Técnica Instituto Superior de Tecnologia do Rio de Janeiro**. Disponível em: <http://www.boente.eti.br/fuzzy/ebook/ebook-fuzzy-goldschmidt.pdf> acesso em: 30 out. 2021.

MAGALHÃES, Regina; VENDRAMINI, Annelise. Os impactos da quarta revolução industrial. **GV EXECUTIVO**, v. 17, n. 1, p. 40-43, 2018.

MENDONÇA, Cláudio Márcio Campos; DE ANDRADE, António Manuel Valente; DE SOUSA NETO, Manoel Veras. Uso da IoT, Big Data e inteligência artificial nas capacidades dinâmicas. **Revista Pensamento Contemporâneo em Administração**, v. 12, n. 1, p. 131-151, 2018.

OLIVEIRA, Elisângela Magela. Transformações no mundo do trabalho, da revolução industrial aos nossos dias. **Caminhos de Geografia**, v. 5, n. 11, 2004.

RAUBER, Thomas Walter. **Redes neurais artificiais**. Universidade Federal do Espírito Santo, v. 29, 2005.

REDES NEURAIS ARTIFICIAIS: PRINCÍPIOS BÁSICOS, v.1, n 13, p. 47-57, jan/jun. . Disponível em: <https://webcache.googleusercontent.com/search?q=cache:AK7FgQxIFpEJ:https://periodicos.utfpr.edu.br/recit/article/download/4330/Leandro+%&cd=3&hl=pt-BR&ct=clnk&gl=br> Acesso em: 30 OUT.2021

SACOMANO, José Benedito et al. Indústria 4.0. Editora Blucher, 2018.

SANTOS, Beatrice Paiva et al. Indústria 4.0: desafios e oportunidades. **Revista Produção e Desenvolvimento**, v. 4, n. 1, p. 111-124, 2018.

CAPÍTULO 10

ANÁLISE DE DADOS EM BI (*Business Intelligence*) OPORTUNIDADES NA GESTÃO DE TOMADAS DE DECISÃO E DEFINIÇÃO DE ESTRATÉGICA DE EMPRESAS DO SETOR ATACADISTA

BI DATA ANALYSIS (Business Intelligence) OPPORTUNITIES IN THE MANAGEMENT OF DECISION MAKING AND DEFINITION OF COMPANIES IN THE WHOLESALE SECTOR

José Vinicius Sousa Lemos¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

Na Faculdade Pitágoras na cidade de São Luís foi desenvolvido um projeto de pesquisa que atuou na utilização das tecnologias envolvidas e comunicação aplicadas. Neste projeto foi desenvolvido um sistema utilizando as linguagens de programação ensinadas no curso de ciência da computação e a lógica de raciocínio do mesmo, alguns projetos como um sistema web colocando informações de forma simples. Pensando assim com essa lógica percebe-se que podem ser utilizadas informações para as tomadas de decisões. As ferramentas de gestão de dados, denominada *Business Intelligence* (BI), podem ser importantes para fornecer informações completas e personalizadas para as camadas da gestão. O objetivo é apresentar a avaliação da aplicabilidade e potencialidade do uso de ferramenta de BI no planejamento das ações de gestão, no mundo cada vez mais conectado, o volume e variedade de dados gerados diariamente são sem precedentes na história da humanidade. As ferramentas de *Business Intelligence* buscam ressaltar por meio de gráficos, telas onde tornam a informação mais atraente aos olhos dos gestores, pois fazem cada vez com que a análise se torne mais clara, para que possa identificar as ferramentas utilizadas pela mesma. Em relação a metodologia do trabalho, utilizou-se a pesquisa descritiva, a mesma desenvolve-se sobre o estudo de caso. Quanto a abordagem do problema, o estudo caracterizou-se como quantitativo. Essa pesquisa busca realizar o estudo sobre o caso observando os benefícios que poderiam ser trazidos com o BI.

Palavras-chave: Business Intelligence. Tomada de Decisões. BI.

Abstract

At the Pitágoras College in the city of São Luís, a research project was developed that focused on the use of the technologies involved and applied communication. In this project a system was developed using the programming languages taught in the computer science course and its reasoning logic, some projects such as a web system putting information in a simple way. Thinking like this with this logic, it is clear that information can be used for decision making. Data management tools, called Business Intelligence (BI), can be important to provide complete and personalized information for the management layers. The objective is to present an assessment of the applicability and potential of using a BI tool in the planning of management actions, in an increasingly connected world, the volume and variety of data generated daily are unprecedented in human history. Business Intelligence tools seek to highlight, through graphics, screens where they make information more attractive to managers, as they make the analysis clearer every time, so that it can identify the tools used by it. Regarding the work methodology, descriptive research was used, which is developed on the case study. As for the approach to the problem, the study was characterized as quantitative. This research seeks to carry out the case study observing the benefits that could be brought with BI.

Keywords: Business Intelligence. Decision-making. BI.

1. INTRODUÇÃO

Neste capítulo foram abordados o tema e o problema deste trabalho, esclarecendo-se os objetivos gerais e os específicos a serem alcançados. Após expõe-se a justificativa do tema em questão.

O termo *Business Intelligence*, também conhecido como inteligência empresarial ou inteligência de negócios, foi criado na década de 80 pelo *Gartner Group*, com o objetivo de especificar um conjunto de metodologias de gestão aplicadas através de ferramentas de software (GARTNER, 2010). O *Gartner Group* é uma organização dedicada à consultoria de pesquisa de mercado na área de tecnologia da informação.

O principal motivo e objetivo do *Business Intelligence* é gerenciar os processos das organizações através do uso de ferramentas que permitem a visualização dos dados de forma clara, auxiliando nas identificações dos comportamentos das informações e favorecendo os processos de tomada de decisões. O objetivo deste estudo consiste em analisar como as ferramentas de BI, podem contribuir para o processo de tomada de decisão de uma empresa varejista no Estado do Maranhão.

2. JUSTIFICATIVA

Sistemas de informação são de grande necessidade e importância para uma empresa, considerando que a velocidade e a capacidade de processamento das informações podem melhorar o desempenho dos negócios, tornando a empresa mais ágil e performática na busca de informações.

Visto que com a grande competitividade no mercado empresarial faz necessário que as empresas devem buscar meios que possam torná-las diferentes umas das outras, buscando estratégias que possam torná-las competitivas. Por isso, deve-se dar enfoque aos sistemas que apoiam as tomadas de decisões.

Esse estudo torna-se relevante do ponto de vista social, pois comprova as informações levantadas dentro da organização, apresentando também as ferramentas que irão trabalhar essas informações, para tornar mais fácil de um sistema de apoio a decisões.

3. PORQUE UTILIZAR POWER BI

3.1 Power Bi Microsoft

Segundo o site oficial do produto, o Power BI é “um pacote de ferramenta de análise de negócios que oferece insights em toda a sua organização”. É um pacote de BI self ser-



visse que oferece varias alternativas de conectividade com dados como planilhas do Excel, fontes de dados locais, big data, fluxo de dados e serviços de nuvem, banco de dados SQL, Google Analytics e entre outros. Nesse sentido, dizemos que se trata de BI self-service por ser de fácil manuseio, não precisar de conhecimento em programação e por ser muito rápido em transformar as intenções entre dados em visualizações dinâmicas, neste ponto podemos destacar como sendo o mais forte destas ferramentas, os dashboards criados pelo software são extremamente versáteis e dinâmicos, que podem ser gratuitos no pacote básico, que facilitam o acesso a ferramenta por empresas de pequeno porte. Além disso, organizações maiores podem se utilizar de pacotes por volume de dados que, podem incluir interações entre a versão desktop, serviços (site) e aplicativo, e integrar vários usuários. Desta forma, o poder BI pode se adequar as mais diversas necessidades que o mundo empresarial pode demandar.

3.2 BI Self Service

Para elucidar como funcionar as plataformas de BI self service, resgatamos Palmisano e Rosine (2003) que diziam que os primeiros produtos de BI eram de difícil manuseio e precisam de conhecimento em programação, o que traziam uma perda de agilidade, e que as ferramentas atuais superam esse gap se tornando ferramentas de fácil utilização por qualquer profissional das empresas. Alinhando com esse contexto, surgem as ferramentas de BI self service, que facilitam ainda mais sua utilização, favorecendo o usuário final, que em muitos casos precisam de agilidade para tomar decisões. As ferramentas antigas eram necessárias envolver a área de TI, que por muitas vezes, retardavam o processo, chegando a ocorrer casos em que a informações perdia validade para tomada de decisão.

3.3 Benefícios e dificuldades

Os benefícios organizações do uso das informações processados pelos sistemas de BI podem ser percebidos por meio da geração de receita, redução de custo e efetividade gerencial. Esses benefícios estratégicos estão associados aos desempenhos da organização (WRIGHT, 1993).

A interagir da empresa uma vantagem competitiva por meio da geração da receita. A melhora no desempenho é esperada através do sucesso da introdução de um novo produto/serviços ou desenvolvimento de um novo mercado (TEO; CHOO, 2001). As empresas que possuem sistemas avançados que monitoram as atividades de seus concorrentes exibem maior lucratividade. Sistemas de BI permitem que as empresas aproveitem a rentabilidade da racionalização da cadeia de suprimentos para aumentar a competitividade. Além disso, a possibilidade de fechar novos negócios é aumentada quando um sistema integrado facilita as transações.

Percebe-se que a informação traz mais benefícios que os dados para a camada tomadora de decisão de uma organização. Segundo Primak (2008), a informação faz parte da base da construção do conhecimento. Infelizmente muitas das iniciativas de Business Intelligence (BI) não alcançam o sucesso. As empresas buscam no BI formas para melhorar

o desempenho organizacional e o diferencial competitivo. Apesar das vantagens e benefícios encontrados nesta solução, algumas tentativas de adoção não vão adiante devido a barreiras encontradas pelo percurso. As dificuldades mais comuns são encontradas dentro da própria organização (ambiente interno). Entre elas estão a barreira cultural, falta de visão estratégica, inexistência ou má qualidade dos dados, centralização da solução e escolha incorreta da ferramenta de BI para os usuários. O BI interfere na forma que a organização pensa e age no dia a dia. E, como toda mudança, há empecilhos a serem enfrentados. A barreira cultural na empresa é um grande problema a ser encarado. Muitas pessoas não querem mudar sua forma de trabalho pelo enraizamento do processo atual e pela comodidade de continuar como está. Também, muitas vezes, é devido a insegurança de terem seus trabalhos ameaçados pela nova tecnologia. Seus benefícios não serão visíveis se a empresa não dispuser de uma estrutura organizacional analítica séria e responsável a disposição dos gestores.

4. POWER BI NA TOMADA DE DECISÃO E TECNICAS

4.1 Informação

Pode-se definir a informação como dados que foram organizados e manipulados para o entendimento do usuário final, Para Rezende (2006 p.62), "informação é todo o dado do trabalho, útil, tratado, com valor significado atribuído ou agregado a ele e com um sentido natural e logico".

Os dados são processados, comparados, classificados, sendo assim transformados em informações para usuário finais.

Para Oliveira (2000, p. 167), "informações é dado trabalhando que permite ao executivo tomar decisões."

É primordial obter informações de qualidade, onde elas tenham alguns atributos que fazem importantes, como: tempo, conteúdo e forma. No Quadro 1 é possível visualizar de forma mais clara esses atributos.

Quadro 1: resumo dos atributos da qualidade da informação.

Dimensões do Tempo	
Prontidão	A informação deve ser fornecida quando for necessária
Aceitação	A informação deve estar atualizada quando for fornecida
Frequência	A informação deve ser fornecida tantas vezes quantas forem necessárias
Período	A informação deve ser fornecida sobre períodos passados, presentes e futuros
Dimensões do Conteúdo	
Precisão	A informação deve estar isenta de erros
Relevância	A informação deve estar relacionada às necessidades de informação de um receptor específico para uma situação específica
Integridade	Toda a informação que for necessária deve ser fornecida
Concisão	Apenas a informação que for necessária deve ser fornecida
Amplitude	A informação pode ter um alcance amplo ou estreito, ou um foco interno ou externo
Desempenho	A informação pode revelar desempenho pela mensuração das atividades concluídas, do progresso realizado ou dos recursos acumulados.

4.2 Sistema de Informação Gerencial (SIG)

Esses sistemas focam em fornecer informação e apoio para a tomada de decisão eficazes para os gerentes. Por isso, são chamados de sistemas de apoio gerencial (O'BRIEN, 2003). Eles fornecem informação na forma de relatórios alguns em exibição de vídeos para exporem os resultados, análises de vendas, relatórios semanais. Para Oliveira (1999 p. 40), "Sistema de Informações Gerenciais (SIG) é o processo de transformação de dados em informações que são utilizadas na estrutura decisória da empresa, proporcionando, ainda, a sustentação administrativa para otimizar os resultados esperados." O SIG auxilia os executivos a consolidar três requisitos básicos para sustentação da empresa: qualidade, produtividade e participação. Onde a qualidade envolve o nível de satisfação dos funcionários associado a uma qualidade de vida também no seu lado pessoal, pois quando ocorrem desequilíbrios nessa relação geralmente ocasionam greves, perda de produção, que podem causar danos a empresa (OLIVEIRA, 2004). Já a produtividade deve consolidar o comprometimento de todos com os resultados parciais da empresa, e a participação deve resultar nas melhorias de qualidade e produtividade.

4.3 Sistemas de Informação Estratégicas (SIE)

Esse tipo de sistema busca auxiliar a alta administração nas tomadas de decisões, ele considera o meio ambiente interno e externo da empresa, para apresentar informações. Para Rezende (2006, p. 137) "Habitualmente, trabalham com muitas informações gráficas, amigáveis e normalmente on-line, observando as particularidades de cada empresa e, ainda, com a opção de descer no nível de detalhada informação." Diante disso, Turban, Rainer Jr e Potter (2007), também destaca que esse tipo de sistema inclui o apoio à análise, comunicação, automação de escritório e o apoio à inteligência. Facilitam a tomada de decisão por serem de fácil acesso aos dados. Como exemplo desse tipo de sistema, podem ser citadas decisões entre: valor de faturamento e contas a pagar, custos em relação ao retorno, com orçamento e análise financeira, quantidade produzida com pedidos em negociação.

Pelo sistema a partir de um código identificador. Quanto à qualidade dos dados, observou-se que ela era adequada, pois os atributos são preenchidos automaticamente com a utilização da tecnologia de código de barras e 70% (setenta por cento) dos itens são pré-definidos por padrões do sistema.

4.4 Pré-processamento

A etapa do pré-processamento é considerada a base para as demais etapas, pois, se essa não for bem definida, poderá impactar negativamente nos processos e, ainda, não obter o conhecimento esperado.

As ações realizadas na fase de pré-processamento foram:

1. Utilizar a etiqueta de paletes para subsidiar a análise das entradas de dados do sistema de gerenciamento e controle do estoque.
2. Verificar a quantidade de dados armazenados no banco de dados fornecidos por meios de planilhas por vezes com várias fórmulas e arquivos diferentes;
3. Renomear os atributos de dados;
4. Efetuar operações preliminares de limpeza de informações.

4.5 Entendendo as variáveis do Banco de Dados

O banco de dados disponibilizado para a pesquisa possui inúmeras variáveis, com um conjunto de atributos que envolvem a localização do endereço dentro do estoque de acabados, segmentação de endereços, códigos de controle de produtos, códigos de nota



fiscal para recebimento de terceiros, problemas de monitoramento de paletes, tempo de vida de produtos, classificação em produtos com data crítica, entre outros.

De modo particular, e por se tratar de uma análise de pré-processamento, destacaram-se como variáveis essenciais os atributos diretamente relacionados à operação de movimentação de produtos no estoque e, nestes, foi necessário realizar a transformação de atributos em chaves de identificação e alguns tratamentos de dados. Entretanto, considerando os objetivos de negócios e da pesquisa e, ainda, a análise preliminar dos dados, pode-se afirmar que pelo menos quatro variáveis são essenciais para o estudo e outras serão geradas a partir dos dados existentes.

1. Chave (identificador de cada paleta - etiqueta);
2. Código do produto;
3. Nota Fiscal;
4. Vendedor;
5. Gerente;
6. Matriz;
7. Comissão;
8. Comissão (porcentagem);
9. Cidade/Estado;
10. Região (entrada ou saída do produto);
11. Produto;
12. Quantidade;
13. Preço;
14. Data.
15. Total.

4.6 Análise dos Dados

A análise dos dados visa estabelecer uma visão geral das informações em que se pretende trabalhar. Neste trabalho foram utilizados dados históricos de movimentação de pa-

letes dentro do estoque de acabados de uma empresa alimentícia, sendo estes produzidos pelo sistema interno de Sistema de Gerenciamento de Estoque que adota as políticas de estoque definidas pela própria empresa.

A Figura 1 apresenta a evolução de armazenamento de dados ao longo dos meses do ano de 2017 dado ao processo de implantação do sistema na área de estoque de acabados da empresa em estudo. A utilização do sistema está sendo ampliada na empresa, onde mais pessoas são responsáveis por inserir informações.

Foram criados filtros dinâmicos e automatizados conforme é atualizado as planilhas. Como por exemplos sistemas por ano e por região.

A Figura1 ilustra os filtros do sistema por ano e região.



5. CONSIDERAÇÕES FINAIS

O objetivo principal deste trabalho é aprimorar a gestão de armazenagem de produtos no estoque de uma indústria de produtos de Informática no setor de atacado, potencializando sua eficácia em ocupação e direcionamento no processo de armazenagem logística.

Para isso, foi efetuada uma pesquisa bibliográfica envolvendo as etapas para realização da análise de dados utilizando métodos de inteligência de negócios, além do estudo de formas de estruturação.

Considerando o estudo relacionado ao planejamento de estoque e a busca de soluções maximizando o potencial ocupacional, este projeto investigou métodos de avaliação dos processos e de análise de dados que auxiliariam na identificação de oportunidades de melhoria, apresentando uma prática de investigação por meio de dados históricos sobre o processo de armazenagem, compra de insumos e venda de produtos acabados.

Referências

AUDY, JORGE LUIS NICOLAS; ANDRADE, GILBERTO KELLER DE; CIDRAL, ALEXANDRE. **FUNDAMENTOS DE SISTEMAS DE INFORMAÇÃO**. PORTO ALEGRE : BOOKMAN, 2005.

BARBIERI, CARLOS. **BI-BUSINESS INTELLIGENCE: MODELAGEM & TECNOLOGIA**. RIO DE JANEIRO: AXCEL BOOKS, 2001.

CERVO, ARNALDO LUIZ; BERVIAN, PEDRO ALCINO; SILVA, ROBERTO DA. **METODOLOGIA CIENTÍFICA**. 6ª EDIÇÃO. SÃO PAULO: PERSON PRENTICE HALL, 2007.

GRAEML, ALEXANDRE REIS. **SISTEMAS DE INFORMAÇÃO: O ALINHAMENTO DA ESTRATÉGIA DE TI COM A ESTRATÉGIA CORPORATIVA**. 2ª EDIÇÃO. SÃO PAULO: ATLAS, 2003.

MCGEE, JAMES; PRUSAK, LAURENCE. **GERENCIAMENTO ESTRATÉGICO DA INFORMAÇÃO: AUMENTE A COMPETITIVIDADE E A EFICIÊNCIA DE SUA EMPRESA UTILIZANDO A INFORMAÇÃO COMO UMA FERRAMENTA ESTRATÉGICA**. 10ª EDIÇÃO. RIO DE JANEIRO: EDITORA CAMPUS, 2002.

O'BRIEN, JAMES A. **SISTEMAS DE INFORMAÇÃO E AS DECISÕES GERENCIAIS NA ERA DA INTERNET**. 1ª EDIÇÃO. SÃO PAULO : SARAIVA, 2003.

O'BRIEN JAMES A. **SISTEMAS DE INFORMAÇÃO E AS DECISÕES GERENCIAIS NA ERA DA INTERNET**. 3ª EDIÇÃO. SÃO PAULO : SARAIVA, 2010.

OLIVEIRA, DJALMA DE PINHO REBOUÇAS DE. **SISTEMAS DE INFORMAÇÕES GERENCIAIS ESTRATÉGIAS TÁTICAS OPERACIONAIS**. 6ª EDIÇÃO. SÃO PAULO : ATLAS S.A., 1999.

OLIVEIRA, DJALMA DE PINHO REBOUÇAS DE. **SISTEMAS DE INFORMAÇÕES GERENCIAIS: ESTRATÉGIAS, TÁTICAS, OPERACIONAIS**. 9. ED. REV. E ATUAL. SÃO PAULO: ATLAS, 2004.

OLIVEIRA, SILVIO LUIZ DE. **TRATADO DE METODOLOGIA CIENTÍFICA: PROJETOS DE PESQUISAS, TGI, TCC, MONOGRAFIAS, DISSERTAÇÕES E TESES**. SÃO PAULO: PIONEIRA, 1999.

CAPÍTULO 11

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*

Hercio Lucas Coelho Goncalves¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

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 Demonstrar 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. (FLÁVIO 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 (BUYA 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 ideia 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. (FLÁVIO 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 so-

luções 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 (CARLOS 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 (JESSICA 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 (RENATO 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 (MAYARA 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 (MAYARA 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; VEDSO, 2016).

A computação em nuvem permite que as indústrias imprimam muito mais funcionalidades no seu dia a dia. Por exemplo, na fabricação de um peça, as máquinas precisam de informações de comando, como quantidade, modelo, material utilizado e 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 (ADRIANO PEREIRA; EUGÊNIO 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 a o que (CLEITON RODRIGUES; FRANZ 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 (MILENA 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 (MAYARA 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 (DIEGO RAFAEL 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 (ADRIANO 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 (ADRIANO 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 (BRUNA THOMÉ; EDUARDO 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 (FERNANDO 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 (FERNANDO 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 (ADRIANO 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 (JULIO ALBA 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 (MYLENA 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 a 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 andróides, IOS e Windows Phone, além de consoles, através de aplicativos, correios eletrônicos e plataformas digitais que permitem esse tipo de armazenamento (LUCAS 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 (RAPHAEL DE AQUINO 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 (RAPHAEL DE AQUINO 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 (LUCAS 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 (LUCAS 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 (RAPHAEL DE AQUINO 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.

BUYA ET AL, RAJKUMAR BUYA, 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.** Disponível em: 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: Towards a Cloud Definition.** ACM SIGCOMM Computer Communication Review, 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.

CAPÍTULO 12

APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL

ARTIFICIAL INTELLIGENCE APPLICATIONS

Karoline Costa Rodrigues¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

A Inteligência Artificial é uma das áreas de pesquisa mais amplas da Ciência da Computação, e tem ganhado espaço em diversas áreas no cenário global. O objetivo principal dessa pesquisa bibliográfica foi demonstrar as aplicações da Inteligência Artificial, sua participação mundial, relevância e corroboração dos meios. E teve como objetivos específicos: apresentar a história da Inteligência Artificial; expor as aplicações da Inteligência Artificial no dia a dia e compreender a tecnologia como aliada para a vida humana. A metodologia utilizada foi a revisão bibliográfica de caráter descritivo e explicativo, a pesquisa foi realizada nas bases de dados Biblioteca Virtual Kroton e Google Acadêmico. Utilizou-se artigos com data de publicação entre 2004 e 2022, nos idiomas português e inglês. As principais áreas da IA são: Aprendizado de Máquina e as redes neurais. As aplicações da IA são usadas para detectar fraudes em páginas da web e em dispositivos móveis e etc. Os gestores e professores da educação da atualidade fazem uso de plataformas digitais como o YouTube, Google, Moodle, como aliada ao ensino. A IA é um dos recursos da atualidade usado pelos bancos, como por exemplo: a BIA. A sociedade tem grande dependência das tecnologias como modo de sobrevivência da sociedade, e essas tecnologias estão presentes nos: carros, aviões, energia elétrica, telefone móvel, televisão, internet e computador, ensino e processamento de linguagem. A ciência e a tecnologia melhoram a compreensão dos processos de saúde e doença. E o marketing digital/marketing eletrônico viabiliza ações de divulgação e venda na internet.

Palavras-chave: Segurança de dados, Medidas de controle, Segurança da informação.

Abstract

Artificial Intelligence is one of the broadest areas of research in Computer Science, and has gained space in several areas on the global stage. The main objective of this bibliographic research was to demonstrate the applications of Artificial Intelligence, its worldwide participation, relevance and corroboration of the means. And it had as specific objectives: to present the history of Artificial Intelligence; expose the applications of Artificial Intelligence in everyday life and understand technology as an ally for human life. The methodology used was the bibliographic review of a descriptive and explanatory nature, the research was carried out in the Kroton Virtual Library and Google Scholar databases. Articles with a publication date between 2004 and 2022, in Portuguese and English, were used. The main areas of AI are: Machine Learning and Neural Networks. AI applications are used to detect fraud on web pages and mobile devices etc. Today's education managers and teachers make use of digital platforms such as YouTube, Google, Moodle, as an ally to teaching. AI is one of the current resources used by banks, such as the BIA. Society is heavily dependent on technologies as a way of society's survival, and these technologies are present in: cars, airplanes, electricity, mobile phones, television, internet and computers, teaching and language processing. Science and technology improve understanding of health and disease processes. And digital marketing/electronic marketing enables dissemination and sales actions on the internet.

Keywords: Data security, Control measures, Information security.



1. INTRODUÇÃO

A Inteligência Artificial é um dos campos de pesquisa mais amplos e fascinantes da Ciência da Computação, vem ganhando espaço em várias áreas no cenário mundial, a IA é ótima em processar grande quantidade de dados e conseguir estabelecer relações de causa e efeito, experiências únicas e entendimentos, amplificando nossa capacidade cognitiva para gerar valor e experiências fantásticas.

É considerada um dos grandes feitos da ciência e tecnologia moderna, sua evolução desencadeou um avanço significativo em diversos setores da sociedade, tendo influência em absolutamente tudo na vida do ser humano, como potencialização e melhora do desempenho das tarefas e aumento da produtividade em um curto intervalo de tempo.

Diante desses aspectos, a problemática da pesquisa tem como objetivo a contribuição para o estudo sobre a importância das aplicações da IA, essa tecnologia está em constante evolução e seu crescimento oferece utilidades gigantescas e com isso diversos setores já estão fazendo uso da mesma para obtenção de feitos mais proveitosos. Diante disso, pergunta-se: quais as aplicações da Inteligência Artificial no mundo contemporâneo?

O presente trabalho tem como objetivo contribuir com mais pesquisa sobre o assunto e esclarecer a sociedade e a comunidade acadêmica de forma clara e sucinta sobre as grandes funcionalidades da Inteligência Artificial, aplicações, métodos utilizados, participações e particularidades.

O objetivo principal dessa pesquisa bibliográfica foi demonstrar as aplicações da Inteligência Artificial, sua participação mundial, relevância e corroboração dos meios. E teve como objetivos específicos: apresentar a história da Inteligência Artificial; expor as aplicações da Inteligência Artificial no dia a dia e compreender a tecnologia como aliada para a vida humana.

Como metodologia foi utilizada a revisão bibliográfica de caráter descritivo e explicativo, a pesquisa foi realizada nas bases de dados Biblioteca Virtual Kroton e Google Acadêmico. A pesquisa mencionou artigos publicados entre 2004 e 2022, nos idiomas português e inglês, foram utilizados como descritores: segurança de dados, medidas de controle e segurança da informação. Foram selecionados os artigos após a leitura e análise dos materiais, e assim foi constituído o corpo do trabalho. Os dados foram selecionados de acordo com o tema do estudo.

2. HISTÓRIA DA INTELIGÊNCIA ARTIFICIAL

Lima, Pinheiro e Santos (2014), afirmam que a Inteligência Artificial (IA) é o conjunto de ações que, se fossem feitas por um ser humano, o mesmo seria dado como inteligente. Desta maneira pode-se comparar as ações dos computadores com as ações do homem para definir se está realizando um comportamento inteligente ou não. Russell e Norvig

(2013) descrevem que a IA é a capacidade dos sistemas cibernéticos (computadores, softwares, sensores e atuadores) de reproduzir funções cognitivas dos humanos, como por exemplo resolver problemas através do aprendizado focado na percepção.

McCorduck (2004) menciona que a ideia de seres artificiais inteligentes e antropomórficos tem tanto tempo quanto a humanidade, e para provar tal ideia, a autora aponta um poema Pigmalião, de Ovídio, escrito pelo escultor Pigmalião — esculpe uma estátua de marfim tão bela e perfeita que se apaixona por ela. Em súplica a Afrodite por um amor que seja à semelhança de sua estátua, se surpreende quando ela própria ganha vida e corresponde ao seu amor.

Na época de Ovídio, McCorduck (2004) descreveu que Heron de Alexandria fazia homens mecânicos, e que tinham como nome “autômatos”. Os autômatos de Heron eram manequins com mecanismos internos que possibilitam a movimentação na qual as configurações eram feitas pelo inventor. O filósofo Aristóteles definiu as regras do silogismo, no qual permitem o desenvolvimento de raciocínios matemáticos de forma exata, sem ambiguidades ou contradições, quando os mesmos eram feitos dentro das regras (FRANCO, 2014).

Mesmo hoje na atualidade o silogismo aristotélico está em vigor na lógica booleana, sendo primordial na função dos computadores. Na era moderna, a história da IA é mostrada em computadores digitais. O primeiro computador digital foi criado em 1941 pelo engenheiro alemão Konrad Zuse, impulsionado pela corrida pela criação de máquinas mais potentes para ajudar durante a Segunda Guerra Mundial (RUSSELL; NORVIG, 2013).

Em 1943 Warren Sturgis McCulloch e Walter Pitts publicaram o artigo seminal “A Logical Calculus of the Ideas Immanent in Nervous Activity” (em português, um cálculo lógico das ideias imanentes à atividade nervosa), sendo a base para construção de redes neurais que são desenvolvidas na atualidade (NILSSON, 2010).

Em 1948, John Von Neumann afirmou, como resposta a uma pergunta que foi feita ao longo de suas palestras: “Você insiste que há algo que uma máquina não pode fazer. Se você me disser precisamente o que é que uma máquina não pode fazer, então eu sempre posso fazer uma máquina que fará exatamente isso!”, a afirmação de Neumann da base a tese de Church-Turing, que diz que qualquer procedimento formal pode ser feito por uma máquina de Turing (por um computador genérico) (MCCORDUCK, 2004).

Em 1950 Alan Turing, prevendo o desenvolvimento da IA, propôs o Teste de Turing para medir a equivalência de inteligência de um computador (LEÇA, 2017). Nilsson (2010) em 1952 relatou que dois pesquisadores conseguiram atingir o mesmo resultado do Teste de Turing, no qual Arthur Samuel, da IBM, e Christopher Strachey da Universidade de Oxford, foram considerados os precursores da IA, onde os dois criaram de forma independente versões do jogo de damas, e o resultado foi que o jogo do computador conseguia ter sucesso mesmo contra bons jogadores amadores.

Samuel e Strachey conseguiram mostrar as primeiras instâncias de que um computador podia ser usado para realizar uma atividade humana. Em 1955 Samuel melhorou seu jogo, adicionando elementos que permitiam ao computador usar dados de jogos anteriores, permitindo o melhoramento do desempenho. E, portanto, essa é a primeira

instância de aprendizado de máquina que tem registrado na história dos computadores digitais (NILSSON, 2010).

Os programas de Samuel e Strachey foram as primeiras instâncias de aplicação de métodos heurísticos para solucionar problemas. E a solução de ambos pesquisadores eram montar uma árvore de busca com diversas possibilidades de jogadas, por meio da aplicação de um método de atribuição de valor a cada função da vantagem que atribuem ao jogador. Portanto, o programa tenta se antecipar às possibilidades, criando uma árvore com diversos níveis de profundidade, no qual busca o caminho de maior valor (RUSSELL; NORVIG, 2013).

No Dartmouth College em 1956, os pesquisadores John McCarthy, Marvin Minsky, Nathan Rochester e Claude Shannon organizaram a primeira conferência sobre inteligência artificial. E esse termo "IA" foi criado para essa conferência, dando início às pesquisas e estudo sobre esse tema. Depois desse evento houve o surgimento de muitos estudos e artigos, dando início ao florescimento de resultados no decorrer das décadas de 50 e 60 (FRANCO, 2014).

Em 1963 Leonard Uhr e Charles Vossler publicaram o artigo *A Pattern Recognition Program That Generates, Evaluates, and Adjusts Its Own Operators* (em português "Um programa de reconhecimento de padrões que avalia e ajusta seus próprios operadores"), que descreveu um programa que tinha capacidade de aprender usando um mecanismo de aquisição de informações, podendo modificar-se seus próprios parâmetros e adaptar-se às condições a ele apresentadas. Esse programa passou a ser chamado de machine learning, ou seja, aprendizado de máquina (LEÇA, 2017).

Joseph Weizenbaun pesquisador do MIT em 1965, criou o programa Eliza, que tinha capacidade de entender sinteticamente um conjunto de sentenças digitadas e de dar respostas, e sua comunicação era feita por trocas de mensagens. Esse foi um dos exemplos mais clássicos da linguagem natural sendo interpretada pelo computador (KELLY, 2017;).

O pesquisador Alain Comerauer em 1972 criou a linguagem Prolog, na qual tinha como função a resolução de problemas através da aprendizagem e interpretação lógica de sentenças. Em 1974, o pesquisador Paul Werbos, mencionou sobre o seu algoritmo de retropropagação, sendo precursor fundamental para o desenvolvimento das redes neurais, sendo usado na atualidade no processo de aprendizagem de máquina (ROSA, 2011).

Hans Berliner em 1979, desenvolveu o programa BKG, e venceu até o campeão mundial de gamão, pela primeira vez na história o computador teve uma vitória expressiva sobre um humano. Em 1997, o computador Deep Blue, da IBM, derrotou o Garry Kasparov, o campeão mundial do jogo de xadrez. E em 2016 o programa AlphaGo, do Google, derrotou o campeão mundial do jogo de tabuleiro Go, Lee Sedol (KELNAR, 2016).

Em 1990 foram desenvolvidas diversas pesquisas sobre a IA em universidades e passaram a ser exploradas pelas empresas. Em 1998 a Google passou a ser conhecida. Essa empresa era sediada em Mountain View, na Califórnia, com especialidade em aplicar a IA em tudo o que faz, bem como, na máquina de busca que arremessou, consagrando essa empresa a sucesso mundial como é conhecida hoje (KHAIDEM, 2018).

As assistentes pessoais da Apple (Siri), da Amazon (Alexa), da Google (OK Google), da Microsoft (Cortana) e da Samsung (Bixby), são exemplos de treinamento de redes neurais, a expressão mais atual da IA, e que pode trazer benefícios ao público em geral. E com o passar dos tempos os assistentes pessoais vão compreender com mais clareza o que se é falado e poderão ajudar com mais precisão (FRANCO, 2014; KELLY, 2017).

2.1 Principais áreas da inteligência artificial

2.1.1 Aprendizado de máquinas

O Aprendizado de Máquina é uma área da IA que tem como objetivo a criação de sistemas com capacidade de aprender através de dados, bem como, por meio da análise de problemas anteriores, e os algoritmos de aprendizado de máquina possuem a capacidade de tomada de decisões (LEÇA, 2017).

O principal objetivo do aprendizado de máquina é o desenvolvimento de modelos de software que passam por treinamentos com altos volumes de dados, e dessa forma, necessita de uma precisão maior dos algoritmos. E devido ao crescimento da era digital, da rede mundial e das redes sociais, bem como, as altas quantidades de informações produzidas no dia a dia, é o cenário perfeito para essa tecnologia (BARNES, 2015).

A aprendizagem profunda é uma área de estudo que facilita o aprendizado de máquina, e tem como foco realizar e executar tarefas inteligentes, que antes eram realizadas por humanos. E seu funcionamento engloba uma grande quantidade de dados à um sistema de computador para que o mesmo possa tomar as decisões sobre as informações novas (KASHYAP, 2017).

Os dados do aprendizado de máquina são alimentados por redes neurais, por meio de construções lógicas que fazem uma série de verificações binárias de verdadeiro ou falso, ou mesmo extraem valores numéricos. Cada bit de dados que passam por meio dessas redes neurais é classificado de acordo com as respostas recebidas, essas redes são complexas o suficiente para processar diversos conjuntos de dados com total precisão (BARNES, 2015; EDISSON, 2017).

E a aprendizagem profunda é a área mais recente dos estudos de aprendizagem de máquina, e seu objetivo inicial é criar inteligência artificial. O termo profundo é referente ao número de camadas de redes neurais, e tem como característica o aprendizado hierárquico, onde os modelos de aprendizado retiram de modo automático o conhecimento através de outros dados (EDISSON, 2017).

Esse tipo de aprendizado possibilita modelos de computadores que são integrados por diversas camadas de processamentos a aprender sobre as informações que contém diversos níveis de abstração. O uso da aprendizagem profunda é bem eficaz na resolução de problemas de dados com imagens, documentos, áudios, textos e arquivos (MEHTA, 2017).

2.1.2 Rede neurais

As Redes Neurais é um assunto da computação com inspiração na natureza que nos rodeia. Por muitos anos os seres humanos trabalharam bastante para desenvolver computadores mais rápidos e com potências maiores, porém esses computadores apresentavam falhas na hora de realizar atividades de uma criança com 3 anos realiza de modo imediato, por exemplo: reconhecer algo ou aprender um assunto novo apenas com a experiência (CONTI; WIGGERS; RIBEIRO, 2016).

A área de conhecimento às Redes Neurais vem crescendo e se tornou diversamente incrível, com variados tipos de redes neurais e aplicações. Uma das redes neurais mais conhecida popularmente são: as redes neurais feedforward, e é bem conhecida devido ao seu algoritmo de treinamento o backpropagatio (MILOJKOVIÜ; LITOVSKI; LITOVSKI, 2012).

A criação das redes neurais é baseada na ideia de simular o cérebro humano em pelo funcionamento e com suas potencialidades. Dessa maneira, os cientistas decidiram criar um modelo de computador que imitasse o comportamento do cérebro humano, ou seja, análogo a fisiologia cerebral. Foram desenvolvidos neurônios artificiais similares aos dos seres humanos, e foram interligados até formar redes que tiveram a capacidade de realizar atividades cognitivas e/ou criativas, que eram anteriormente restritas somente ao cérebro (RAHMAN; ESMAILPOUR; ZHAO, 2016).

Dessa maneira, a definição de uma Rede Neural é como um processador distribuído, é constituído por um grande número que apresentam unidades de processamento simples, e que são propensos a naturalidade de armazenar conhecimento experimental, tornando-o disponível para ser usado. Essas unidades de processamento simples no início eram neurônios artificiais que foram definidos por McCulloch e Pitts em 1943, e esse aprendizado foi transformado em algoritmo por Charles Hrbb em 1949. Desta forma, se pode ver que as Redes neurais não é uma área nova, pois já havia pesquisa consolidada a muitas décadas (IMEN *et al.*, 2015).

Um das principais áreas de aplicação que as redes neurais costumam a ter sucesso é na área de previsão. Pois, essas redes conseguem entender os padrões através de dados crus, entendendo muito da dinâmica subjacente aos dados, e com isso realiza um bom trabalho de extrapolação, criando previsões muito confiáveis e precisas (EFE; CEBECI, 2013).

3. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO COTIDIANO

O dia a dia tem grande influência pelo mundo audiovisual, e as Tecnologias são os meios de fazer e representar. Com a crescente criação de momentos e ambientes informatizados estão acarretando grandes atividades eletrônicas em todas as áreas da vida humana, sendo esse conjunto classificado como uma nova dimensão social da atualidade (CONTI; WIGGERS; RIBEIRO, 2016).

No decorrer dos últimos anos vem acontecendo um crescimento acelerado da presen-

ça da IA no dia a dia. E em diversas situações usamos a IA, e na maioria das vezes nem percebemos, como os modelos criados por algoritmos de IA. Usamos também em atividades rotineiras como ler mensagens via e-mail, dirigir veículo autônomo ou semiautônomo, lavar roupas, escolher série ou filme para assistir em uma plataforma de streaming (FACELI, 2021).

Coelho (2017) relata que hoje em dia o aprendizado de máquina (Machine Learning) é uma importante área da IA, essa tecnologia associada a aplicação de algoritmos criam uma interação a partir de dados, usando isso para ensinar um produto inteligente, a realizar atividades e aprender sozinho no meio que se encontra.

Prado e Hisatugu (2016), dentro da área de aprendizado de máquina surgiu uma nova tecnologia designada como "Deep Learning" ou Aprendizado Profundo. O aprendizado profundo é fundamentado no conceito de redes neurais que reproduzem o cérebro humano. E a cada dia que passa essas IA's vem ganhando mais espaço na sociedade, sendo visto nos sistemas que controlam os carros, no processamento de linguagens, aplicações na medicina, reconhecimento de imagens, em diagnósticos radiológicos, no desenvolvimento de medicamentos e etc.

A IA não está ligada somente a robôs ou agentes autônomos. Muitas das nossas atividades diárias são alimentadas por algoritmos de Machine Learning, como por exemplo: anúncios em tempo real, resultados de pesquisa na Web, detecção de fraudes em páginas da web e em dispositivos móveis, previsão de falhas em equipamentos, detecção de invasão de rede, análise de sentimentos fundamentadas em textos, reconhecimento de imagens e etc. Sendo assim, a inteligência artificial vai além do que a ficção científica retrata (COELHO, 2017).

3.1 Chatbot

O chatbot é um assistente virtual inteligente, e é um resultado de um avanço em diversas áreas da ciência ao longo dos anos, como o banco de dados, IA, processamento da linguagem natural e rede de comunicação de dados (CRUZ; ALENCAR; SCHMITZ, 2018).

A IA se dedicou a criar sistemas similares a seres humanos, e o processamento da linguagem natural tem como objetivo facilitar a interação do homem com a máquina, com a criação dos bancos de dados fizeram técnicas de armazenamento, as redes de comunicações com transferência de dados e os assistentes virtuais inteligentes foi realizado graças aos avanços dessas áreas (PANICALI, 2019).

Para desenvolver um chatbot é necessário que o mesmo tenha a capacidade de entender questões dos seres humanos, bem como, estabelecer a heurística, encontrar respostas e consultar os bancos de dados para poder gerar uma resposta para cada pergunta. O estudo da comunicação e da língua foram necessários para a evolução dos chatbots, devido a língua ser dinâmica e evoluir a todo tempo, e isso torna essencial a atualização contínua do vocabulário usado por essas tecnologias (CRUZ; ALENCAR; SCHMITZ, 2018).

Calado (2016) relata que existem dois tipos de chatbots:



- O primeiro com IA fundamentado em regras e possui capacidade de entender, aprender a linguagem natural;
- O segundo chatbot funciona através de regras, roteiros prontos ou mesmo palavras-chaves, sendo assim, se uma pessoa escreve algo diferente do que foi planejado, o chatbot não entende, e, portanto, não interpreta a interação. Os chatbots é diferente de assistentes virtuais, apesar de terem características similares, há diferença entre essas tecnologias.

Os chatbots realizam sua interação por chats, aplicativos de mensagens, e podem enviar links e arquivos de modo automático segundo a necessidade do usuário. E os assistentes virtuais usam a voz e textos para realizar o comando, e suas respostas é de acordo com as pesquisas na internet, pode ser em forma de vídeo, texto, imagem e etc. como por exemplo o Google Assistant (MUTANT, 2020).

3.2 Uso da inteligência artificial no ensino

Os gestores e professores da educação atuam como multiplicadores do conhecimento por meio das plataformas digitais como o YouTube, Google, Moodle, bases de dados online e livrarias eletrônicas, e podendo usá-los no ensino. Há muitos materiais como jogos, imagens, vídeos, animações e textos eletrônicos, que poderiam ser disponibilizados aos alunos. A todo momento são criados materiais didáticos, e os mesmos poderiam ser usados dentro da sala de aula. Mas, por diversos motivos, dentre eles a falta de políticas de formação continuada nem sempre acontece (PINTO; RIBEIRA; SILVEIRA, 2018).

A plataforma de ensino a distância com tecnologia é alimentada por base de dados e oferta a IA como ferramenta principal para a apresentação de aulas online e também para pesquisa, como por exemplo: Khan Academy é uma ONG que disponibiliza aulas virtuais para diversos temas (PREBIANCA *et al.*, 2013).

Idoeta (2017) descreve uma experiência que teve no Brasil no estado de São Paulo, no Centro Educacional SESI, em Arthur Alvim, esse centro disponibiliza aos seus estudantes uma plataforma virtual para eles realizarem variadas atividades, tendo acompanhamento e feedback online. Essa plataforma realiza a verificação da aprendizagem usando algoritmos próprios, indicando aos alunos outras aulas e modos de estudos, de acordo com as necessidades e dúvidas que cada um apresenta.

As plataformas educacionais são baseadas em IA, e possibilita que as organizações de ensino construam uma rede de tecnologia para capacitar e conectar alunos individuais, familiares, professores e outras escolas. Desta maneira, oferecem ao aluno uma base de dados extensa e interativa. Esse sistema é complexo, lógico e físico, e estar em constante construção e mudanças, para oferecer personalização na aprendizagem através da construção do perfil de cada aluno e assim, indicar temas para cada momento singular (SILVA, 2015).

Os programas de computadores que têm acesso às plataformas de dados viabilizam infinitas possibilidades de interações com dados hipertextualizados. E com isso, as

informações disponibilizadas a cada aluno são inter cruzadas com as bases de dados das plataformas, e isso traz melhores resultados, por meio de desenhos individuais baseados em aspectos técnicos, éticos, pedagógicos e psicológicos para uma boa aprendizagem personalizada (XAVIER, 2013).

Para que se tenha sucesso nesse tipo de aprendizagem, são primordiais o planejamento e a orientação continuada do docente (SILVA, 2015). Estes modelos de ensino, de acesso a informações digitais, podem colaborar com a atual educação do Brasil, pois no nosso país a educação nem sempre é satisfatória, não possui estrutura, qualidade satisfatória e currículo. E a aprendizagem personalizada possibilita sanar as principais dificuldades de cada aluno (PIAZZI, 2014; FAVA, 2018).

3.3 Aplicações da IA nos aplicativos de bancos

A IA vem mudando os modelos operacionais das organizações financeiras, de acordo com a pesquisa realizada pela PRICEWATERHOUSE (2019), os serviços bancários são o terceiro setor mais afetado pela IA. E esse setor se destaca pela rapidez nas mudanças e pela inserção de novas tecnologias. E umas das principais tecnologias introduzidas é a personalização do planejamento financeiro, feito por robôs-conselheiros, que possibilitam a criação de soluções customizadas de investimentos para os consumidores em massa.

O uso da IA permite que as companhias de serviços bancários mudam completamente suas formas de trabalharem, criando produtos e serviços inovadores, transformando a experiência do usuário. Sendo assim, as organizações financeiras vêm passando por grandes pressões de competitividade, pois a IA é um elemento que alavanca a produtividade, sendo um complemento ao fator de produção, tendo resultados que podem transformar todo serviço. Ao fazerem uso de máquinas que aprendem, se adaptam e melhoram seus resultados, podem trazer um grande valor ao negócio e ao cliente, possibilitando a diminuição dos custos (ACCENTURE, 2018).

As tecnologias cognitivas são uma nova maneira de atrair clientes, impulsionar a eficiência operacional e ganhar competitividade. Exigem habilidades específicas para manejar os novos modelos de negócios e de colaboração entre concorrentes. A IA permite que as organizações bancárias através de dados desenvolvam soluções para o uso de ferramentas disruptivas, para se obter uma assertividade maior, além de diminuir os prazos (DELOITTE, 2019; ACCENTURE, 2018).

As instituições financeiras vêm investindo bastante em tecnologia para melhorar o atendimento ao cliente e os processos operacionais e aumentar a segurança. A IA é um dos recursos bem atuais que está sendo usado pelos bancos. No Brasil, as maiores instituições financeiras estão fazendo o uso de duas formas de IA: o uso de inteligência artificial no atendimento a clientes com bots e assistentes virtuais, nas transações bancárias, em contact centers e em diversos canais (ESTADÃO, 2019).

A tecnologia também está sendo usada em áreas internas dos bancos, em setores de backoffice, ou seja, no setor de apoio operacional, nas operações das empresas, na leitura de contratos, no setor jurídico, nos recursos humanos e nos cadastramentos de contas

(FEBRABAN, 2019).

O Banco do Brasil, Bradesco, Banco Original, Santander e Banrisul são algumas instituições que fazem uso da tecnologia IBM Watson (plataforma de inteligência artificial da IBM) que é utilizada para atender os usuários em variados canais de atendimento ou mesmo em apoio (backoffice) (FEBRABAN, 2019).

No Brasil uma das iniciativas digitais mais conhecidas é a BIA (Bradesco Inteligência Artificial), que usa a plataforma Watson. O Bradesco, em 2016, foi a primeira empresa no país que realizou o treinamento desse sistema na língua portuguesa para realizar a interação em linguagem natural, para tirar dúvidas dos funcionários da agência bancária. No decorrer do tempo notou-se que o resultado foi melhor do que o estimado, e a assistente virtual foi ficando mais inteligente, permitindo a expansão do projeto aos clientes do banco, e na atualidade podem tirar suas dúvidas e fazer serviços sem a necessidade de ajuda (IBM, 2019).

Desde a implementação da BIA a interação entre funcionários e clientes já ultrapassou a marca de 125 milhões. Em poucos meses de treinamento, a BIA passou a entender 100% das perguntas em formato escrito e 83% das perguntas faladas. Essa assistente virtual tem a capacidade de responder cerca de 5 mil perguntas dentro de uma hora, estando relacionadas em média a 60 serviços (ESTADÃO, 2019).

A BIA apresenta uma taxa de assertividade de 95%, e apenas 5% das perguntas necessitam de uma assistência adicional. O banco Bradesco com o uso da Bia otimizou o atendimento de funcionários e clientes em mais de 5 mil agências, e em vários casos o tempo de resposta que antes levava cerca de 10 minutos passou para segundos (ELIFE, 2018).

Os bancos que mais fazem o uso da IA são os que estão preparados para repensarem suas estratégias e abordagens aos clientes, em suas metodologias e seus dados (ACCENTURE, 2018).

4. A TECNOLOGIA COMO ALIADA PARA A VIDA HUMANA

O fenômeno da globalização teve grande contribuição para a criação de laços econômicos, culturais, sociais etc., diminuindo relacionamentos que tempos atrás não existiam. A tecnologia de informação aliada ao crescente avanço das telecomunicações criou uma infraestrutura fundamental para o desenvolvimento de um novo conceito de globalização. E hoje a sociedade apresenta uma grande dependência das tecnologias como modo de sobrevivência da sociedade, e isso mostra que a sociedade atual é cada vez mais virtualizada (NICOLA; ESTIMA, 2018).

Os temas inovação tecnológica e tecnologia estão em alta nos meios de comunicação, nas agendas governamentais, agências que promovem as pesquisas, bem como, variadas organizações sociais, e tem forte influência no setor de saúde. Acredita-se que estamos vivendo uma época histórica de desenvolvimento tecnológico sem vínculos anteriores, fazendo com que a atual sociedade seja reconhecida como tempo do conhecimento e da tecnologia (MAIA, 2018).

É comum que as organizações, empresas e instituições façam uso da aprendizagem permanente, bem como produzam novos conhecimentos e tecnologias como foco de estratégias de sobrevivência e crescimento. As famílias enxergam na escolaridade de nível superior, no domínio de conhecimentos e tecnologias atuais como caminho para que seus filhos possam ter um futuro promissor (PEREIRA, 2019).

Hoje em dia é impensável viver sem alguns recursos e instrumentos como por exemplo: avião, automóvel, energia elétrica, telefone móvel, televisão, internet e computador. Da mesma forma, manter e garantir a saúde sem os antibióticos, próteses, anestésicos, vacinas, órteses, respiradores, marcapassos, exames radiológicos e transplantes são inconcebíveis (SOUZA *et al.*, 2018).

A IA tem diversas aplicações e englobam:

- **Sistemas Especialistas:** tem a necessidade de processar as informações não numéricas, e tem capacidade de apresentarem conclusões sobre variados assuntos. E tem como base o conhecimento e a projeção para emular a especialização do ser humano em algum tema específico. Esses sistemas são construídos com base em uma base de conhecimentos construídos de fatos, heurísticas e regras sobre o domínio, e tem capacidade de oferecer sugestões às pessoas que fazem uso dos mesmos (GONÇALVES, 2009).
- **Robótica:** robôs dotados de IA, possuem a capacidade de auxiliar os seres humanos em atividades de alta complexidade. Os avanços nos estudos na área de robótica são fenomenais, e tem o crescimento acelerado, e apresentam um futuro bem promissor, deixando em questão como os desenvolvedores vão lidar com as questões éticas (NICOLA, ESTIMA, 2018).
- **Processamento de Linguagem Natural:** possibilita o computador reconheça comandos de voz em uma linguagem natural, e pode ser utilizada para recuperar informações sem a necessidade de digitar os comandos ou buscar por palavras-chaves, como por exemplo, as corretoras de ações usam para reconhecimento de clientes (PEREIRA, 2019).
- **Ensino:** a área da educação é uma das áreas que mais se beneficiam com a melhoria da IA, pois, mudou a forma de interação entre aluno e professor, possibilitando a criação de um ambiente de disponibilidade 24 horas por dia, 7 dias da semana, possuindo uma rede de suporte para interação que antes eram realizadas somente em salas de aula (STEFANINI, 2018).
- **Agricultura:** a IA auxilia o agricultor, produtor ou engenheiro agrônomo, na tomada de decisão, mostrando o melhor momento para plantar ou colher, esses dados são mostrados através de projeções e gráficos, criados pela IA (MAIA, 2018; STEFANINI, 2018).
- **Saúde e Biotecnologia:** a IA nesse segmento auxilia os médicos e pacientes a terem um diagnóstico com mais rapidez, podendo aumentar as chances de cura de uma doença. Possibilita a criação de cadeiras de rodas controladas através de um olhar, ou mesmo por uma rede neural, sendo capaz de armazenar dezenas de

milhares de diagnósticos e processar os dados em velocidade que o ser humano não é capaz, viabiliza a criação de um novo tratamento, ou mesmo de um medicamento. Essa é uma das áreas que mais usa o conceito de *Machine Learning*, onde a máquina aprende as informações que médicos e pacientes compartilham (LOBO, 2017).

- Carros Autônomos: com a criação da conexão de internet 5G, onde os dados são trafegados em uma velocidade muito alta, os carros autônomos serão beneficiados. Com a chegada dessa tecnologia, possibilitará as conexões com as chamadas cidades inteligentes, e os carros poderão interpretar as placas de trânsito, semáforos, poderão trocar de pista em uma rodovia, sem a interferência de um humano. Já existem carros que realizam essas funções, mas com a chegada do 5G e diversas montadoras de carros inseridas nesse segmento, a possibilidade de sucesso é ainda maior (GUIMARÃES, 2019).
- Assistentes Pessoais: possuem capacidade de criar lembretes, reuniões, atividade de rotina, nessa área da IA tem a Siri da Apple que reconhece e interpreta o comando de voz. É uma tecnologia *Machine Learning*, ou seja, este tipo de software sofre atualizações corriqueiras, e tem como objetivo melhorar a experiência do usuário (STEFANINI, 2018).

4.1 Tecnologia na área da saúde

A ciência e a tecnologia favorecem uma compreensão mais precisa sobre os processos de saúde e doença, bem como, suas implicações sobre a vida humana. O uso delas é indispensável na trajetória do cuidado integral do paciente. Na atualidade, é necessário arranjos educacionais, procedimentos técnicos, sistemas, máquinas e equipamentos para garantir o acesso ao cuidado integral às pessoas que fazem uso do sistema de saúde, seja ele privado ou público (SOUZA *et al.*, 2012).

O uso de tecnologias na área da saúde vem crescendo e ganhando adesão em diversos centros e sistemas, e é uma ferramenta essencial para o diagnóstico e tratamento de doenças. As tecnologias em saúde são: equipamentos, medicamentos, procedimentos técnicos, sistemas de suporte, educacionais, organizacionais e protocolos assistenciais. O uso dessas tecnologias permite ações específicas e detalhadas no processo de diagnóstico, prevenção, tratamento e reabilitação de doenças (SANTOS; FROTA; MARTINS, 2016).

Os testes de avaliação de função pulmonar, avaliação de força de potência muscular, análise de marcha em 3 dimensões é um dos exemplos de aplicação da IA mais recente na medicina (BRIDI *et al.*, 2018).

4.2 Uso da inteligência artificial em vendas, compra e marketing

O entendimento de marketing, é dado como a execução de todas as ações de comércio que possuam serventia para dirigir o escoamento de produtos e serviços do produtor ao comprador. Também é compreendido como um conjunto de operações que abrange a vida da mercadoria, bem como, sua planificação de produção, até o instante que é adquirido pelo cliente (KOTLER; KARTAJAYA; SETIAWAN, 2017).

O marketing é a atividade, conjunto de organizações e métodos para criar, comunicar, entregar e trocar as ofertas que possuem valor para os consumidores, parceiros e população em geral. Com o avanço tecnológico crescente, as organizações são forçadas a organizar suas operações tradicionais, a melhorar seus processos, usar novos sistemas de informação para manter atualizados os sistemas já existentes. As tecnologias digitais têm grande potencial de impedir o comportamento do consumidor, as ferramentas de gerenciamento e a metodologia organizacional, e tem como o marketing a chave principal neste processo (MIKLOSIK; EVANS, 2020).

Quando há o lançamento de um produto novo no mercado, deve-se atender as necessidades e preferências dos clientes, para que sejam alcançados os resultados almejados. O marketing tem como função nos negócios, o planejamento, a promoção e a venda das mercadorias nos comércios existentes. A criação de novos produtos e novos comércios, para aumentar o público de consumidores, faz uso do marketing para melhorar esses aspectos, bem como, visa o atendimento de qualidade para suprir as necessidades dos clientes atuais e dos possíveis potenciais (ALMEIDA; SILVA; NOVÔA, 2019).

O conceito de marketing é fundamentado na satisfação dos desejos do usuário-consumidor/cliente, no qual engloba desde o planejamento, criação de produtos, estratégias de vendas e intervenções nos processos de produção. Portanto, o marketing gera iniciativas que envolvem pesquisas de mercado, campanha publicitária, promoção de venda e etc. (KOTLER; KARTAJAYA; SETIAWAN, 2017). E tem como objetivo final o aumento de lucros por meio da produção e oferta de produtos e serviços fundamentais para alcançar as demandas do usuário-consumidor/cliente (NEVES, 2018).

O marketing digital, marketing online ou marketing eletrônico (e-marketing) são as principais denominações desse fenômeno que abrangem as ações de divulgação e venda na internet, assim como, em outros canais digitais. O marketing abrange os marketings de conteúdo, de redes sociais, de busca e outros (PULIZZI, 2016).

É necessário que uma organização crie uma estratégia de marketing digital, tendo como alguns motivos: a) manter o relacionamento entre a marca do produto e o usuário-consumidor; b) facilitar a correção de erros; c) custo baixo em relação ao marketing tradicional; d) aumento da possibilidade de segmentação, ou seja, a maior assertividade quanto ao público-alvo; e) resultados reais (ALMEIDA; SILVA; NOVÔA, 2019).



5. CONSIDERAÇÕES FINAIS

A Inteligência artificial é um conjunto de ações que se fossem realizadas por uma pessoa, ele seria dado como inteligente. Samuel e Strachey mostraram que as primeiras instâncias de que um computador poderia ser utilizado para fazer uma atividade humana. Em 1955 Samuel melhorou seu jogo, permitindo o melhoramento do desempenho. Em 1990 foram desenvolvidas várias pesquisas sobre a IA em universidades e foram exploradas pelas empresas. As assistentes pessoais da Apple (Siri), da Amazon (Alexa), da Google (OK Google), da Microsoft (Cortana) e da Samsung (Bixby), são exemplos de treinamento de redes neurais. As principais áreas da IA são: Aprendizado de Máquina e as redes neurais.

As aplicações da IA são usadas para detectar fraudes em páginas da web e em dispositivos móveis, previsão de falhas em equipamentos, detecção de invasão de rede, reconhecimento de imagens etc. O chatbot é um assistente virtual inteligente que tem como objetivo facilitar a interação do homem com a máquina por meio do processamento da linguagem natural. Os gestores e professores da educação da atualidade fazem uso de plataformas digitais como o YouTube, Google, Moodle e outros, sendo utilizado no ensino. A IA é um dos recursos da atualidade usado pelos bancos, e a mais conhecida é a BIA (Bradesco Inteligência Artificial).

A tecnologia de informação aliada ao avanço das telecomunicações criou uma infraestrutura fundamental para o desenvolvimento de um novo conceito de globalização. E hoje a sociedade tem grande dependência das tecnologias como modo de sobrevivência da sociedade, e isso mostra que a sociedade atual está cada vez mais virtualizada. Essas tecnologias estão presentes nos: carros, aviões, energia elétrica, telefone móvel, televisão, internet e computador. Sistemas Especialistas; robótica; ensino; processamento de linguagem. A ciência e a tecnologia melhoram a compreensão mais precisa sobre os processos de saúde e doença, bem como, suas implicações sobre a vida humana.

O marketing digital, marketing online ou marketing eletrônico (e-marketing) abrangem as ações de divulgação e venda na internet, assim como, em outros canais digitais. Sendo assim, é de grande importância o estudo das inteligências artificiais, pois é a partir delas que será norteado muita das ações humanas e de atividades do cotidiano, e sua utilização pode facilitar e melhorar a realização de atividades que antes demandava mão de obra e bastante tempo, passou a ser feita em alguns clicks devido ao uso de IAS. Investimentos em pesquisas para o desenvolvimento de novas inteligências artificiais é crucial para a realização de estudos de novos algoritmos, e com isso pode beneficiar e melhorar o dia a dia do ser humano.

Referências

ACCENTURE. **Redefine banking with artificial intelligence**, 2018. Disponível em https://www.accenture.com/_acnmedia/pdf-68/accenture-redefine-banking.pdf. Acesso: 21 abril. 2022.

ALMEIDA, T. F. S. DE; SILVA, H. A. DA; NOVÔA, N. F. **Marketing Digital: novas possibilidades de ações estratégicas em agências especializadas**, 2019. Disponível em: <<https://www.aedb.br/seget/arquivos/artigos17/28525322.pdf>>. Acesso em: 26 abril. 2022.

BARNES, J. Microsoft Azure Essentials Azure Machine Learning. Redmond: Microsoft Press, 2015.

BRIDI, D. *et al.* Análise da marcha de crianças com paralisia cerebral com e sem uso de órteses de tornozelo e pé. **Sci. Med.**, v. 28, n. 2, 2018.

CALADO, C. **Afinal, o que é chatbot e como ele pode melhorar o atendimento nas empresas?** 23 de abril de 2016. Disponível em <<https://take.net/blog/chatbots/o-que-e-chatbot/>>. Acesso em 23 abril. 2022.

COELHO, L. **Machine Learning: o que é, conceito e definição.** Cetax.com, 2017. Disponível em: <https://www.cetax.com.br/blog/machine-learning/>. Acesso em: 13 abril. 2022.

CONTI, G; WIGGERS, K. L; RIBEIRO, S. R. A. "**Representação em Malhas 3D a partir de dados de textura do solo interpolados mediante Rede Neural Artificial: Estudo de caso FESCON - Ponta Grossa - PR**", Geo UERJ, n. 28, p. 410-429, Agosto de 2016, Rio de Janeiro/RJ, Brasil.

CRUZ, L. T; ALENCAR, A. J; SCHMITZ, E. A. **Assistentes Virtuais Inteligentes e Chatbots: Um guia prático e teórico sobre como criar experiências e recordações encantadoras para os clientes da sua empresa.** Rio de Janeiro, Brasil. BRASPORT Livros e Multimídia Ltda, 2018.

DELOITTE. **A nova física nos serviços financeiros - Inteligência artificial transforma o ecossistema das finanças.** São Paulo, 2019. Disponível em: <https://www2.deloitte.com/br/pt/pages/financial-services/articles/inteligencia-artificial-financas.html>. Acesso em: 12 abril. 2022.

EDDISON, L. **Deep Learning: A Technical Approach To Artificial Intelligence For Beginners**, 2017.

EFE, S. B; CEBECI, M. Power Flow Analysis by Artificial Neural Network. **International Journal of Energy and Power Engineering**, v. 2, n. 6, p. 204-208, 2013. doi: 10.11648/j.ijepe.20130206.11. Acesso em: 10 abril. 2022.

ELIFE. **O que podemos aprender com Bia, assistente virtual do Bradesco?** 2018. Disponível em: <https://elife.com.br/index.php/2018/08/16/o-que-podemos-aprender-com-bia-assistente-virtual-do-bradesco/>. Acesso em: 06 abril. 2022.

ESTADÃO. **Inteligência artificial começa a captar a intenção do cliente.** São Paulo, 2019. Disponível em: <https://publicacoes.estadao.com.br/financasmais2019/inteligencia-artificial-comeca-a-captar-a-intencao-do-cliente/>. Acesso em: 12 abril. 2022.

FACELI, K. *et al.* **Inteligência Artificial – Uma Abordagem de Aprendizado de Máquina.** 2. edição. GrupoGen, 2021. Disponível em: <https://www.grupogen.com.br/e-book-inteligencia-artificial-uma-abordagem-de-aprendizado-de-maquina>. Acesso em: 20 abril. 2022.

FAVA, R. **Trabalho Educação e Inteligência Artificial: a era do indivíduo versátil.** Porto Alegre: Editora Penso, 2018.

FEBRABAN. **Bancos miram parcerias e expansão para a inteligência artificial.** 2019. Disponível em: <https://portal.febraban.org.br/noticia/3356/pt-br/>. Acesso em: 12 abril. 2022.

FRANCO, C. R. **Inteligência Artificial.** Londrina: Editora e Distribuidora Educacional, 2014.

GONÇALVES, A. **Inteligência Artificial e Sistemas Especialistas**, 2009. Disponível em: <https://administradores.com.br/artigos/inteligencia-artificial-e-sistemas-especialistas>. Acesso em: 10 abril. 2022.

GUIMARÃES, C. **5G promete tornar carros autônomos mais inteligentes já em 2020**, 2019. Disponível em: <https://olhardigital.com.br/carros-e-tecnologia/noticia/5g-promete-tornar-carros-autonomos-mais-inteligentes-ja-em-2020/89680>. Acesso em: 4 abril. 2022.

IBM. **Com BIA, Bradesco e IBM transformam o atendimento de milhões de usuários.** São Paulo, 2019. Disponível em: <https://www.ibm.com/blogs/ibm-comunica/com-bia-bradesco-e-ibm-transformam-o-atendimento-de-milhoes-de-usuarios/>. Acesso em: 12 abril. 2022.

IDOETA, P. A. **Como a Inteligência Artificial já está mudando salas de aula no Brasil e no mundo.** BBC Brasil, São Paulo, 25 de agosto de 2017. Disponível em: http://www.planalto.gov.br/ccivil%20_03/_Ato2015-2018/2017/Decreto/D9057.htm. Acesso em: 11 abr. 2022.

IMEN, L. *et al.* "Optimal Power Flow Study Using Conventional and Neural Networks Methods", **4th interna-**



tional conference on renewable energy research and applications, Palermo, Italy, 2015. Disponível em: https://www.researchgate.net/publication/251990627_Transaction_based_power_flow_solution_and_transmission_loss_allocation_using_neural_network. Acesso em: 10 maio 2022.

KASHYAP, P. **Machine Learning for Decision Makers**. Bangalore: Apress. 2017.

KELLY, K. **Inevitável: As 12 Forças Tecnológicas que Mudarão o Nosso Mundo**. São Paulo: HSM, 2017.

KELNAR, D. **The fourth industrial revolution: a primer on Artificial Intelligence (AI)**. Medium, [S. l.], 02 dez. 2016. Disponível em: <https://medium.com/mmc-writes/the-fourth-industrial-revolution-a-primer-on-artificial-intelligence-ai-ff5e7fffcae1>. Acesso em: 12 mar. 2022.

KHAIDEM, R. **The future of drones in Artificial Intelligence**. DZone, [S. l.], 03 jan. 2018. Disponível em: <https://dzone.com/articles/the-future-of-drones-in-artificial-intelligence>. Acesso em: 13 mar. 2022.

KOTLER, P; KARTAJAYA, H; SETIAWAN, I. **Marketing 4.0: Moving from traditional to digital**. New Jersey: Ed Wiley, 2017.

LEÇA, I. **Inteligência Artificial em ação – seis aplicações da IA**. SAP News Center. São Paulo, jan. 2017. Disponível em: <https://news.sap.com/brazil/2017/01/18/>. Acesso em: 28 mar. 2022.

LIMA, I; PINHEIRO, C. A. M; SANTOS, F. A. O. **Inteligência Artificial**. Rio de Janeiro: Campus, 2014.

LOBO, L. C. Inteligência Artificial e Medicina. In: **Revista Brasileira de Educação Médica**. Rio de Janeiro, 2017. v. 41 n. 2 p. 185-193. Disponível em: http://scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022017000200185&lng=en&nrm=is. Acesso em: 6 abril. 2022.

MAIA, F. **Big data e inteligência artificial no setor automobilístico é um caminho sem volta**, 2018. Disponível em: <https://epocanegocios.globo.com/Web-Summit/noticia/2018/11/big-data-e-inteligencia-artificial-no-setor-automobilistico-sao-caminho-sem-volta.html>. Acesso em: 4 maio. 2022.

MCCORDUCK, P. **Machines Who Think**. Boston: A. K. Peters Ltd., 2004.

MEHTA, R. **Big Data Analytics with Java**. Birmingham: Packt Publishing Ltd, 2017.

MIKLOSİK, A; EVANS, N. Impact of Big Data and Machine Learning on Digital Transformation In Marketing: A Literature Review. **IEEE ACCESS**, V. 8, 2020. DOI: 10.1109/ACCESS.2020.2998754. Acesso em 11 abril. 2022.

MILOJKOVIÜ, J; LITOVSKI, I; LITOVSKI, V; "ANN Application for the Next Day Peak Electricity Load Prediction", **11th Symposium on Neural Network Applications in Electrical Engineering**, September 2012, Belgrade, Serbia.

MUTANT. **Você sabe qual a diferença entre chatbot e assistente virtual?** Disponível em: <<https://mutantbr.com/blog/diferenca-entre-chatbot-e-assistente-virtual/>>. Acesso em 11 abril. 2022.

NEVES, B. C. Aproximação conceitual e possibilidades do marketing digital: o bibliotecário estrategista em mídias sociais. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, v. 13, n. 1, 2018. DOI: 10.22478/ufpb.1981-0695.2018v13n1.39354. Acesso em: 17 abril. 2022.

NICOLA, V. G. O. M; ESTIMA, V. R. C. **Inteligência Artificial em Robôs Humanoides**. 2018. Disponível em: <http://www.each.usp.br/petsi/jornal/?p=2471>. Acesso em: 3 abril. 2022.

PANICALI, A. P. **Análise de dados para evolução de chatbots**. 18 de abril de 2019. Disponível em: <<https://take.net/blog/chatbots/analise-de-dados-para-evolucao-de-chatbots>>. Acesso em 25 mar. 2022.

PEREIRA, S. L. **Introdução à Inteligência Artificial**. São Paulo, 2019. Disponível em: <https://www.ime.usp.br/~slago/IA-introducaDo.pdf>. Acesso em: 08 abril. 2022.

PINTO, E. M; RIBEIRO, G. R; SILVEIRA, A. C. J. DA. **Inteligência artificial na educação profissional técnica de nível médio: desafios da prática docente em escola pública**. In: COSTA, Maria Adélia da (org.) Educação Profissional. Goiânia: Espaço Acadêmico, 2018.

PRADO, E; HISATUGU, W. **Aplicações de Deep Learning em Medicina no Mundo - 1ª parte**. Convergência Digital, 2016. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&inoid=42511&sid=15>. Acesso em: 13 abril. 222.

PREBIANCA, G. V. V. *et al.* O uso de softwares educacionais como ferramentas mediacionais e de inclusão tecnológica. **ETD: Educação Temática Digital** 15.3, p. 474-494, 2013. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/etd/article/view/1267>. Acesso em: 10 de abril. 2022.

PRICEWATERHOUSE (PWC). **O real valor da IA para seu negócio**. São Paulo, 2019. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2019/real-valor-ia-seu-negocio.html>. Acesso em: 22 abril. 2022.

PULIZZI, J. **Marketing de conteúdo épico**. São Paulo, DVS, 2016.

RAHMAN, M. N; ESMAILPOUR, A; ZHAO, J; **“Machine Learning with Big Data An Efficient Electricity Generation Forecasting System”**, Elsevier: Big Data Research - Volume 5, September 2016.

ROSA, J. L. G. **Fundamentos da Inteligência Artificial**. Rio de Janeiro: LTC, 2011.

RUSSELL, S; NORVIG, P. **Inteligência Artificial**. Rio de Janeiro: Campus, 2013.

SANTOS, Z. M. S. A; FROTA, M. A; MARTINS, A. B. T. **Tecnologias em saúde: da abordagem teórica a construção e aplicação no cenário do cuidado**. EduEc., 2016. Disponível em: . Acesso em: 15 de abril. 2022.

STEFANINI. **As 7 principais aplicações de inteligência artificial nas empresas**, 2018. Disponível em: <https://stefanini.com/pt-br/trends/artigos/as-7-principais-aplicacoes-de-inteligencia-artificial-nas-empres>. Acesso em: 5 abril. 2022.

SILVA, R. S. **Ambientes Virtuais e Multiplataformas Online na EAD**. Editora Novatec, 2015.

SOUZA, M. C. *et al.* Necessidades de saúde e produção do cuidado em uma unidade de saúde em um município do nordeste, Brasil. **O mundo da saúde**, v. 38, n. 2, p.139-148, 2014. Disponível em: https://bvsm.s.saude.gov.br/bvs/artigos/mundo_saude/necessidades_saude_producao_cuidado_unidade.pdf. Acesso em: 10 de abril. 2022.

SOUZA, C. G. *et al.* Ponto Ótimo Cardiorrespiratório em Futebolistas Profissionais: Uma Nova Variável Submáxima do Exercício. **Int. J. Cardiovasc Sci.**, v. 31, n. 4, p. 323-332, 2018. Disponível em: <https://www.scielo.br/j/ijcs/a/WpZpsMjhV3rgNm9Nzf4rfVw/?format=pdf&lang=pt>. Acesso em: 18 de abril. 2022.

XAVIER, A. C. **Educação tecnológica e inovação: desafio da aprendizagem hipertextualizada na escola contemporânea**. Revista (Con) Textos Linguísticos. Espírito Santo: UFES, vol. 7, nº 8.1, 2013. Disponível em: <http://periodicos.ufes.br/>. Acesso em: 21 abr. 2022.

CAPÍTULO 13

SEGURANÇA DE DADOS

DATA SECURITY

Nara Virginia Marinho Arraes¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

Com a evolução da tecnologia e crescimento do público ao acesso, passou-se a ter preocupação em relação a segurança de dados que as instituições recebem de clientes, é essencial que as empresas que contém dados de clientes, possuam integridade em manipular as informações do modo que foi passado. E assim, manter a confidencialidade das informações caso haja necessidade de ter acesso a tais informações futuramente. É fundamental que as empresas passem segurança que os dados estarão protegidos, para atrair mais público e melhorar o crescimento da empresa. O objetivo principal dessa pesquisa bibliográfica foi analisar itens indispensáveis para realizar uma boa segurança das informações. E teve como objetivos específicos: descrever os principais pilares do sistema de informações; definir Sistema de Backup para ter uma cópia dos dados e mencionar as principais ferramentas utilizadas pelas empresas para ter proteção adicional das informações. Como metodologia foi utilizada a revisão bibliográfica de caráter descritivo e explicativo, a pesquisa foi realizada nas bases de dados da Biblioteca Virtual Kroton e Google Acadêmico. A pesquisa utilizou artigos publicados entre 2012 e 2022, nos idiomas português e inglês. Os principais pilares do sistema de informações são: ativo de informação, vulnerabilidade, ataque, incidente de segurança, probabilidade e impacto. Os principais sistemas de backup utilizado pelas empresas são: EMC Networker e o Big Data. As principais ferramentas utilizadas pelas empresas para ter proteção adicional das informações são os algoritmos; a criptografia, bem como, a assinatura digital e as redes privadas virtuais.

Palavras-chave: Segurança de dados, Sistema de informação, Banco de dados.

Abstract

With the evolution of technology and the growth of the public to access, there has been concern about the security of data that institutions receive from customers, it is essential that companies that contain customer data have integrity in handling the information in the right way. that was passed. And thus, maintain the confidentiality of the information in case there is a need to have access to such information in the future. It is essential that companies pass security that the data will be protected, to attract more public and improve the company's growth. The main objective of this bibliographic research was to analyze essential items to perform a good information security. And it had as specific objectives: to describe the main pillars of the information system; define Backup System to have a copy of the data and mention the main tools used by companies to have additional protection of information. As a methodology, a descriptive and explanatory bibliographic review was used, the research was carried out in the databases of the Kroton Virtual Library and Google Scholar. The research used articles published between 2012 and 2022, in Portuguese and English. The main pillars of the information system are: information asset, vulnerability, attack, security incident, probability and impact. The main backup systems used by companies are: EMC Networker and Big Data. The main tools used by companies to have additional protection of information are algorithms; encryption, as well as digital signatures and virtual private networks.

Keywords: Data security, Information system, Database.



1. INTRODUÇÃO

A grande evolução da tecnologia e crescimento do público ao acesso, fez com que houvesse o crescimento com a preocupação sobre a questão da segurança de dados que empresas recebem de clientes. A maior parte do que fazemos hoje na internet pede nossos dados, seja em uma inscrição, compras, transações bancárias entre outros. Fazendo com que nossos dados fiquem em bancos de grandes empresas.

É de grande importância que as empresas que contém dados de pessoas, tenham a integridade em manipular essas informações como foi passado. E com isso, a certeza da confidencialidade, que para ter acesso à tais informações apenas pessoas ou entidades que são autorizadas e confiáveis para caso precise em uso futuro. Com isso, grandes e pequenas empresas estão com foco maior em ter uma boa estrutura e recursos para que possa ter uma equipe especializada trabalhe em manter uma boa segurança de tais informações. Passar a segurança de que os dados estão protegidos é de grande importância, para poder atrair mais público e conseqüentemente o crescimento da empresa.

E com esse crescente em necessidade de segurança a esses dados que vivemos mundialmente, iremos abordar ao longo de nosso trabalho como empresas se comportam e controlam essas informações que cada dia mais chegam novas. Diante disso, pergunta-se: como empresas se organizam para realizar a proteção do banco de dados?

O que foi apresentado neste trabalho, é segurança de informação ou banco de dados, que vem em uma crescente necessidade com o aumento das tecnologias e do público mundial. Fazendo assim que grandes empresas hoje investem fortemente em uma boa área de T.I, para conseguir manter tais informações em uma base, pois é de grande importância que a informação seja protegida para evitar roubo, vazamentos, perda ou sequestros. E assim, passando segurança e confiabilidade aos seus clientes. Desta forma, é importante entender e estudar ferramentas necessárias para ter uma boa estrutura de segurança, pois, informações são uma grande riqueza para uma grande empresa.

O objetivo principal dessa pesquisa bibliográfica foi analisar itens indispensáveis para realizar uma boa segurança das informações. E teve como objetivos específicos: descrever os principais pilares do sistema de informações; definir Sistema de Backup para ter uma cópia dos dados e mencionar principais ferramentas utilizadas pelas empresas para ter proteção adicional das informações.

Como metodologia foi utilizada a revisão bibliográfica de caráter descritivo e explicativo, a pesquisa foi realizada nas bases de dados Biblioteca Virtual Kroton e Google Acadêmico. A pesquisa considerou artigos publicados entre 2012 e 2022, nos idiomas português e inglês, foram utilizados como descritores: segurança de dados, sistema de informação e banco de dados. Foram selecionados os artigos após a leitura e análise dos materiais, e assim foi constituído o corpo da pesquisa. Os dados foram selecionados de acordo com o tema do estudo.

2. PRINCIPAIS PILARES DO SISTEMA DE INFORMAÇÕES

A informação é um instrumento fundamental para toda organização, seja qual for o porte ou segmento de atuação. Os processos organizacionais funcionam com a informação, e a geração de conhecimento decorre a partir do compartilhamento das informações. Os gestores usam a informação para tomar decisões para que haja alcance de seus objetivos e melhora do seu desempenho no mercado. Portanto, a informação é importante para a criação de estratégias, e com isso, impulsiona a utilização de Tecnologia da Informação (TI) nos métodos organizacionais para se ter uma proteção satisfatória (GALEGALE; FONTES; GALEGALE, 2017).

A informação na atualidade é um dos maiores e mais importantes patrimônios que uma empresa pode ter. Hoje em dia pode-se notar que empresas possuem em quase sua totalidade o núcleo de negócio (core business), tendo poucos ativos tangíveis, no qual pode valer bilhões de dólares. Um grande exemplo é o Google, uma empresa de software para internet dos Estados Unidos da América, sendo umas das maiores empresas globais (CABRAL; CAPRINO, 2015).

Tempos atrás as informações das empresas eram disponíveis em papéis, e a análise das informações tinham que ser feitas de modo manual. Com o crescimento das empresas, e com o desenvolvimento de variadas atividades complexas, foi necessário automatizar diversos processos e atividade para facilitar a gestão e tomada de decisões, e isso só foi possível com a disseminação dos computadores nos meados de 1980, permitindo que as empresas pudessem armazenar e analisar as informações através de planilhas eletrônicas, sendo utilizadas até os dias atuais, como único meio de armazenamento e análise de dados de várias micro e pequenas empresas (FONTES, 2012).

Um dos maiores bens de uma empresa é a informação, ela permite a evolução da tecnologia e na disponibilidade dessas informações em variados locais. Isso mostra a capacidade que o ser humano tem em criar coisas fantásticas. A informação permite a comunicação em tempo real independentemente da localidade, assim como, o armazenamento de dados na internet podendo ser acessado em qualquer momento e lugar, dentre outros (ABNT, 2006).

A segurança da informação (SI) é essencial para a proteção, preservação, confidencialidade, disponibilidade, integridade e autenticidade da informação, e evita as vulnerabilidades dos ativos relacionados a ela, sejam averiguados por ameaças, podendo causar perdas nos negócios da organização. Tais informações não estão restritas a sistemas de computação, nem a formato de informação eletrônica (KIM; SOLOMON, 2014).

De uma forma simples e direta, a Informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto.

A cultura de uma organização segue a segurança da informação, e tem como objetivos três pontos de vistas: (I) técnico, com destaque no emprego de controles tecnológicos como parâmetro de proteção da informação; (II) social, com ênfase na motivação de pessoas e no proceder geral para solução de adversidades de segurança e (III) sociotécnico, que visa a análise dos benefícios e na diminuição das desvantagens dos dois pontos de



vistas anteriores de modo concomitante (SIPONEN, 2001).

Os problemas relacionados à segurança de informação são abordados em variadas dimensões e por inúmeras iniciativas, seja na literatura tanto quanto nas organizações. Para Almeida, Souza e Cardoso (2010, p.156), as dimensões dos negócios podem ser vista “a partir da necessidade de implementá-la, em geral não há clareza sobre o que deve ser protegido e sobre como fazê-lo”, e para o norteio do trabalho dos gestores responsáveis por projetos de segurança, há apoio ao uso de uma ontologia para classificar a informação no ambiente organizacional com finalidade de proteção.

A Informação tem a definição de um conjunto de dados tratados e organizados de tal modo para que se tenham algum significado ou sentido dentro de um contexto.

A norma ISO/IEC 27002 descreve sobre os atributos básicos da informação, chamado de princípios básicos da segurança da informação por vários autores, também conhecidos como os conceitos dos destes três principais pilares da informação são:

- Confidencialidade: “Garantia de que o acesso à informação é restrito aos seus usuários legítimos.” (BEAL, 2008, p. 1). Ou seja, seu acesso é permitido apenas a determinados usuários.
- Integridade: “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais” (SÊMOLA, 2003, p. 45). Ou seja, informação não adulterada.
- Disponibilidade: “Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna” (BEAL, 2008, p. 1), ou seja, independente da finalidade, a informação deve estar sempre disponível.

Além destes, segundo Lyra (2008, p.4), podemos citar mais alguns aspectos complementares para garantia da segurança da informação:

- Autenticação: “Garantir que um usuário é de fato quem alega ser”. • Não repúdio: “Capacidade do sistema de provar que um usuário executa uma determinada ação” (LYRA, 2008, p.4):
- Legalidade: “Garantir que o sistema esteja aderente à legislação”.
- Privacidade: “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.
- Auditoria: “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.

2.1 Ativo de Informação

De acordo com a ISO/IEC 27001:2005, um ativo é “qualquer coisa que tenha valor para organização”. Sendo assim, pode existir vários tipos de ativos como informações sendo elas: acordos e contratos, bases de dados, documentações de sistema, manuais de usuário, planos de continuidade, trilhas de auditoria e etc., bem como, pessoas e suas qualificações, ativos de software (aplicativos, ferramentas, sistemas e etc.) serviços (eletricidade, refrigeração, iluminação e outros), e os que são intangíveis como por exemplo: a reputação da empresa (ABNT NBR ISO/IEC 27002:2005).

Um dos principais fatores que garantem a segurança da informação é a identificação correta, controle e atualização recorrente dos diversos ativos. E isso tem como objetivo gerar uma proteção correta, desta forma, é fundamental conhecer a Gestão de Ativos (HUANG; RAU; SALVENDY, 2010).

É princípio básico reconhecer todo ativo e que seja documentado pela organização, e deve ser estabelecido um responsável que irá lidar com a manutenção dos controles. Os controles podem ser delegados a outros profissionais, mas, a responsabilidade deve ser sempre vistoriada pelo proprietário (NETO; SILVEIRA, 2007).

Deve ser feita a correta classificação dos ativos, com base na criticidade, importância, sensibilidade e seu valor para a organização. E assim, poderá ser definido os níveis de proteção (ABNT NBR ISO/IEC 27002: 2005).

De acordo com Beal (2008, p. 63), a classificação dos ativos “ocorre de acordo com o valor e o grau de sensibilidade atribuído pela organização”. Portanto, os ativos com alta sensibilidade, alto impacto no negócio ou mesmo no processo, necessitam de um investimento alto. Deve ser feita uma classificação criteriosa dos ativos, pois, tem relação direta com o custo que será necessário para proteger esses ativos, e assim, definir o que tem necessidade de proteção ou não.

Desta maneira, nem todo ativo deve ser protegido, e a classificação eficiente permite considerar as necessidades do negócio, e deve ser feita por alguém que tenha o conhecimento elevado sobre a organização do negócio (ALMEIDA; SOUZA; CARDOSO, 2010).

2.1.1 Vulnerabilidade

A vulnerabilidade tem ligação direta ao ponto fraco de um ativo, sendo entendida como uma fragilidade. É um erro no procedimento (sistemas), falha de um trabalhador, ou configuração errada dos aplicativos de segurança, seja ela proposital ou não, acarretando no processamento de informações não confiáveis. E quando ocorre esse erro, há o descumprimento de um ou de vários princípios da segurança da informação (ALEXANDRIA, 2009).



2.1.2 Ataque

De acordo com Beal (2008, p.14), um ataque é um “evento decorrente da exploração de uma vulnerabilidade por uma ameaça”, ou seja, um ataque é a concretização de uma ameaça. Os ataques podem ter diversos objetivos que infringem os princípios da segurança, como por exemplo: uma invasão a uma rede corporativa por um hacker impedindo o uso da mesma.

Um ataque inflige o princípio de disponibilidade, pois, a informação que poderá ser solicitada pelo usuário não poderá ser acessada. Os ataques podem ser classificados como passivos (aqueles que não prejudicam no conteúdo do recurso que foi atacado) como por exemplo: observação e conhecimento de informações armazenadas nos sistemas institucionais ou análise de tráfego de uma rede, e ativos (prejudicam de forma direta o conteúdo atacado, modificando e eliminando informações ou mesmo pode criar informações falsas) (ALEXANDRIA, 2009).

2.1.3 Incidente de Segurança

A ISSO/IEC TR 180044:2004 expõe que um incidente tem como entendimento “um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação”. Ou seja, eventos de segurança indesejados que possam infligir os principais pilares da segurança de informação.

Os incidentes de segurança podem ser a perda da integridade de dados, desastres advindos por fenômenos da natureza como: incêndios, alagamentos, terremotos e etc., divulgação de dados inadequados, bem como, queda de energia, invasões por hackers, greves trabalhistas, defeitos em equipamentos dentre outros (FERNANDES; ABREU, 2014).

Uma gestão ineficiente dos incidentes de segurança da informação pode acarretar em danos sérios para os negócios. Sendo assim, um incidente pode ou não impactar nos negócios da empresa, e isso ocorre em consequência da que isto causa ao ativo da organização. Portanto, um ativo de valor alto gera um alto impacto e vice-versa (KIM; SOLOMON, 2014).

2.1.4 Probabilidade e Impacto

A probabilidade é a chance de uma falha de segurança ocorrer, ao se observar o grau de vulnerabilidade é encontrado os ativos e ameaças que possam influenciá-lo (LYRA, 2008). Probabilidade, vulnerabilidade e ameaças tem ligação direta, ou seja, a probabilidade se refere às “chances” de uma vulnerabilidade ser uma ameaça (FONTES, 2015).

É possível que um ativo tenha diversas vulnerabilidades que não possuam ameaças,

ou seja, probabilidade próxima de zero. Mas, é possível que esse conjunto de vulnerabilidades se tornem ameaças. O impacto é diferente da probabilidade, e ocorre após o incidente (NETO; SILVEIRA, 2007).

Um incidente de segurança pode causar ou não um impacto nas metodologias dos negócios da empresa. De acordo com Beal (2008, p.14) seria um “efeito ou consequência de um ataque ou incidente para a organização.”

3. SISTEMAS DE BACKUP

Leal (2019) descreve que a segurança da informação é vital para as empresas. A segurança da informação tem como finalidade fazer a proteção e gerir a informação. Fontes (2012, p.6) define que, “A informação é um recurso essencial para toda e qualquer organização, independentemente do seu porte e segmento de atuação no mercado”. Portanto, se faz necessário para todas as empresas, pois, auxilia na tomada de decisões, planejamento e crescimento, devido a necessidade de guardar muitas informações.

De acordo com Castilhos (2013, p.55) “a segurança da informação é obtida a partir da implementação de um conjunto de políticas, processos e procedimentos e estruturas”. Para se dar continuidade a uma empresa, e para sua sobrevivência, é fundamental guardar muito bem suas informações. Uma segurança de informação eficaz, só terá êxito se for associado a um conjunto de controles adequados, como por exemplo: a política de segurança de informações só terá êxito se for fiscalizado.

Segundo Cardoso Neto *et al.* (2012, p.2) o backup pode ter como definição: “cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados.” A rotina de backup é percebida como algo chato para muitas pessoas. E devido a isso vários gestores de sistemas vem trabalhando para simplificar a automatizar a tarefa de realização de backup, para diminuir o tempo que se leva para realizar esse procedimento.

Segundo com Jesus e Schimiguel (2018, p.23) “para backup de pequeno e médio porte a solução de backup em nuvem apresenta grandes vantagens, devido ao fato de seu tamanho ser pequeno. Além da vantagem de utilização do backup em nuvem, que permite a inexistência de um local para armazenamento, e a escalabilidade, aumentando gradualmente o tamanho do backup de acordo com a necessidade, não requer um custo inicial”.

O Recovery Time Objective (RTO) é definido como a quantidade máxima de tempo que um processo de negócios fundamentados em TI pode estar indisponível anterior ao início de eventos adversos inaceitáveis para uma empresa, ou seja, perdas financeiras, reputação, lesão na satisfação do cliente e outros. Recovery Point Objective (RPO) tem como definição a quantidade máxima de dados que se pode perder, sem causar danos que prejudiquem a empresa (PING *et al.*, 2010).

Tempo de tensão, é o período de tempo em que os dados têm que permanecer antes da exclusão ou em caso de troca de armazenamento que venha a ser arquivado. E a jane-

la de backup é o tempo necessário para realizar um procedimento de backup, sem danos da aplicação (ISMAIL *et al.*, 2013).

O full backup ou backup incremental é o procedimento da cópia de dados de uma área em um determinado tempo. E tem duas desvantagens:

- A leitura e escrita total do sistema de arquivos é muito demorado;
- E o armazenamento de cópia do sistema de arquivos ocupa uma boa parte da capacidade de mídia de backup (CHEVERNAK *et al.*, 1998).

O backup incremental faz a cópia de dados que foram adicionados após o último backup, e esse procedimento é mais rápido e os arquivos são menores. E tem como vantagem a redução do tamanho dos backups, pois, os arquivos possuem poucas mudanças em um determinado tempo (CHEVERNAK *et al.*, 1998).

No backup diferencial ou acumulativo guarda apenas dados que sofreram alterações desde a realização do último backup total. Esse processo de recuperação de dados se dá restaurando as informações do último backup total e logo após a restauração do backup diferencial é indicado ser feito (CHEVANANCE, 2004).

Synthetic backup ou backup sintético, tem como objetivo reduzir o impacto no tráfego de dados na rede do cliente no período que é feito o backup. Esse processo é composto pelo backup full e pelos incrementais subsequentes que estavam em fita ou em disco. E tem como classificação: o backup pode ser classificado com relação ao estado da aplicação: hot (quente) e cold (frio) (VERAS, 2010).

A aplicação do processo de cold backup (off-line backup) é inativa, e no hot backup (online backup) quando esse processo é aplicado a sua execução é em conjunto com o acesso dos usuários em tempo real aos dados (MCDOWALL, 2011). No hot backup a disponibilidade do serviço não passa por comprometimento, mas, diminui a qualidade do desempenho (VERAS, 2010).

Um backup pode ser feito por arquivo, aplicação ou imagem (ou bloco). O backup por arquivo guarda os arquivos e diretórios, e possibilita recuperar arquivos individuais. E o backup de aplicação permitindo a recuperação de arquivos individualmente. O backup por Imagem é realizado por backup bloco, por bloco do conteúdo do disco, e sua recuperação é mais rápido em caso de catástrofes (VERAS, 2010).

3.1 EMC Networker

O EMC Networker é um software que faz operações de backup/recuperação de dados em fitas e discos, deduplicação em ambientes físicos e virtuais e replicação contínua (DUBOIS; AMATRUDA, 2010). Esse software é composto no mínimo por cinco componentes: NetWorker Client, NetWorker Storage Node, NetWorker Server, NetWorker Management Console e NetWorker License Manager (EMC CORPORATION, 2007).

Os NetWorker Clients ou clientes de backup tem sua alimentação com dados ou aplicações, sua função é recolher dados a serem salvos, e depois os dados serão enviados ao NetWorker Storage Node, ou seja, para o servidor de armazenamento e com isso, recuperar os dados ao longo do processo de recuperação.

O NetWorker Storage Node tem como função organizar os dados advindos dos clientes de backup e fazer a gravação no dispositivo de backup.

O NetWorker Server ou servidor de backup tem como função direcionar e apoiar os clientes de backup e realizar as operações de recuperação de dados. Desta maneira, o servidor de backup recebe os metadados de backup dos usuários e dos nós de armazenamento, alocando-os no catálogo de backup.

O NetWorker garante alto desempenho e escalabilidade. E disponibiliza uma plataforma com vasto suporte de opções para proteção de dados, bem como, backup em disco, replicação contínua, e deduplicação em ambientes físicos e virtuais (DUBOIS; AMATRUDA, 2010).

Os Storage Nodes têm funcionalidade de servidores secundários de backup, e compartilhar a carga de trabalho, sua configuração em rede SAN, alivia o fluxo através da LAN.

O Backup to disk, permite que o backup seja feito em disco, e tem como vantagens o aumento do desempenho, e possui ferramentas de clonagem de disco para fita com mais rapidez.

Backup to tape é um suporte diversos tipos de fitas, unidades e bibliotecas, e faz uso da ferramenta OTF (Open Tape Format) que possibilita que os dados heterogêneos fiquem na mesma fita, permitindo a portabilidade entre variadas plataformas de fitas. Snapshot backup, é um suporte usado para a tecnologia de replicação com base em array e em softwares de criação e uso de snapshots.

O Block-based backup, possibilita a realização de backup e recuperação de dados a nível de bloco, usando um módulo adicionável, o SnapImage e o NDMP-based backup é um suporte ao protocolo NDMP (Network Data Management Protocol).

Deduplication com EMC Avamar, é usado em conjunto com o Avamar, e realiza a deduplicação na origem dos dados, decrescendo a carga do tráfego pela rede LAN. E a Interface NetWorker Management Console tem cinco botões: Events, Enterprise, Libraries, Reports e Setup (EMC CORPORATION, 2007).

Os botões abrem novas janelas na Interface NetWorker Management Console. A janela Events fornece dados a respeito dos eventos gerenciados. E a janela Enterprise permite selecionar um servidor NetWorker para gerenciar, e monitorar o servidor e seus usuários de backup. Já a janela Enterprise viabiliza abrir a janela Administration e dá acesso ao servidor NetWorker (DE CAMPOS *et al.*, 2012).

3.2 Big Data

O Big Data é muito usado para o tratamento, manipulação e comunicação de dados pessoais. O Big Data viabiliza a junção de diversas fontes de informação, por meio de correlações sistemáticas feitas, e gera uma nova informação (MANYIKA *et al.*, 2011). Desse modo, o Big Data permite a análise, tratamento, manipulação e comunicação de dados pessoais em massa (DUMBILL, 2012; BOYD; CRAWFORD, 2012).

Os dados tem origem da Web e das redes sociais (dados de fluxo de posts, feeds de noticiais, de cliques e blogs), dados de biometria (DNA, impressões digitais, identificação automática e reconhecimento facial), dados de transações (registros de ligações, de reclamações nas empresas e compra de cartão de crédito), dados que foram gerados por pessoas como documentos eletrônicos, ligações telefônicas, exames e registros médicos, e os dados machine to machine que são gerados por máquinas, dispositivos de GPS, sensores (INTEL, 2015; ADREJEVIC; GATES, 2014).

Os cinco VS são: volume, ou seja, a quantia de dados acumulados; variedade é os meios de propagação e tipos de dados em uso; a velocidade, ou seja, é a taxa de transmissão de dos dados; a veracidade possibilita definir se os dados são confiáveis; e o valor que é o resultado obtido ao utilizar as ferramentas de Big Data e tem como objetivo manter em os sistemas e as plataformas em harmonia, viabilizando o resultado que se é esperado (VEJA, 2013; PANOPTYKON FOUNDATION, 2015).

Os dados são classificados em três categorias: dados estruturados, no qual eles pertence a um SGBD relacional associado a um esquema relacional, dados semiestruturados, que são irregulares ou incompletos e varia segundo um esquema, compreensíveis por máquinas porém não por pessoas, como por exemplo: documentos HTML e logs de web sites, e os dados não estruturados, ou seja, não possui estrutura nem viabiliza agrupar vídeos, tabelas, imagens e e-mails (INTEL, 2015).

4. FERRAMENTAS UTILIZADAS PELAS EMPRESAS PARA TER PROTEÇÃO ADICIONAL DAS INFORMAÇÕES

4.1 Algoritmo

O algoritmo é definido como um conjunto previsto de regras ou instruções bem definidas para a solução de um problema, como o desempenho de um cálculo, em um número finito de etapas'. Desta maneira, pode-se afirmar que para que o processamento possa ser realizado pelos algoritmos, tais devem receber instruções necessárias de modo detalhado para realizar o processamento (BURTTERFIELD; NGONDI, 2016).

Há vários tipos de algoritmos, os de chave pública possuem bons mecanismos de gerenciamento de chaves, de autenticação e de não-repúdio se comparado a chave privada. Tem utilidade em ambientes que necessitam da geração de chaves de forma dinâmica, como por exemplo em sistemas heterogêneos (SCHINIANAKIS, 2017).

Esses tipos de algoritmos são usados para gerar mensagens de autenticação, encriptação de payloads e verificação de integridade. A principal desvantagem está no gerenciamento da chave, ou seja, pela necessidade de ter uma chave antecipada (BURTTERFIELD; NGONDI, 2016; SCHINIANKIS, 2017).

4.2 Criptografia

Criptografia essa palavra tem origem grega e significa “escrita secreta”. É uma cifra, ou seja, é uma transformação de caractere por caractere ou de bit a bit. Ela usa um conjunto de métodos que tem como utilidade transformar um texto de linguagem clara em um texto decifrado com aparência de texto sem sentido. Tem como finalidade garantir a privacidade das pessoas. E o processo inverso da cifragem denomina-se como decifragem. E para usar o processo de cifragem e decifragem, é necessário informações confidenciais, ou seja, chaves (STALLINGS, 2014).

Há dois tipos de chaves:

- Chave Simétrica: ou criptografia de chave privada. O emissor da chave utiliza uma chave para cifrar a mensagem, e o destinatário usa a mesma chave para decifrá-la.
- Chave Assimétrica: É conhecida como criptografia de chave pública. Esse tipo de criptografia utiliza duas chaves diferentes, para se ter comunicação segura por meio de canais de comunicação inseguros (BURNETT, 2002).

A chave é muito importante dentro da criptografia, pois oferece sigilo e cuidado para que ninguém que não possua autorização possa usá-la de maneira errada e colocar em risco esse conjunto de algoritmos. O uso de bits aplicados na codificação é fundamental, pois uma chave de 8 bits tem capacidade de gerar 256 combinações diferentes. E uma chave de 128 bits é 275 milhões de vezes mais difícil de ser descoberta comparada a uma de 90 bits (TANENBAUM, 2003).

Para cada informação pode-se fazer uso de chaves diferentes. Sendo assim, mesmo que alguém descubra uma chave, ele não conseguirá descobrir todas as informações (STALLINGS, 2014).

4.2.1 Criptografia simétrica

A criptografia de chave simétrica faz uso da mesma chave para cifragem e decifragem. Portanto, a chave tem que ser conhecida pelo remetente e pelo destinatário da mensagem. A principal dificuldade desse método é a disposição segura das chaves, pois nesse sistema a chave é um número qualquer que possua um tamanho correto e que tenha a seleção automática (BURNETT, 2002).



A duas formas de cifrar dados. Por meio de cifra de bloco ou cifra de fluxo:

- Cifra de fluxo: opera sobre cada bit da mensagem de forma individual, são algoritmos úteis quando o transmissor tem necessidade de enviar uma mensagem para o destinatário um fluxo contínuo de informações criptografadas (VELOSO, 2002).
- Cifra de bloco: apresenta como definição para um algoritmo que possui um tamanho de fragmento de informações para cifrar ou decifrar, e divide o texto simples em blocos e sua operação é independente (BURNETT, 2002).

4.2.2 Criptografia assimétrica

A criptografia assimétrica, ou criptografia de chaves públicas, é fundamentada no uso de pares de chaves para criptografar/descriptografar mensagens. Ambas as chaves têm relação por meio de um processo matemático, que faz uso de funções unidirecionais para codificar a informação. A chave pública qualquer pessoa pode ter acesso e é usada para cifrar, e a chave privada é utilizada para decifrar. Uma mensagem cifrada só pode ser decifrada com uma chave privada que tenha relação com a chave pública. Esse método é bem seguro, pois não necessita compartilhar a chave privada, mas tem como desvantagem o tempo maior de processamento dessa mensagem (BURNETT, 2002).

Esse sistema tem como principal problema a complexidade usada na criação dos algoritmos, e os mesmos devem ter capacidade para reconhecer a dupla de chaves que existem para associar as mesmas quando for necessário, e isso gera um poder altíssimo de processamento computacional (STALLINGS, 2014).

4.3 Assinatura digital

A assinatura digital é um mecanismo que tem como fundamento a criação de código usando mensagem, através de uma chave privada. A assinatura digital ocorre quando um usuário A envia uma mensagem codificada por sua chave a um usuário B e a partir disso será gerada uma assinatura para o usuário A e será colocada na mensagem. O usuário B quando receber a mensagem terá que decodificar fazendo uso de uma chave pública do usuário A, e logo após será gerada uma segunda assinatura verificando a primeira, e só será comprovada se as duas forem idênticas, e assim o usuário B terá confirmação se a mensagem foi enviada ao usuário A (CARVALHO, 2010).

4.4 Redes Privadas Virtuais (*Virtual Private Networks – VPN*)

As redes privadas são compostas por “túneis” de criptografia em pontos autorizados. E sua criação faz uso da própria internet ou de redes públicas ou privadas, para realizar a transferência de informações de modo seguro entre usuários remotos ou redes internas

corporativas. A VPN é uma das redes mais seguras para troca de informações dentro da rede corporativa, pois, os dados são protegidos para não permitir a modificação ou interceptação dos dados (FONTES, 2011).

4.5 Políticas de segurança da informação

As políticas de segurança da informação têm como foco disponibilizar aos usuários da informação nas organizações um conjunto de regras, para manter as informações da empresa seguras. E cabe à direção da empresa determinar as políticas (SANTANA, 2016).

Na maioria das vezes são as empresas que criam suas políticas de segurança, e tal escolha é feita para se adequar ao perfil pessoal da mesma. Porém, essas políticas têm como bases um modelo, como por exemplo Freitas (2016) relata que o modelo se baseia na política de senha, política da internet e política de e-mails, tais políticas têm como objetivo evitar que os usuários contraíam malwares e vírus.

A política de senhas determina que:

- a) a senha deve possuir o mínimo de 6 caracteres composto por números e letras;
- b) a senha é de uso individual e caso o usuário perceba que sua senha foi descoberta a mesma deverá ser trocada;
- c) o uso da senha é de responsabilidade do usuário, então o mesmo deve ter cuidado para mantê-la segura.

A política de internet descreve que:

- a) o uso recreativo da internet não deve ser feito no horário de trabalho;
- b) é proibido fazer uso de aplicativos de mensagem instantânea se não autorizada pela equipe de segurança;
- c) acesso a site de jogos, apostas, bate-papo, sites pornográficos serão bloqueados e devem ser monitorados.

E a política de e-mails ressalta que não deve usar o e-mail da empresa para fins pessoais; evitar o uso de anexos muito grandes e não repassar aviso de vírus, correntes, criança doente ou desaparecida.

5. CONSIDERAÇÕES FINAIS

A informação é um instrumento fundamental para toda empresa, seja qual for o porte ou segmento de atuação. Os atributos básicos da informação, chamado de princípios básicos da segurança da informação (confidencialidade, integridade, disponibilidade, autenticação, legalidade, privacidade e auditoria). Os principais pilares do sistema de informações são: ativo de informação, vulnerabilidade, ataque, incidente de segurança, probabilidade e impacto. Um dos principais fatores que garantem a segurança da informação é a identificação correta, controle e atualização recorrente dos diversos ativos, para garantir a segurança dos dados dos clientes e da empresa.

É necessário que as empresas definam seus sistemas de backup para guardarem uma cópia dos dados, pois, a segurança da informação é obtida a partir da implementação de um conjunto de políticas, processos e procedimentos e estruturas. Os principais sistemas de backup utilizados pelas empresas são: EMC Networker e o Big Data.

As principais ferramentas utilizadas pelas empresas para ter proteção adicional das informações são os algoritmos e podem ter a chave pública ou privada, já a criptografia tem dois tipos: a chave simétrica e a assimétrica; bem como, a assinatura digital e as redes privadas virtuais. Sendo assim, é essencial o estudo dos sistemas de segurança de dados, pois é a segurança desses dados garantem a integralidade e confidencialidade das informações dos clientes e da empresa, e dificulta a ação de hackers, bem como, a utilização indevida desses. É fundamental investir em pesquisas para o desenvolvimento de novos sistemas de backups, para garantir uma segurança de alto nível, e beneficiar as empresas e seus clientes.

Referências

- ADREJEVIC, M; GATES, K. **Big data surveillance:** introduction. **Surveillance & Society**, v. 12, n. 2, p. 185-196, 2014.
- ALEXANDRIA, J. C. S DE. **Gestão de Segurança da Informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica.** São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.
- ALMEIDA, M. B; SOUZA, R. R; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. **Informação e Sociedade: Estudos**, v. 20, n. 1, p. 155-168, 2010.
- ARAUJO, N. S. **Segurança da Informação (TI).** 2008. Disponível em: <https://administradores.com.br/artigos/seguranca-da-informacao-ti>. Acesso em: 12 de abril. 2018.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT)– **Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação:** NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT, 2003.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:2005 Tecnologia da informação:** técnicas de segurança. Rio de Janeiro, 2006.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001:2013.** Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação, 2013.
- BASTOS, A; CAUBIT, R. **Gestão de Segurança da Informação.** ISO 27001 e 27002 Uma Visão Prática. Rio Grande do Sul. Zouk, 2009.

- BEAL, A. **Segurança da Informação**. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo. Atlas, 2005 – Reimpressão 2008.
- BOYD, D; CRAWFORD, K. Critical questions for Big Data. Information, **Communication & Society**, v. 15, n. 5, p. 662-679, 2012.
- BURNETT, S; PAINE, S. **Criptografia e Segurança** – O guia oficial RSA. 1ª edição. Rio de Janeiro: Campus, 2002.
- BUTTERFIELD, A; NGONDI, G. E. **A Dictionary of Computer Science**. 7. ed. New York: Oxford University Press, 2016.
- CABRAL, C; CAPRINO, W. **Trilhas em Segurança da Informação**: Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.
- CARDOSO NETO, C. *et al.* **BACKUP**. **Revista de Trabalhos Acadêmicos**, 2014.
- CARVALHO, A. **Segurança da informação**. Rio de Janeiro: Ufrj, 2010. 31 p. Aula 2.
- CHEVANCE, R. J. **Server architectures**: Multiprocessors, clusters, parallel systems, web servers, storage solutions. Digital Press, 2004.
- CHEVERNAK, A; VELLANKI, V; KURMAS, Z. **Protecting file systems**: A survey of backup techniques. In Joint NASA and IEEE Mass Storage Conference, 1998.
- DE CAMPOS. *et al.* **Network intrusion detection system using data mining**. International Conference on Engineering Applications of Neural Networks. Springer Berlin Heidelberg, p. 104-113, 2012.
- DUBOIS, L; AMATRUDA, R. **Backup and Recovery**: Accelerating Efficiency and Driving Down IT Costs Using Data Deduplication, EMC Corporation, 2010.
- DUMBILL, E. **What is big data?**: an introduction to the big data landscape. O’Reilly, 2012. Online. Disponível em: <https://beta.oreilly.com/ideas/what-is-big-data>. Acesso em: 10 abril. 2022.
- EMC CORPORATION. **EMC NetWorker Release 7.4 Service Pack 1 Multiplatform Version Installation Guide**, Dec, 2007.
- FERNANDES, A. A.; ABREU V. F. **Implantando a governança de TI**: da estratégia à gestão dos processos e serviços (4a edição). RJ: Brasport, 2014.
- FRIEDRICH, L. D. P. M. **Um sistema web para análise de gestão da segurança da informação segundo a norma ABNT NBR ISO IEC 27002**. Disponível em: http://www.redes.ufsm.br/docs/tccs/Lucimara_Friedrich.pdf. Acesso em: 14 de abril. 2022.
- FONTES, E. **Clicando com segurança**: tratando as questões atuais da proteção da informação na organização e na família. Rio de Janeiro: Brasport, 2011. 257 p
- FONTES, E. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.
- FONTES, E. G. L. **Políticas de segurança da informação**. Rio de Janeiro: RNP/ESR, 2015.
- GALEGALE, N. V; FONTES, E. L. G; GALEGALE, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. *Perspectivas em Ciência da Informação*, v. 22, n. 3, p. 75-97, jul./set. 2017.
- HUANG, D. L; RAU, P. L. P; SALVENDY, G. Perception of information security. **Behaviour & Information Technology**, v. 29, n. 3, p. 221-232, 2010.
- INTEL. **Curso Big Data**. 2015 Disponível em: dialogoti.intel.com/pt-br/curso/big-dat. Acesso em: 30/04/2022.
- ISMAIL, B. I. *et al.* **Architecture of scalable backup service for private cloud**. In Open Systems (ICOS), 2013 IEEE Conference on, p. 174-179, 2013.
- ISO/IEC 27035:2011 ISO/IEC 27035:2011, Disponível em: <https://translate.google.com/translate?hl=pt-BR&sl=en&u=https://www.iso.org/standard/44379.html&prev=search&pto=aue>. Acesso em: 01 abril. 2022.

JESUS, G. B. A; SCHIMIGUEL, J. Implementação de backup como processo de segurança da informação. **Atlante: Cuadernos de Educación y Desarrollo**, Málaga, p.1-28, fev. 2018.

KIM, D; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014. 385 p. ISBN 978-0-7637-9025-7.

LEAL, J. C. Identificando pontos em comum entre tipos de políticas de segurança da informação: pontos importantes a serem considerados na implementação de uma política de segurança da informação. **ForScience**, v. 7, n. 1, 2019. <https://doi.org/10.29069/forscience.2019v7n1.e252>

LYRA, M. R. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro. Ciência Moderna, 2008.

MANYIKA, J. *et al.* **Big data**: The next frontier for innovation, competition, and productivity. The McKinsey Global Institute, May 2011. Disponível em: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>. Acesso em: 27 abril. 2022.

MCDOWALL, R. D. Computer (In) security-2: computer system backup and recovery. **The Quality Assurance Journal**, v. 5, n. 3, p. 149-155, 2011.

NETTO, A. S; SILVEIRA, M. A. P. Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**, vol. 4, n. 3, p. 375-397, 2007.

PANOPTYKON FOUNDATION. **Home**. Panoptikon Foundation. 2015. Online. Disponível em: [em,panoptikon.org](http://panoptikon.org). Acesso em: 12 jun. 2015.

PING, Y. *et al.* **Remote disaster recovery system architecture based on database replication technology**. In Computer and Communication Technologies in Agriculture Engineering (CCTAE). International Conference On, v. 1, p. 254-257, 2010.

REVISTA VEJA. Edição 2321 – Entenda o que é Big Data, 2013.

SANTANA, W. R. DE. **POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO**. 2016. Disponível em: http://www.neutronica.com.br/wp-content/uploads/PSI-Material-v1.0-Parte_II.pdf. Acesso em: 14 abril. 2022.

SCHINIANKIS, D. Alternative security options in the 5G and IoT era. **IEEE Circuits and Systems Magazine**, v. 17, n. 4, p. 6-28, 2017.

SÊMOLA, M. **Gestão da Segurança da Informação**. Uma visão executiva. Rio de Janeiro. Elsevier, 2003 – 11º reimpressão.

SIPONEN, M. T. A paradigmatic analysis of conventional approaches for developing and managing secure IS. In: INTERNATIONAL CONFERENCE ON INFORMATION SECURITY, 16., 2001, MA, USA. **Proceedings of...** Trusted information: The new decade challenge. MA: Kluwer Academic Publishers Norwell, p. 437-452, 2001.

STALLINGS, W. **Criptografia e Segurança de Redes**. 6ª edição. São Paulo: Pearson Education, 2014.

STALLINGS, W. **Criptografia e segurança de redes: Princípios e Práticas**. 6ª edição. Pearson Education do Brasil, 2015.

TANENBAUM, A. S. **Redes de Computadores**. Campus; 4ª edição; 2003.

VELOSO, C. J. M. **Criptologia** – Uma ciência fundamental para tratamento de informações sigilosas, 2002. Disponível em: <http://www/>. Acesso em: 28 de abril de 2022.

VERAS, M. Virtualização: Tecnologia Central do DataCenter. 2 ed. - Rio de Janeiro: Brasport, 2016.

CAPÍTULO 14

SEGURANÇA EM DATABASE

SECURITY IN DATABASE

Lucas Evangelista Chaves Junior¹

¹ Ciência da Computação, Faculdade Pitágoras, São Luís - MA

Resumo

É coerente que ocorreu um grande avanço tecnológico desde os primeiros computadores. Dessa forma, cresceu a necessidade de armazenamento de dados. Então, um banco de dados fez-se importante para base de tomadas de decisões e armazenamentos. Tal importância traz consigo a obrigação de proteção dos dados que nele está contido para o uso das empresas é também informações sigilosas no banco de dados. Visto que, essas informações são muito valiosas, e sendo mal utilizadas ou mal protegidas, geram grandes problemas. É necessário que seja monitorado o acesso às informações incluídas no banco para que haja mais controle. Saber como é o funcionamento e muito importante é também manter a segurança de um banco é fundamental. Por isso, tornar-se-á definido um banco de dados, além do mais, como um sistema de gerenciamento de banco de dados é importante para possibilitar uma boa aplicação de um banco, por essa razão será apontada como formas de segurança em banco de dados e sua importância. Mediante de Revisão de Literatura, qualitativa e descritiva.

Palavras-chave: Banco de dados; Importância; Segurança; Necessário.

Abstract

It is understandable that there has been a great technological advance since the first Computers. Thus, the need for storage of said. That is why a database has become an important base for takings, of decisions. Such relevance brings with it the obligation to protect the most information contained in the database. Since, information may be contained valuable and being misused or poorly protected create big problems. It's it is necessary to monitor access to information included in the bank to to act more control. Knowing how it works and what is very vital is also maintaining a bank's security is critical. Therefore, it will be considered and defined a database, in addition to demonstrating how a data management system database is important to to promote good use of a database, for. At the end, forms of database security and their importance will be identified. Through Literature Review, qualitative and descriptive.

Keywords: Database; Importance; Safety; Required.

1. INTRODUÇÃO

Levando em conta a evolução tecnológica, aconteceu grandes avanços nos últimos anos. Através disso é possível que os banco de dados faça o trabalho e a até a extinção de processos antes difíceis. A atenuação da necessidade de um espaço fixado em uma empresa para armazenamentos de dados, e a facilidade e segurança dada pela união de informações em um só lugar, gerou que os banco de dados se transformassem no meio mais eficiente de armazenamento de dados.

Os bancos de dados estão presentes em quase toda empresa que existe é cada vez maior o número de companhias que adere a essa tecnologia, isso faz parte do avanço que existiu nessa tecnologia. A maior parte das empresas e pessoas estão em busca de armazenar dados e informações, por tanto, o banco de dados traz rapidez e recursos primordiais nessa execução.

Aconteceu consideráveis avanços desde a criação do primeiro banco de dados, já que praticamente estão em todos os lugares, pelo meio de computadores smartphones e máquinas produzindo grande volume de informações. Dessa forma a necessidade colher, armazenar e processar faz com que os banco de dados estejam em constante contatos com pessoas, a parti de consultas de estoques, bancárias e compras pela internet

Desse modo, será estabelecido para a realização dessa pesquisa método de Revisão de Leitura, qualitativa e descritiva. Buscando esclarecer questões importantes à segurança em banco de dados, conceitos e definindo o que é um banco de dados em um SGBD e, demonstrada o quão importante é a segurança em banco de dados.

Esta pesquisa fará consultas em artigos, livros e trabalhos publicados por autores como Christopher J Date em "Introdução à sistema de banco de dados" que faz introdução a banco de dados bem como Elmasri, Ramez e Navathe, Shamkant B, em "Sistemas em banco de dados" e Silberschatz A., H .F.Korth e S Sudarsha em "Sistemas em banco de dados" que em suas publicações respondem questões sobre sistemas em banco de dados, e Marcos Sêmola em "Segurança de segurança da informação: uma visão executiva" e Gustavo Alves em "Segurança da informação : uma visão inovadora da gestão " que fala sobre segurança da informação.

2. BANCO DE DADOS

2.1 Aplicações de banco de dados

Antes do avanço tecnológico e da popularização das tecnologias, era comum a prática de excessivos gastos de tempo em tarefas que já são feitas de forma rápida. Um exemplo muito claro dessa situação que ainda existe em determinados lugares, é de empresas que havia a necessidade de armazenar informações em papel, frequentemente a necessidade de um espaço físico somente para esse objetivo. Essa prática possibilitava uma grande



quantidade de papel e impossibilitava a organização de forma simples, além da dificuldade de localização de arquivos e fragilidade da segurança.

Os bancos de dados são capazes de ser vistos como o equivalente eletrônico a um armário de arquivamentos. Visto que as fichas em papel se tornaram registro, que foram colocadas em pastas que se tornam tabelas e que deixaram de serem colocadas em armários e são agora colocadas em banco de dados. De outra forma é apenas conjuntos ou recipientes para um acervo de arquivos de dados computadorizado.

Registros de pessoas em uma tabela é exemplo de banco de dados. Pôs isso na tabela os dados referentes a pessoas cadastradas estão na mesma linha, isso chamamos de registros. O tipo de categoria de informação nome ou telefone sobre uma pessoa fica separado em colunas, nas quais se chamam campos. Uma lista de telefone, lista de compras ou de contatos são exemplos de banco de dados presentes no nosso dia-dia.

Os autores Abaham, Korth e Sudarsham (2012) mencionam que “a revolução da internet na década de 1990 aumentou significativamente o acesso ao direito as bases de dados do usuário.” Com toda essa mudança muitas empresas converteram seus sistemas que eram automáticos como telefones listas, para sistemas de banco de dados e aplicações na web. Com toda essa mudança foi possível ficar com várias informações online facilitando acesso por exemplo de livros armazenamentos de cadastros de sites.

Com esses procedimentos, desenvolve se novas tecnologias como o banco de dados as empresas começaram a fazer mais investimentos nessa tecnologia com mais compras de computadores, e com isso teve uma otimização nos armazenamentos, visto que passaram a ser armazenadas de forma digital no banco de dados.

Os bancos de dados tornaram-se imprescindíveis às empresas, pois centralizaram os dados que antes era variado e disperso (SILVA, 2002). Apesar de esta tão introduzido nos processos da vida habitual, muitas das vezes o usuário final não nota o que está acessando um banco de dados.

2.2 Conceitos e princípios

Segundo Machado (2009, p. 20), “um banco de dados tem que ser determinado com um grupo de dados adequadamente relativos”. O autor diz que um banco de dados possui propriedades através das quais mostra que sua dimensão, vale além de uma simples coleção de dados. A primeira propriedade de um banco de dados é relacionando-se e com uma estrutura de dados com significado. Ele tem uma coleção de dados aleatórias, sem uma finalidade ou objetivo não é considerado um banco de dados.

Seguindo essa ideia Elmasri e Navathe (2001) mostram que um banco de dados por ser de qualquer tamanho, ou complexidade variável, como pode fazer um cadastro simples de um cliente que contém nomes, endereço e telefone com muitos registros. Todavia, o cadastro de clientes de um banco ou entidades do governo com receitas Federal por conter milhões de registro, armazenados perante distintas categorias como pelo nome, pelo endereço, pelo número do CPF e outros.

Tais aspectos indicam o banco de dados como um arquivo que armazena diferentes informações organizadas e distribuídas em tabelas, que estão relacionadas e se comunicam umas com as outras.

“O banco de dados tem por obrigação armazenar dados. Com o objetivo os bancos de dados ajudam as empresas a manter uma demanda de cadastro de usuários solicitada por organizações” (FERREIRA, 2005). Esses que precisaram fazer o armazenamento dos dados importantes que poderão futuramente. O banco de dados deve possuir capacidade a capacidade de armazenar essas informações de maneira contínua e duradoura, para que haja completa segurança.

2.3 Vantagens de um banco de dados

A aplicação da base de dados oferece inúmeras vantagens. Navathe (2022) demonstra as formas mais importantes da utilização do banco de dados está o controle centralizado dos dados, que simplifica a organização de dados separados dentro de uma empresa, impedindo a redundância, para que dentro de um banco não exista dados repetidos ocupando espaço, bem como o compartilhamento de informações apenas para pessoas autorizadas.

O banco de dados quando são bem construídos deveram garantir a segurança das informações, satisfazendo as restrições de acesso. Impedindo que usuários não tenha acesso a informações sigilosas. E garantir a recuperação e backups dos dados caso ocorra perdas, e garantir o controle de concorrência, provendo o acesso seguro simultâneo ao banco de dados, caso dos usuários estejam solicitando a mesma informação.

Bem como o compartilhamento de informações, portanto, dentro de uma empresa o banco deve ser acessível, porém, as alterações serão feitas de acordo com o grau de autorização de cada usuário. Os bancos de dados vieram para facilitar as transações, trazendo agilidade nas operações de armazenamentos dos dados com segurança e melhorando cada tomada de decisões (ALVES, 2002).

3. FUNCIONAMENTO DE UM SGBD

3.1 SGBD

Para Ramez Elmasri (2012), o sistema de banco de dados (SGBD) não deve ser confundido com o próprio banco de dados. Um SGBD é feito por um conjunto de softwares e dados atrelados para o acesso aos dados. A função de armazenar uma informação, e altera ou até mesmo recuperá-la do banco de dados, cabe ao sistema de gerenciamento permitir ou não o acesso ao banco de dados.



Elmasri e Navathe (2002) resume confirmando que um banco de dados é mantido e utilizado por meio de softwares conhecido como Sistema de Gerenciamento de Banco de Dados (SGBD), equivale a uma coleção de dados inter-relacionando e um conjunto de programas para acessá-los. É um sistema que facilita o processo de intenção, construção e manipulação de um banco de dados.

Determinar uma base de dados envolve a especificação de tipos de dados a serem armazenados na base de dados. Construir uma base de dados e o processo de armazenar os dados por meio que seja controlado por um SGBD. Utilizar uma base de dados mostra a aplicação de funções, como as de consulta para recuperar dados específico, e modificações da base de dados para refletir mudança no minimundo (inserções, atualizações e remoções), e geração de relatórios.

3.2 Bancos de Dados *Versus* Processamento Tradicional de Arquivos

Em um processamento tradicional de arquivos, é implementado um ou mais arquivos para a necessidade de cada usuário, já em um banco de dados existe um único repositório de dados, onde todos os usuários acessam os dados que lhe convém. O Quadro apresentado traz as principais características que diferem um sistema desenvolvido na perspectiva de um banco de dados versus um desenvolvimento pelo tradicional gerenciamento de arquivos.

Quadro 1: BD versus PTA

BANCO DE DADOS	PROCESSAMENTO TRADICIONAL DE ARQUIVOS	VANTAGENS DOS BANCOS DE DADOS
Meta Dados	Definição dos dados é parte do código de programas de aplicação	Eliminação de redundâncias
Capaz de permitir variadas aplicações e independência entre dados e programas	Dependência entre aplicação específica e dados	Eliminação de redundâncias e facilidade de manutenção

Fonte: O.K. Takai, I.C. Italiano e J.E. Ferreira. Introdução a banco de dados. DCC- IMEUSP, 2005.

3.3 Perfis de usuários

Para Elmasri e Navalhe (2002) a primeira meta de um banco de dados é organizar um ambiente para recuperar e armazenar novas informações no banco de dados. Pois, um banco de dados de pequeno porte pode ser definido, construído e manipulado por uma única pessoa. No entrando, se tratando de um banco de dados de grande porte, é necessário o envolvimento de muitas pessoas no projeto no uso de manutenção.

Sêmola (2003) afirma que o administrador de um banco de dados (DBA) é o supervisor do banco de dados, ele é responsável pela a autorização de acesso ao banco monitoramento e coordenação de uso. Está comprometido com os aspectos físicos do banco de dados (estruturas de armazenamentos, métodos de acesso etc.).

Dessa forma o projetista do banco é responsável pela identificação dos dados e elaboração de estruturas apropriadas para o armazenamento. Entender os requisitos necessários ao grupo de usuários do banco antes de sua implementação.

3.4 Modelos de dados

Existem muito modelos de dados criados. Sendo capaz de classificar modelos baseados nos tipos de conceitos que provêm para descrever a estrutura da base de dados. Modelos de dados conceituais ou de alto-nível veem das ideias de usuários. Já os modelos de dados físicos ou baixo nível proveem de conceitos que apresentam os detalhes de como os dados são armazenados em computadores (SEMULA, 2003).

Modelos de alto-nível possuem conceitos tais como Entidades, atributos e relacionamento. Uma entidade é um objeto que representa na base de dados. Um atributo é uma propriedade que descreve uma característica de um objeto. Relacionamentos entre os objetos são facilmente de serem representados em modelos de dados de alto-nível, que me determinados vezes são chamados de Modelos Baseados em objetos devido, principalmente, a sua característica de descreverem seus objetos e seus relacionamentos.

Modelos de Dados de Baixo-Nível descrevem como os dados são armazenadas no computador, representando informações em formato de registros ordem dos registros e caminho de acesso. Um Caminho de Acesso é uma estrutura de que facilita a busca de um registro particular na base de dados.

3.5 Arquitetura de um SGBD

Seguindo a arquitetura ANSI/SPARC (Study Group on Data Base Management Systems), que propõe que os sistemas de banco de dados sejam divididos em três níveis gerais: nível interno, nível conceitual e nível externo.

O nível Interno é o mais próximo do armazenamento físico, indica como os dados realmente são armazenados fisicamente. Possui um esquema interno que descreve a estrutura de armazenamento físico da base de dados. O esquema interno usa modelo de dados físico e descreve e todos os detalhes de armazenamento de dados e caminhos de acesso a base de dados.

O nível Conceitual é a representação de todo o conteúdo das informações do banco de dados, é considerado a visão do grupo de usuário. Possui um esquema conceitual é uma descrição global da base de dados, que omite detalhes da estrutura de armazenamento físico e se concentra na descrição de entidades, tipos de dados relacionamentos e restrições.

O nível Externo é o mais próximo do usuário, é como os dados são vistos pelo os usuários individuais. O nível externo ou visão possui esquemas externos ou visões de usu-



ários. Cada esquema externo descreve a visão da base de dados de um grupo de usuários da base de dados. Cada visão descreve, tipicamente, a parte da base dados que um particular grupo de usuários está interessado e esconde deste o restante da base de dados. Um modelo de dados de alto-nível ou um modelo de dados de implementação podem ser usados nesse nível.

4. SEGURANÇA

Como visto o banco de dados tornaram-se parte integrante do cotidiano. Neles podem estar contidas informações valiosas, e necessitam de proteção. Porém é comum aparecer problemas de segurança em banco de dados, dessa forma é preciso que exista atenção em pontos cruciais de proteção no banco.

4.1 Conceitos básicos

Para Date (2003) o termo de segurança tem como significado “o estado de qualidade ou condição de quem ou do que está livre de perigos, incertezas assegurando de danos e riscos eventuais.” E a segurança da informação corresponde para Alves (2006) “a normas, procedimentos ferramentas e técnicas para garantir que os sistemas não possuam perdas, preservando seu valor”.

Date (2003) diz que para a segurança na área da computação existem princípios de segurança, que se utilizam de controles específicos. Esses podem ser divididos em Controles Físicos e Lógicos.

Os controles físicos são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura que a suporta. São medidas que são usadas para garantir a proteção física dos recursos contra ameaças voluntárias e involuntárias.

Já os controles lógicos são barreiras que limitam ou impedem o acesso à informação, que está em ambiente controlado, geralmente sistemas. Devido ao fato de haver um grande número usando de pessoas usando um determinado sistema é necessário o tratamento nos acessos não autorizados ao próprio sistema, e também partindo de outros computadores, possuindo cuidado no acesso a arquivos.

4.2 Segurança em banco de dado

Para quando se fala de segurança em um sistema de banco de dados, vale lembrar que esse sistema é como outro qualquer. Logo, sua segurança está altamente atrelada à segurança do ambiente onde está inserida. Nesse sentido, todos os aspectos de segurança da informação, segurança de hardware, segurança de rede, são pertinentes à segurança de um banco de dados (ALVES, 2006).

A questão da segurança em banco de dados não se restringe apenas ao que é possível gerenciar por meio do SGBD. Diferentes precauções devem ser tomadas no SGBD, na especificação de consultas, na programação das aplicações, no hardware e na rede relacionada ao uso do SGBD.

Além de questões de segurança em termos de tecnologia, também é preciso preocupação com questões éticas e legais, assim como as políticas de uso da informação estabelecidas pelas organizações também precisam ser consideradas. Toda e qualquer decisão tomada junto ao sistema de banco de dados, precisa necessariamente observar esses aspectos. Por isso conhecer é importante para que se faça o uso correto dos recursos que vão implementar questões de segurança dentro de sistemas de banco de dados.

4.3 Princípios de Segurança

Para Rob e Coronel (2011), a segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar a informação. A seguir, estão os atributos que devem ser levados em consideração para solucionar problemas, pois se tornam vulneráveis sem o devido cuidado.

Em relação a questões de segurança, existem três principais questões que são importantes de serem observadas. A questão da perda de integridade, perda da disponibilidade e perda de confidencialidade. Todas essas perdas são danosas ao usuário de sistema de banco de dados, e precisam ser observadas no momento estabelecer as políticas de segurança.

A perda de integridade é aquela que diz respeito ao conteúdo que está armazenada no sistema de banco de dados. Então a integridade do banco de dados, diz respeito à necessidade de proteger as informações contra modificações inapropriadas, criação ou exclusão de dados ou modificação de seus valores. Essa perda pode ser decorrente de ações intencionais ou acidentais e pode permitir fraude ou tomada de decisão incorreta.

Elmasri, Navathe, (2011), definem que é preciso que exista Integridade das informações, mantendo suas características originais. A integridade está para assegurar que os dados no banco de dados se mantenham exatos, certos e validos, preservando o banco contra modificações não autorizadas

Em relação à disponibilidade, é preciso lembrar que a todo o momento em que o usuário precisa acessar valores dentro do sistema de banco de dados, esse sistema precisa estar disponível. A expectativa dos usuários é que o sistema esteja disponível a qualquer momento. Se o sistema não atende a esses requisitos, existe a perda da disponibilidade, que também diz respeito à falta de segurança em termos de uso do sistema.

A indisponibilidade se refere à ocorrência de problemas para o uso do sistema e de seus recursos (funcionalidade e dados). Sofrem com a indisponibilidade tanto usuários humanos quanto outros sistemas (programas) que acessam o banco de dados.



E por fim, a perda da confidencialidade, diz respeito ao quanto é possível confiar que as informações referentes aos dados pertinentes estejam realmente seguras contra o acesso indevido.

4.4 Garantindo a segurança

Além dos três principais princípios existem outros que também fazem parte desse processo importante na garantia de segurança. Outro ponto chave é o “Não Repúdio”, onde seja impossível esconder a autoria de uma informação (ALVES, 2006). Uma pessoa ou empresa não pode negar a autoria daquela informação, também pode ser chamado de irretratabilidade.

A autenticidade é também está inclusa e como Alves (2006) aponta, é a garantia que seja verdadeira a informação enviada. Este princípio indica que quando uma informação é enviada seja proveniente de quem ela realmente diz ser.

Vulnerabilidade está associada a pontos fracos ou falhas que podem ser explorados para obter acesso a um ativo. Segundo a pesquisa da PC 2018, funcionários e ex-funcionários são as duas principais causas na incidência em segurança da informação.

Já ameaça é qualquer coisa que possa explorar a vulnerabilidade, intencional ou acidentalmente, e obter, danificar ou destruir um ativo. Exemplos de ameaças são os crackers, que exploram fraquezas emocionais e/ou configurações fracas, ou a ignorância das pessoas para obter, danificar ou destruir um ativo. Outro exemplo são funcionários insatisfeitos ou que não respeitam regras, que também podem querer obter, danificar ou destruir um ativo. Normalmente ameaças não podem ser controladas.

Seguindo a classificação da Microsoft de ameaças, a STRIDE, onde cada letra corresponde a uma ameaça em potencial, as mais conhecidas ameaças são:

- spoofing (invasão disfarçada) – o spoofing ocorre quando um invasor (usuário ou sistema) se passa por um usuário legal do sistema;
- tampering (adulteração) – a adulteração ocorre quando um invasor adultera o sistema;

A partir dessas definições, Date (2000), fala que segurança de banco de dados se refere à proteção de dados contra revelação, alteração ou destruição não autorizada. E o gerenciamento do sistema para que isso não ocorra, tem como principal ator nesse cenário de sistemas de bancos de dados o administrador, onde ele tem o papel de cuidar de todos os aspectos importantes dentro do ambiente do sistema criando os controles.

4.5 Tipos de controle

O Administrador de Banco de Dados (DBA) possui uma conta com direitos de super-usuário, a qual atribui a ele a responsabilidade de zelar pela segurança no SGBD e banco de dados associados. É este o papel que vai garantir que não existam as perdas, é na realidade, quem pode criar contas, conceder e revogar privilégios, e estabelecer os níveis de segurança por meio de ações mandatórias ou discricionárias (BITTENCOURT, 2004).

No controle discricionário, um usuário terá privilégios diferentes sobre dados diferentes, incluindo a capacidade de acessar arquivos específicos de dados, campos específicos de uma tabela ou mesmo poder utilizar determinadas operações sobre a base de dados (ler, inserir, excluir, alterar, atualizar).

O controle de fluxo na realidade diz respeito a como os valores ou as informações transitam dentro do sistema, como eles são acessados a partir de um tipo de acesso feito de forma externa para dentro do sistema, ou como o sistema vai liberar essa informação para que o usuário/sistema acesse. Isso é feito a partir de uma série de ações que envolvem programação das aplicações (ALVES, 2006).

A depender do recurso de programação usado e do ambiente em que o sistema está instalado e executando, pode-se eventualmente ser aberta uma porta para ataques ao sistema de banco de dados. Então essa é uma questão importante a ser estudada que possui uma série de teorias, conceitos e precauções que se deve estudar em relação a, por exemplo, linguagem de programação e ao estilo de programação que está sendo usada (SÊMOLA, 2003).

Em relação à criptografia, é uma área muito bem desenvolvida em relação à segurança da informação dentro da computação que estuda os algoritmos de criptografia. A criptografia de dados é uma excelente medida para solucionar o armazenamento e transferência sem segurança. É uma forma de dificultar o acesso à informação real, protege dados sigilosos que podem ser transmitidos por redes de comunicação. É utilizada para prevenir que usuários não autorizados acessem as partes confidenciais do banco de dados, codificando os dados e trazendo assim, dificuldades para serem decifrados (SÊMOLA, 2003).

O Controle de tem por objetivo impedir pessoas e/ou programas não autorizados leiam e/ou atualizem a base de dados, sendo está uma das constantes dificuldades dentro de uma empresa e que necessita continua atenção.

A segurança de um banco de dados precisa incorporar provisões para restringir o acesso ao sistema como um todo. Essa função, chamada de controle de acesso, é tratada criando-se contas do usuário e senhas para controlar o processo de login pelo SGBD, e quais as ações que as pessoas são permitidas executar (execução, visão, criação, remoção ou atualização) (ELMASRI; NAVATHE, 2011).

Logo, usar comando em termos de sintaxe é simples, mas, o que é complexo, o que precisa ser muito bem pensado é a estratégia que deverá ser seguida para usar os comandos. E essas estratégias precisam estar em conformidade com questões éticas e com as políticas de segurança da organização onde esse sistema está implementado. Como



exemplo de concessão de privilégio esta as palavras reservadas.

GRANT e AUTHORIZATION: Palavras reservada de SQL que permite conceder privilégios, dar autorizações aos usuários. Com esse comando, é possível dar a outros usuários privilégios, que são, por exemplo, INSERT, DELETE, UPDATE, REFERENCES, TRIGGERS, SELECT e etc., porém, com comandos adicionais como WITH GRANT OPTION, faz com que ao receber privilégios, o usuário também possa conceder privilégios a terceiros. Com o comando REVOKE é possível revogar privilégios já concedidos a usuários.

Então é possível trabalhar com esses comandos de concessão de privilégios de diferentes formas, com uma sintaxe que não é complicada, mas sempre possuindo cuidados com a estratégia que é usada quando se concede esses privilégios a usuários de um sistema (FILHO; CAVALCANTI; FILHO, 2010).

Por fim o backup de dados é outro método importantíssimo, pois impede a perda de dados pelos mais diferentes motivos, seja utilizando mídias ópticas ou HDs. Criar rotinas dentro do banco para que seja feito uma cópia semanal ou mensal dos arquivos é sempre uma forma de assegurar que seus dados não sejam perdidos. Ou então HDs espelhados, para caso o servidor principal falhe o segundo passe a ser utilizado (ALVES, 2006).

5. CONSIDERAÇÕES FINAIS

Diante das informações apresentadas neste trabalho, foi possível perceber que os bancos de dados se tornaram parte integrante e inseparável dos avanços tecnológicos. Portanto, somente com eles foi possível haver o armazenamento dos milhares de dados que estavam sendo criados constantemente nas diferentes aplicações. Sua presença em empresas proporcionou um diferencial no mercado em comparação aqueles não possuem.

Procurou-se neste trabalho deixar de forma clara e objetiva o que é um banco de dados e o como é feita a sua segurança. Para isso, foi preciso apresentar os conceitos e o seu funcionamento, juntamente com suas características, desde como se resultou as modificações no processo de armazenamento com os bancos de dados, a perfis de usuários e modelos de dados.

Na manutenção da segurança de um banco foi preciso entender primeiramente o que é segurança e quais os princípios que os permeiam. Logo após, foi feita a apresentação dos tipos de controle e a exemplificação pratica dos métodos.

Os Bancos de Dados funcionam como parte de um ambiente maior e por estarem sendo constantemente exigidos, precisam estar estruturados e protegidos, e o campo da segurança em banco de dados tornou-se uma área complexa, mas promissora. Por isso é necessário que exista uma maior difusão de como é importante um banco de dados e com isso proporcionar maior facilidade a estudos sobre sua segurança

Referências

- ALVES, Gustavo A. **Segurança da informação: uma visão inovadora da gestão**. Rio de Janeiro: Ciência Moderna, 2006.
- BITTENCOURT, Rogério Gonçalves. **Aspectos Básicos de Bancos de Dados**. Florianópolis, 2004. Disponível em <https://www.marilia.unesp.br/Home/Instituicao/Docentes/EdbertoFerneda/BD%20-%20Aspectos%20Basicos.pdf>.
- DATE, Christopher J. **Introdução a sistemas de banco de dados**. 8. ed. Rio de Janeiro: Elsevier, 2003.
- ELMASRI, R., NAVATHE, S. B. **Sistema de banco de dados: fundamentos e aplicações**. Trad. Teresa Cristina Padilha de Souza. Revisão técnica de Sérgio da Costa Cortez. Rio de Janeiro: LTC, 2002.
- ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6. ed. São Paulo: Pearson, 2011.
- FILHO, Clóvis Luiz de Amorim; CAVALCANTI, Paulo Diego de Oliveira Bezerra e FILHO, Marcello Benigno de Barros Borges. **SQL Injection em ambientes Web**. Curso de Sistemas de Informação. N. 9, Jul/Dez 2010.
- MACHADO, Felipe N. R. **Banco de Dados: projeto e implementação**. 2. ed. São Paulo: Érica, 2008.
- ROB, Peter; CORONEL, Carlos. **Sistemas de banco de dados: Projeto, Implementação e Gerenciamento**. 8 ed. São Paulo: Cengage Learning, 2011.
- SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003, p. 45.
- SILBERSCHATZ A. / H. F. KORTH/ S. SUDARSHAN. **Sistema de Banco de Dados**, tradução da 6a. ed. [por] Daniel Vieira, Rio de Janeiro, Elsevier, 2012.
- SILVA, REGILAN MEIRA. **Banco de Dados**. Instituto Federal de Educação, Ciência e Tecnologia da Bahia – IFBA, 2004.
- TAKAI O.K.; ITALIANO I.C.; FERREIRA J.E. **Introdução a banco de dados**. DCC-IMEUSP, 2005. Disponível em <http://www.ime.usp.br/~jef/apostila.pdf>.

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: 978-65-80751-24-2

BR



9 786580 751242