FRUTOS DO CONHECIMENTO

ADMINISTRAÇÃO E NEGÓCIOS
CIÊNCIA DA COMPUTAÇÃO

Organizadores

Irapuan Glória Júnior
Marcos Oliveira de Morais

Ana Paula Freitas de Lima
Beatriz de Lima Cunha
Camila França de Oliveira
Elson Santos da Costa
Filipe Correa dos Santos Andrade
Francisco Paraguai de Souza Filho
Gabrielly Nunes de Oliveira
Giovanna Oliveira Pina
Irapuan Glória Júnior
Janete Almeida Carriel

Jéssica Aparecida Leal de Souza
Jucelaine Lopes de Oliveira
Marcos de Oliveira Morais
Nicole Nascimento de Santana
Regina Elena de Medeiros
Stephany Victoria Nascimento da Silva
Vanessa Lopes de Almeida
Vitória Liliel da Silva
Wiliam Carlos Galvão

Volume 1

Frutos do Conhecimento

Organizadores

Irapuan Glória Júnior

Marcos de Oliveira Morais

Uma obra vinculada ao
Journal of Technology & Information

www.jtni.com.br

perse

São Paulo

2023

Supervisão: Irapuan Glória Júnior

Capa e editoração eletrônica: Irapuan Glória Júnior

Revisão ortográfica: os autores

<<Ficha Catalográfica>>

Livro **JTnI - Frutos do Conhecimento**

Lista de Autores por Ordem Alfabética

Ana Paula Freitas de Lima

Beatriz de Lima Cunha

Camila França de Oliveira

Elson Santos da Costa

Filipe Correa dos Santos Andrade

Francisco Paraguai de Souza Filho

Gabrielly Nunes de Oliveira

Giovanna Oliveira Pina

Irapuan Glória Júnior

Janete Almeida Carriel

Jéssica Aparecida Leal de Souza

Jucelaine Lopes de Oliveira

Marcos de Oliveira Morais

Nicole Nascimento de Santana

Regina Elena de Medeiros

Stephany Victoria Nascimento da Silva

Vanessa Lopes de Almeida

Vitória Liliel da Silva

Wiliam Carlos Galvão

Dedicamos aos nossos familiares.

Sumário

Introdução..... 11

Administração e Negócios

O Impacto de Poluição da Passagem do Rio Tietê em Santana de Parnaíba sobre as Atividades Comerciais da Região..... 15

Um Estudo Sobre o Ambiente de Trabalho e os Riscos à Geração dos Casos da Síndrome de *Burnout* entre Mulheres..... 25

Logística Reversa das Lâmpadas Compactas e Tubulares..... 65

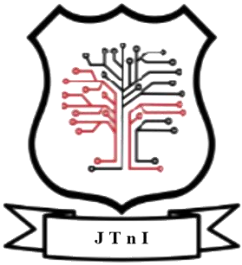
Ciência da Computação

A Indústria 4.0 e os Aplicativos de Entrega de Alimentos..... 89

Segurança da Informação e Proteção dos Dados: Aplicação Web..... 123

Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital..... 163

Apêndice - O Símbolo do JTnI..... 221



INTRODUÇÃO

Irapuan Glória Júnior

Marcos de Oliveira Morais

Introdução ao Livro

Este livro nasceu com a petulância de propagar, ainda mais, o conhecimento gerado pelos pesquisadores brasileiros que ousadamente, superando os obstáculos individuais que a vida apresenta, conseguiram publicar em um dos números do *Journal of Technology & Information*.

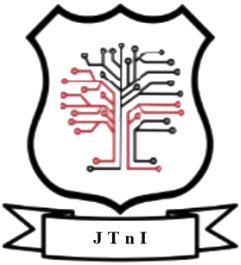
O uso dos adjetivos utilizados não é meramente midiático, visto que no Brasil há baixa quantidade de artigos científicos geradas pelos nossos pesquisadores devido ao fato das dificuldades de obtenção de recursos financeiros, estímulos acadêmicos e cultura nacional.

Apenas destes infortúnios, os autores tiveram êxito! Vislumbrando uma nação mais científica e evolutiva, elaboraram seus textos com otimismo e satisfação.

Desta forma, convido o autor a mergulhar nas pesquisas realizadas pelos autores.

Irapuan Glória Júnior e Marcos de Oliveira Morais

Organizadores do Livro e Editores do JTnI



CAPÍTULO 1

O Impacto de Poluição da Passagem do Rio Tietê em Santana de Parnaíba sobre as Atividades Comerciais da Região

Vitória Liliel da Silva

Nicole Nascimento de Santana

Ana Paula Freitas de Lima

1 Introdução

O Rio Tietê é considerado o mais importante rio que atravessa o estado de São Paulo com 1.250km de extensão, entre Mogi das Cruzes e Pirapora do Bom Jesus Constatino e Graviola (2020). As políticas públicas de saneamento básico e recursos hídricos, do governo do estado de São Paulo, têm enfrentado grandes desafios há décadas, mesmo com as mudanças da gestão do governo, os incentivos para o tratamento e despoluição do rio Tietê continuam (Oliveira, 2015).

A sociedade tem convivido durantes anos com essa riqueza natural que gera problemas sociais e ambientais e vem mobilizando protestos ao poder público, devido aos incômodos proporcionados nos centros urbanos residenciais e comerciais (Maes, 2023).

Na região metropolitana de São Paulo é possível identificar vários fatores que justificam o fluxo do mercado imobiliário. As organizações são constituídas por estruturas políticas e culturais que podem sofrer disrupções devido a

transformação (Kotler, 2016), a poluição é um dos elementos causadores de divisões dos aglomerados na região metropolitana de São Paulo.

O governo do estado de São Paulo tem investido bilhões de reais na despoluição do rio (Maes, 2023), mas grande parte deste investimento é direcionado ao saneamento básico, com o tratamento de esgoto, expansão da rede e coletores troncos (Oliveira, 2015).

No município de Santana de Parnaíba, o rio atravessa a cidade, gerando odor e espuma, proporcionando incômodo aos munícipes e comerciantes. Esses odores e espumas são influências do "Rio Tietê" percebidas pelo comércio local como do macroambiente, que são ameaças externas que fogem do controle da gestão empresarial (Hitt et al, 2011).

Diante deste contexto, este trabalho tem como questão de pesquisa: "Qual o impacto da poluição do "Rio Tietê" sobre o comércio local de Santana de Parnaíba?". Os objetivos são: (1) Identificar políticas públicas do

município para a despoluição do rio; e (2) Elencar os impactos no comércio local.

Conforme o resultado obtido, conseguimos analisar a situação atual do rio, as principais queixas dos comerciantes locais e o que a gestão pública tem realizado para amenizar esse problema, que afeta a população geral, analisando também hipóteses a serem utilizadas por eles e meios para solucionar a questão.

2 Referencial Teórico

2.1 O Rio Tietê

De acordo com os autores Constatino e Graviola (2020) a hidrovia brasileira tietê-paraná é conhecida nacionalmente por seus 1.250 quilômetros que cobrem quase todo o estado de São Paulo de leste a oeste, e marca a geografia urbana da capital paulista, a maior cidade do país, o Tietê nasce na cidade de Salesópolis, a 22 quilômetros do Oceano Atlântico, e desce para o interior de São Paulo. A história do rio teve como uma de suas origens e descoberta por alguns bandeirantes, que fizeram o uso do

rio como um meio de transporte para assuntos comerciais com o interior do Brasil e o litoral paulista (Matias, 2023).

Segundo a Prefeitura do Município de Tietê (2023), a partir da década de 1950, com o deslocamento da população e o crescimento da indústria na cidade de São Paulo, o rio passou a receber esgoto doméstico e industrial dentro dos limites da cidade, poluindo e poluindo suas águas.

A degradação do rio ao longo dos anos deu origem pelo aumento populacional, gerando uma expansão desordenada e aumentando o processo de industrialização, o que teve como resultado no ano de 1970 com índice de Oxigênio na água equivalente a zero, restando apenas espumas e o mau cheiro (Mendes, 2022).

Grande parte da poluição no rio Tietê atualmente é relacionada à própria Sabesp, que em muitas regiões e municípios faz o despejo sem tratamento nos rios, córregos e represas que compõem a bacia hídrica do rio Tietê, sendo após esses atos a empresa foi denunciada em 2012 pelos seus atos de poluição hídrica, e o ministério público exigiu

que a empresa (SABESP) fosse a responsável pela universalização de coleta e tratamento de esgoto coletados, tendo até 2024 para cumprir com essa ação (Carvalho, 2015).

O microambiente ajudará você a entender o impacto das operações do dia a dia da empresa e suas relações com clientes e fornecedores, enquanto o estudo do macroambiente fornece mais confiança em questões de longo prazo que afetam o ambiente geral em que a empresa opera (Moreira, 2008). Sendo que nesse contexto a situação atual do rio afeta na influência do mercado.

2.2 Centro Comercial de Santana de Parnaíba

A história de Santana de Parnaíba tem suas raízes no povoado que se desenvolveu em torno de uma capela construída por Manuel Fernandes Ramos, integrante da expedição Mem de Sá de 1561 (Nascimento, 2021).

De acordo com informações do guia turístico em parceria com o Centro de Apoio ao Trabalho - CAT (2021), o centro histórico da cidade começa no final do século XVI

com a construção de uma igrejinha às margens do rio Tietê em 14 de novembro de 1580, sendo umas das cidades mais antigas de São Paulo, a vila de Parnahyba foi fundada por Suzana Dias junto com seu filho André Fernandes, que estão por navegarem no rio Anhembi (Tietê) onde a navegação já não era possível e sua família resolveu por arrumar uma moradia e se estabeleceram no lugar aonde conhecemos pela cidade de Santana de Parnaíba.

O fato de ter chegado ao mercado em 1982 ajudou a preservar centenas de casas construídas com técnicas tradicionais, como taipa de pilão, cercas, pique e adobe, o que tornou uma localização boa para comércios se instalarem devido ao turismo, e em julho de 2007, o centro histórico foi afetado por uma enchente, causada pelo rio em sua margem, o que afetou não só os moradores, como também o comércio local (Santana De Parnaíba, 2013).

2.3 Políticas Públicas

Com uma série de processos, a política pública são ações governamentais para estabelecer direitos à população de forma de sanar suas pendências como cidadão.

A teoria da burocracia, escrita pelo sociólogo alemão Max Weber, visa estudar as organizações, sua estrutura e desenvolvimento histórico-social, e tem como principal vantagem utilizar a racionalidade como ferramenta para o alcance da eficiência nas organizações (Cruz et al., 2022). Com base nela, as instituições públicas burocráticas começaram a substituir as formas hereditárias de gestão e ganhou importância pela necessidade de maior previsibilidade e precisão no trato dos problemas organizacionais, que precisam ser analisados de forma burocrática (Carlo et al., 2017).

A SABESP (2021) integrou o projeto "Rio Tietê", o que levou a oferecer saneamento básico a 12,4 milhões de pessoas, além de contribuir com a despoluição, tendo o índice de coleta e tratamento em 92% diferente do início do projeto em 1992, onde o índice era de 70%. Porém o número da mancha de poluição aumentou no ano de 2022 de 85km para 122km, em apenas um ano, e um dos motivos da perda da qualidade da água é a transferência de sedimentos não tratados e contaminados acumulados no

reservatório de Pirapora do Bom Jesus para o Médio Tietê (Maciel, 2022).

Desde o começo do projeto, segundo Maes (2023) foram investidos mais de R$17 bilhões em ações para rio, e até 2026 o governo do estado de São Paulo pretende investir até R$5,6 bilhões para realizar a despoluição do maior rio de Tietê, sendo que grande parte desse investimento vai ser para os procedimentos de saneamento básico, como o aumento da capacidade de tratamento de esgoto e expansão das redes e coletores, além de que de todo o total investido R$800 milhões devem vir do Banco Interamericano de Desenvolvimento (BID).

Na cidade de Recife-PE, o rio conhecido como rio Capibaribe passou com desgastes ambientais muito grandes de acordo com David (2022) o rio se tornando um esgoto a céu aberto, em razão a população local que passou a depreciar as águas locais sem o tratamento adequado do governo, porém em 2012 a política nacional de mobilidade urbana (PNMU) passou por um projeto chamado "Rios da Gente", onde tinha como objetivo melhorias do transporte público e a recuperação dos rios, a meta estipulada era

prevista para até 2014, mas até 2021 menos de 2% da obra foi concluída, estando em aberto até nos dias de hoje.

3 Metodologia

A pesquisa possui caráter qualitativo, foi realizada uma pesquisa bibliográfica direcionada a autores em cada abordagem deste trabalho. A coleta de dados foi realizada por meio de questionários direcionados aos consumidores, foram entrevistadas 44 pessoas, os comerciantes, foram entrevistados 05 comércios e a Secretaria de Meio Ambiente da Prefeitura Municipal de Santana de Parnaíba (Tabela 1).

Tabela 1 – Metodologia de Pesquisa

Item	Descrição	Autor
Natureza	Qualitativa	Gil (2019)
Metodologia	Pesquisa bibliográfica	Theóphilo e Martins (2016)
Coleta de Dados	- Questionário - Entrevistas e - Documentos.	Marconi e Lakatos (2017)
Unidade de Análise	Santana de Parnaíba	Theóphilo e Martins (2016)

4 Análise e Interpretação dos Resultados

A análise de dados foi realizada concomitantemente com a pesquisa bibliográfica, a realização de interpretações dos questionários, entrevistas e documentos.

Com base no levantamento de dados, com os consumidores/moradores de Santana de Parnaíba por meio de questionário on-line, foram 44 respostas, onde fica evidente que a poluição influência de forma negativa os comércios da região com 89% dos respondentes. Os

consumidores desistem das compras nos comércios às margens do "Rio Tietê" se tiver com alto odor, com 58% dos respondentes. No ponto de vista geral 100% dos respondentes concordam que se haver intervenção pública para tratamento da poluição do "Rio Tietê", os ambientes comerciais melhorariam.

Em entrevista com 5 comércios, sendo um restaurante, uma adega, duas lojas comerciais e uma loja de fast-food, todos concordam que o odor do "Rio Tietê" desagrada os clientes que frequentam seus estabelecimentos. Quando se questiona, se o comerciante se incomoda com o odor, todos responderam que é sim, mas não tem o que fazer. Esse fato é preocupante, visto que não se tem conhecimento das ações que o poder público pode desenvolver para criar políticas públicas para resolução deste problema. Ao questionar sobre as ações que a prefeitura municipal realiza para despoluição do rio, muitos disseram que não fazem nada e que seria importante a ação da prefeitura. Os comerciantes concordam que o fato do "Rio Tietê" passar pela cidade e em dias de odor afasta os turistas.

Os comércios estão sofrendo impactos do macroambiente, variáveis de influências ambientais, a poluição do "Rio Tietê" é considerada um fator externo, por não estar sob o controle da empresa, o que deve deter maior atenção.

Em uma entrevista com a bióloga, que atua a mais de 7 anos na área, teve experiência em algumas empresas privadas, indústrias e atualmente como servidora pública na prefeitura de Santana de Parnaíba, da Secretaria de Meio Ambiente, fornece informações de como o "Rio Tietê" é prejudicial à saúde dos moradores, além impactar a visita de turistas a cidade por conta da poluição. Explica que o município não possui política pública para resolução do problema. O que fazem para diminuir os efeitos gerados para a comunidade, é uma ação chamada "Xô Mosquito", onde em épocas quentes, tem uma proliferação muito grande de mosquitos, e são aplicados inseticidas na várzea do Tietê para minimizar a proliferação. Embora não utilizem técnicas desenvolvidas para esta finalidade, acham conveniente o uso de metodologias que ajudem a tornar o

rio um pouco mais agradável e não só fiscalizar o controle de pragas.

O nível de poluição é examinado pela SOS Mata Atlântica anualmente e em 2022 o resultado foi de qualidade péssima, diante deste cenário a prefeitura irá solicitar verbas ao Estado para desenvolvimento de projetos. A bióloga informa que no momento não está sabendo de nenhum tipo de investimento ou autorização. Foi evidenciado que a prefeitura tem ciência dos impactos negativos aos moradores, comerciantes e turistas.

Entretanto, a Prefeitura de Santana de Parnaíba mostra-se interessada na metodologia de despoluição da margem caso ocorra algum projeto do Estado de São Paulo e está disposta a utilizar as ferramentas de verificação que já fazem para fiscalizar, como um processo sistemático para contribuir. Conforme suas colocações, acha importante incluir novas formas de elaborar e implementar o planejamento, no sentido de minimizar problemas futuros, bem como, considerar problemas e situações que possam vir a acontecer num prazo maior de tempo. A prefeitura faz o monitoramento em regiões de tubulações por onde passa

o esgoto da cidade, mas apenas o controle, e que não tem fiscais o suficiente para todos os trechos de esgotos, deixando alguns sem a realização de fiscalização.

Existe um processo de despoluição com uso de Macrófitas Aquáticas, esse processo é conhecido como rizo filtração, onde é preciso que a água contaminada entre em contato com as raízes das plantas. Para isso, os sistemas de tratamento por rizo filtração, precisam ter o contato efluente de profundidade do sistema, correspondente às profundidades das raízes das plantas aquáticas. As macrófitas são as espécies mais utilizadas para esse tipo de processo, ainda podendo fazer a fito remediação de materiais inorgânicos, como os metais pesados, elas apresentam uma boa tolerância e um desenvolvimento contínuo, mesmo em contato com substâncias de metais pesados (Carlos, 2022).

5 Conclusões

Apesar das evidências de que a despoluição do "Rio Tietê" ainda seja pouco estudada e empregados no município, acredita-se que o uso da ferramenta de pesquisa

e de monitoramento, pode auxiliar o processo estratégico no setor do turismo e comércio local.

Embora os métodos sejam praticamente desconhecidos internamente na prefeitura, detectou-se que os profissionais envolvidos nas questões estratégicas da secretaria estudadas são simpatizantes do método e acreditam que ele é importante. Dessa forma, nota-se que há espaço para o estímulo ao conhecimento e adequação dos métodos para construção de cenários na secretaria, em que pesem as dificuldades apontadas a implementação de projetos em prol do "Rio Tietê".

Em resposta a questão de pesquisa, existem impactos negativos da poluição do "Rio Tietê" em relação ao comércio local em Santana de Parnaíba. A prefeitura municipal não possui políticas públicas que visa a despoluição do rio. Os impactos destacados pelos comerciantes e moradores são: a inibição de visitas à cidade de turistas, perda de clientes e desagrado dos moradores ao seu odor.

A contribuição para a teoria é aprofundar conhecimentos das políticas públicas municipais e os impactos causados dos comerciantes locais frente a poluição do rio. As contribuições para a prática foram apresentar informações como base à novas pesquisas sobre as ações empregadas sobre a despoluição do rio. Como proposta de pesquisas futuras, uma análise das políticas públicas adotados nos municípios e realizar um comparativo e análise de eficiência destas políticas, bem como uma possível solução para a despoluição

Referencial Bibliográfico

Carlo, A. M., & Carlo, C. C. (2017). Teoria da Burocracia: uma revisão literatura. REVISTA DE TRABALHOS ACADÊMICOS–UNIVERSO BELO HORIZONTE, 1(2).

Carlos, L (2022). Fito remediação de solo ou substrato contaminado pela ação do homem no ambiente. Disponível em: https://files.comunidades.net/saudeintegral/TCC_de_FERTILIZACAO_de_SOLOS_2022_Luiz_Carlos_Fernandes.pdf. Acesso em: 10 abr. 2023.

Carvalho, Liana. (2015). Sabesp despeja esgoto no Tietê. Disponível em: https://www.ocafezinho.com/2015/08/03/sabesp-despeja-esgoto-no-tiete/. Acesso em: 16 nov. 2022.

Constatino, N; Graviola, G (2020). Percepção do Rio Tietê na paisagem urbana de Barra Bonita, Brasil. Disponível em:

http://cegot.org/ojs/index.php/GOT/article/view/2020.19.005. Acesso em: 16 nov. 2022.

Cruz, R., & MARINNI, H. (2022). Teoria da burocracia na administração pública brasileira: uma revisão sistemática. *Revista Brasileira de Administração Científica*, *13*(3).

Centro de Apoio ao Trabalho - CAT (2021) – Guia turístico de Santana de Parnaíba. SECOM.

David, F (2022). Impacto da despoluição dos rios Tietê e Pinheiros na mobilidade urbana da cidade de São Paulo. Disponível em: ttps://repositorio.ufscar.br/handle/ufscar/16758. Acesso em: 26 fev. 2023.

Gil, A. C. (2019) Como Elaborar Projetos de Pesquisa. 7º. ed. São Paulo: Atlas.

Hitt, M, ET AL (2011). Administração estratégica: competitividade e globalização. 2. ed. São Paulo: Cengage Learning.

Kotler, P., & Keller, K. L (2016). Marketing Management Shanghai: Shanghai People's Publishing House.

Maciel, C (2022). SOS Mata Atlântica: mancha de poluição do Rio Tietê cresce 40%: Em um ano de monitoramento, o rio também perdeu na qualidade da água. São Paulo: Agência Brasil. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-09/sos-mata-atlantica-mancha-de-poluicao-do-rio-tiete-cresce-40. Acesso em: 16 fev. 2023.

Maes, J (2023). Governo de SP anuncia R$ 5,6 bi até 2026 em investimentos na despoluição do Tietê. Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/ambiente/2023/03/governo-de-sp-anuncia-r-56-bi-ate-2026-em-investimentos-na-despoluicao-do-tiete.shtml#:~:text=O%20governo%20de%20S%C3%A3o%20Paulo,o%20maior%20rio%20do%20estado. Acesso em: 13 abri. 2023.

Matias, Á (2023). Rio Tietê. Disponível em: https://mundoeducacao.uol.com.br/geografia/rio-tiete.htm. Acesso em: 15 mar. 2023.

Mendes, T (2022). Estudo de caso descritivo sobre a viabilidade do projeto Tietê com foco no tratamento de efluentes. 82 p. 2022. Trabalho de Conclusão de Curso (Graduação em Engenharia Química) – Universidade Federal do Pampa, Campus Bagé, Bagé. Disponível em: https://repositorio.unipampa.edu.br/jspui/handle/riu/7043. Acesso em: 13 abri. 2023.

Moreira, J. C. T. et al. (2008) Serviços de marketing: um diferencial competitivo. São Paulo: Saraiva.

Nascimento, G (2021). Santana de Parnaíba: conheça a história e os principais pontos turísticos da cidade. Cidadão e Repórter. Disponível em: https://www.cidadaoereporter.com.br/viver-bem/turismo/tur2021/santana-de-parna%. Acesso em: 13 abri. 2023.

Oliveira, E (2015). Desafios e perspectivas para recuperação da qualidade das águas do Rio Tietê região Metropolitana de São Paulo. Universidade de São Paulo.

Prefeitura do Município de Tietê (2023). História. Disponível em: https://www.tiete.sp.gov.br/14_historia.php. Acesso em: 26 abr. 2023.

SABESP (2021). Projeto Tietê leva saneamento a 12,4 milhões de pessoas e contribui para reduzir poluição. Disponível em: https://site.sabesp.com.br/ site/imprensa/noticias-detalhe.aspx?secaoId=65&id=8598. Acesso em: 28 fev. 2023.

SANTANA DE PARNAÍBA (2013). História. Disponível em: https://docs.google.com/document/d/1NaQYsgW9piWDCGvka6II9159eBsjaJTgkngoTf85Otw/edit#. Acesso em: 02 mar. 2023.

Theophilo, C, & Martins, G (2016). Metodologia Da Investigação Cientifica. (3a). Atlas.

Apêndice 1 – Questionário com Comércio Local

1. Você, cliente, acha que o rio tem influência de forma negativa nos comércios da região? (comerciante, vá na opção "outros")
2. Você já saiu de um ambiente (lojinha de bairro, mercado, farmácia, padaria, entre outros) por conta do mal cheiro do rio?
3. Na sua opinião, se o rio fosse tratado isso melhoraria os ambientes comerciais da região?

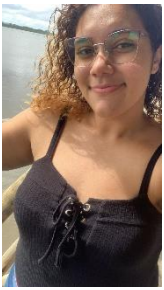
Apêndice 2 – Questionário com a Bióloga da Prefeitura do Município.

1. O que é feito pela prefeitura para amenizar os impactos da poluição do rio Tietê?
2. Vai ser investido um dinheiro para ser realizada a despoluição do rio, isso vai ser aderido em Santana de Parnaíba?
3. Você acredita que o rio Tietê tem impacto negativo no setor de turismo e comércio aqui na cidade?
4. Sobre a poluição, você acredita que são mais os moradores ou indústrias?
5. Sobre a fiscalização, não tem pessoas para fiscalizar?

Apêndice 3 – Entrevista Comércio Local

1. Pela sua percepção, como o seu cliente lida com o fato do rio Tietê estar próximo ao seu local de refeição?
2. E para o senhor, como lida com o rio próximo ao seu comércio?
3. O odor do Rio te incomoda ou algum outro funcionário?
4. O senhor acha que a prefeitura da cidade conseguiria ajudar mais em relação ao comércio em conjunto com a despoluição do rio?
5. Na sua opinião, o rio acaba afastando possíveis turistas?

Autores deste Capítulo



Vitória Liliel da Silva

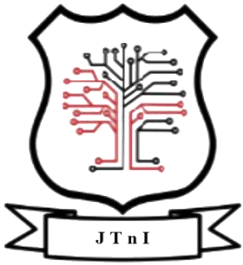
Graduada em Gestão Comercial pela FATEC Santana de Parnaíba, com formação técnica em logística pela ETEC Bartolomeu Bueno da Silva, além de ter especialização em design gráfico e noções básicas de linguagem de programação como o HTLM pela escola SAGA. Autora do artigo publicado no *Journal of Technology & Information*, sobre "O Impacto de Poluição da Passagem do Rio Tietê em Santana de Parnaíba sobre as Atividades Comerciais da Região" v. 3, n 1.

Nicole Nascimento de Santana

Graduada em Processos Gerenciais pela Universidade Anhembi Morumbi, pós-graduanda em Negócios Internacionais e Comercio Exterior e graduanda em Gestão Comercial pela FATEC de Santana de Parnaíba. Cursou ainda Licenciatura em História pela Universidade Federal de São Paulo (UNIFESP), mas acabou não concluindo. Entusiasta na temática socioambiental ou sociocultural.

Ana Paula Freitas de Lima

Mestranda no Programa de Pós-Graduação de Administração (PPGA) na Universidade Paulista (UNIP), possui Graduação em Administração com habilitação em Marketing pela Faculdade Integração Zona Oeste (2006) e MBA em Gestão Empresarial Integrada pelo Centro Universitário - UNIFIEO (2009). Atua como professora convidada na Associação Educacional IBS Américas com disciplinas na área de Administração e Negócios voltado para Microempreendedores. Ministro aulas no Centro Paula Souza nas disciplinas de Plano de Negócios e Marketing e atuo como diretora acadêmica na Faculdade de Tecnologia de Santana de Parnaíba.



CAPÍTULO 2

Um Estudo Sobre o Ambiente de Trabalho e os Riscos à Geração dos Casos da Síndrome de *Burnout* entre Mulheres

Janete Almeida Carriel

Beatriz de Lima Cunha

Giovanna Oliveira Pina

Jucelaine Lopes de Oliveira

1. Introdução

A sobrevivência humana desencadeou situações adversas, que requerem um equilíbrio funcional peculiar. Nesse contexto, a perturbação desse equilíbrio causada pelo Covid-19 e as medidas adotadas para controlar sua disseminação provavelmente exigem ajustes nos tratamentos psicológicos e fisiológicos, uma vez que a pandemia resultou em altas demandas de trabalho, levando ao aumento da incidência da Síndrome de *Burnout* (Sá et al,2022).

De acordo com o Ministério da Saúde (2020) a Síndrome de *Burnout* é um distúrbio emocional com sintomas de exaustão extrema, estresse e esgotamento físico, resultante de situações de trabalho desgastante, que demandam muita competitividade e responsabilidade.

A Síndrome de *Burnout* é uma doença mental que está se tornando mais prevalente no local de trabalho e pode ter efeitos prejudiciais tanto para os indivíduos quanto para os empregadores. resultando em baixa produção,

absenteísmo e altas taxas de rotatividade (Trigo, Teng & Hallar, 2007).

Sua principal causa está atrelada ao excesso, muito comum em profissionais que atuam sob pressão e, em ambientes hostis com rotinas cansativas, possivelmente com lideranças agressivas, associadas a expectativas irreais quanto ao desenvolvimento; especialmente quando os diversos obstáculos impedem de alcançar o resultado esperado gera um abalo emocional, frustração, além de influenciar diretamente seu comportamento no ambiente de trabalho e fora dele (França & Rodrigues, 2011).

Essa discussão sobre ambiente e vida, já vinha sendo amplamente abordada por Tamayo & Tróccoli (2002) que definiam a Síndrome de *Burnout* como: um conjunto de causas negativas que afeta o indivíduo como profissional, decorrente da tensão emocional crônica no trabalho, sendo caracterizado pelas dimensões da exaustão emocional, despersonalização e diminuição da realização pessoal.

É preciso observar que todos estão sujeitos aos riscos e danos à saúde provocados pelo excesso de trabalho, entretanto com impactos distintos entre os gêneros, em razão da diferenciação de força de trabalho entre homens e mulheres, em grande parte motivados pelos conflitos de papeis e dos processos de socialização, relacionados a excessiva rigidez dos valores diferenciados sexualmente e a repressão sexual sobre a mulher (Beauvoir,1949)

O estudo tem como objetivo investigar as consequências da Síndrome de *Burnout* em mulheres que atuam nas empresas situadas em Santana de Parnaíba. Para isso, adota-se uma abordagem qualitativa, com a coleta e análise de dados não estruturados. A pesquisa inclui uma entrevista direcionada com uma profissional diagnosticada com Burnout, e a aplicação de um questionário fechado a mulheres da região. O questionário busca identificar as causas comuns da síndrome, bem como a percepção das profissionais em relação ao trabalho e aos papéis sociais e profissionais.

2. Referencial Teórico

2.1. Síndrome de *Burnout* no Brasil

A Síndrome de *Burnout* é definida pelo Ministério da Saúde (2020) como "um distúrbio emocional com sintomas de exaustão extrema, estresse e esgotamento físico resultante de situações de trabalho desgastante, que demandam muita competitividade ou responsabilidade".

De acordo com o Ministério Público do Estado do Piauí (MPPI, 2020), a Síndrome de *Burnout* está associada ao local de trabalho que não foi adequadamente administrado, sendo um fenômeno diretamente vinculado às relações de trabalho que acabam se transformando em ansiedade e nervosismo intenso e o indivíduo afetado acaba sendo levado ao seu limite físico e emocional, com sentimentos de esgotamento e desmotivação.

Isto se dá, devido ao mercado de trabalho cada vez mais competitivo e o alto número de demissões no país, bem como a cobranças por melhores resultados, toda esta pressão, somada ao cansaço e até mesmo às más lideranças,

está tornando o ambiente de trabalho cada vez mais prejudicial à saúde.

Segundo a pesquisa realizada pela *International Stress Management Association* (ISMA-BR) em 2018, 32,0% dos profissionais brasileiros sofrem com a Síndrome de *Burnout*, totalizando mais de 33 milhões de cidadãos, bem como 90,0% dos entrevistados praticavam o presenteísmo, mas, emocionalmente ou mentalmente encontram-se distantes do trabalho. Com o mercado de trabalho cada vez mais competitivo, os profissionais sentem uma cobrança diária por melhores qualificações e bons resultados, assumindo altas cargas de trabalho para superar as expectativas das empresas.

Portanto, esta situação é muito favorável para o surgimento da Síndrome de *Burnout*, pois a tensão constante, seja no contexto físico e/ou mental e a baixa produtividade, que pode vir acompanhado de culpa, gera sofrimento que impacta a vida dessas pessoas. E quem são os mais propícios a desenvolver esta síndrome?

De acordo com Cox (2021), jornalista da BBC News Brasil, os dados que olham especificamente para a Síndrome de *Burnout* em mulheres são preocupantes, isto porque segundo uma pesquisa feita pela plataforma LinkedIn, com quase 5 mil respondentes, 74,0% das mulheres disseram que estavam muito ou razoavelmente estressadas por motivos ligados ao trabalho, em comparação com apenas 61,0% dos empregados do sexo masculino que responderam à pesquisa.

Ainda sob o ponto de vista de Cox (2021) esse número está relacionado à diversos fatores, dentre eles está o período em que o mundo se encontrava, diante da proliferação da Covid-19 e a potencialização do isolamento social, que resultou na alteração da forma de trabalho sendo alterada do modelo presencial para o modelo *home-office.*

2.2. O Aumento de Incidência dos Casos de Síndrome de *Burnout*

De acordo com Alves (2016), "A pressão no trabalho pode evoluir para o estresse e o estresse pode

evoluir para quadros ansiosos e depressivos", e o trabalho *home-office* proporcionou a cobrança excessiva de tarefas, a falta de estrutura e preparo dos gestores e das instituições, contribuiu para o aumento dos transtornos mentais.

Com objetivo de averiguar os aspectos relacionados ao preparo das organizações para o modelo de trabalho *home-office*, o Data Senado (2020) realizou um estudo ao qual apontou que 58% das organizações não estavam preparadas para esse modelo laboral, e que a principal dificuldade dos colaboradores no processo de adaptação foi conciliar as atividades laborais com as atividades domésticas, isto porque o ambiente de trabalho e o ambiente de descanso foram fundidos em um só.

Para as mulheres essa mistura de ambientes acabou sendo mais agravante, pois, além de exercer os papéis de mãe, dona de casa e esposa, elas tiveram que agregar sua vida profissional dentro do mesmo ambiente, que antes era disposto como seu refúgio.

A invasão das atividades laborais para o lar da colaboradora é prejudicial para a sua saúde mental, tendo

como consequência o desenvolvimento da Síndrome de *Burnout* já que, as profissionais acabam trabalhando muito mais do que se estivesse na empresa, misturando o trabalho com a vida pessoal gerando assim uma sobrecarga significativa, isso porque 65,0% das empresas não tiveram preocupação em acompanhar a saúde física e psicológica de seus funcionários (FIA,2020).

2.3. O Papel das Empresas em Relação a Saúde Mental das Colaboradoras

É inquestionável a importância das organizações para criar um ambiente laboral saudável para todos, após a declaração oficial da Pandemia COVID 19 por meio do decreto legislativo Nº 6 de 20 de março de 2020, neste momento, a rotina das pessoas mudou, e quando falamos das mulheres, houve uma dissolução das estruturas e redes de apoio, deixando em evidência o impacto social desproporcional no que tange aos aspectos de gênero.

A ocorrência de dados estatísticos apresentando as mulheres como o gênero mais afetado, não denota necessariamente algum tipo de fragilidade feminina, mas sim, a

consequência direta de um quadro de sobrecarga que na maioria das vezes reúne aspectos físicos e emocionais.

A gravidade destes dados apenas reforça que, a problemática e objetivos desta pesquisa são relevantes, pois, apresentam uma análise sobre como as organizações podem rever suas práticas de trabalho e com isso, desenvolver estratégias especificas para promover saúde e bem-estar para as suas colaboradoras.

Cox (2021) ressalta que, as mulheres são mais suscetíveis a desenvolver a Síndrome de *Burnout*, o que pode afetar negativamente a produtividade e o bem-estar delas no trabalho. Segundo o autor, esse aumento está relacionado a diversos fatores, dentre eles está a pandemia e o isolamento social, que resultou na alteração da forma de trabalho sendo alterada do modelo presencial para o modelo *home-office*.

Para gerar soluções, Souza (2022), aponta três iniciativas que as empresas podem adotar para contribuir com a melhora da saúde mental das mulheres, são elas: *empatia, flexibilização e estabelecer limites saudáveis no trabalho*.

Para o autor a empatia consiste em ouvir com atenção ao invés de replicar visões estereotipadas sobre as mulheres e assumir o que elas precisam para terem mais saúde, performance,

e satisfação, levando em conta o que a pessoa fala e expressa, afinal o objetivo é que os líderes reconheçam as emoções e percepções como válidas e autenticas, criando um ambiente adequado para que o diálogo ocorra de forma franca e saudável.

Já a flexibilização, se faz necessário por compreender que incessantemente as mulheres se sentem angustiadas e sobrecarregadas em suas atividades diárias, sem ter a oportunidade de negociar prazos, metas e expectativas, com o acesso à tecnologia e a inserção de autonomia permite que haja flexibilidade na maneira como o trabalho é desenvolvido.

Por fim, a terceira iniciativa é estabelecer limites saudáveis no trabalho, em razão de fatores culturais as mulheres têm tendência a assumirem grandes demandas de atividades, sendo elas pessoais e profissionais pela dificuldade em dizer "não", pelo constrangimento e medo de frustrar outras pessoas e pela insegurança de ser criticada ou mal avaliada.

Deste modo as organizações podem desempenhar um papel de apoio ajudando as mulheres a desenvolverem novas habilidades de comunicação, inteligência emocional e liderança, tais incentivos ajudam na expectativa de se sentirem seguras e se posicionar com clareza, estando confortável em expor suas opiniões e definir seus limites.

Pensar no bem estar dos profissionais no ambiente de trabalho não é necessariamente uma novidade, como apresenta a pesquisa Gupy (2021), 37,7% das companhias já adotam benefícios voltados para melhorar e contribuir com a saúde mental de seus colaboradores, tendo como exemplo a seguradora Porto Seguro que para manter a saúde mental do time, oferece participações em projetos como corridas de rua, aulas de dança, *pilates*, *Muay Thai*, violão e gaita, bem como mensalidades de academia, acupuntura e ingressos para festivais gastronômicos além de contar com um suporte do "Alô Saúde", com profissionais disponíveis 24 horas.

O que se coloca como uma iniciativa inovadora é reconhecer que há distinção entre as realidades dos diferentes gêneros e aplicar um tratamento justo não necessariamente está relacionado com ‘igualdade’, mas sim, com o reconhecimento dos valores, situações e pensamentos, desta forma, as estratégias empresariais e o endomarketing serão realmente eficazes.

3. Metodologia

Considerando os diversos impactos decorrentes das relações entre as questões econômicas e a saúde mental no contexto laboral, surge o seguinte questionamento: "Como a

Síndrome de *Burnout* tem afetado as mulheres que atuam nas empresas situadas em Santana de Parnaíba?"

E é por esta razão que o estudo busca analisar as consequências do esgotamento profissional em colaboradoras, que, além de cumprir a carga horária na empresa, dividem seu tempo também entre atividades domésticas e maternas, exercendo uma tripla jornada ou até ‘quádrupla’ quando por exemplo, necessitam estudar para se manter relevantes no mercado.

Em prol do objetivo geral, são objetivos específicos: identificar as causas da Síndrome de *Burnout* e possíveis soluções para reduzir o número de ocorrências nas empresas.

A construção teórica possibilita não só apresentar, como também compreender a correlação entre as atividades profissionais e as responsabilidades cotidianas das mulheres, observando como está tríplice ou quadrupla jornada as torna mais susceptíveis ao desenvolvimento da Síndrome de *Burnout*.

Para as empresas, entender as causas, possibilita desenvolver estratégias para melhorar a o clima e o comportamento organizacional, além da promoção de ações substanciais à geração de condições para a manutenção da saúde mental e o bem-estar de seus funcionários.

A metodologia aplicada baseia-se no caráter qualitativo, que de acordo com Souza (2018) é uma abordagem de pesquisa que busca compreender e interpretar fenômenos sociais e culturais, através da coleta e análise de dados não estruturados, como entrevistas, observação participante e análise de documentos.

A coleta de dados foi pautada em duas ferramentas complementares, a primeira, entrevista direcionada com profissional diagnosticada com *Burnout*, por psiquiatra (profissional capacitado para tais diagnósticos), e segunda ferramenta, questionário fechado direcionado à respondentes da região de Santana de Parnaíba, investigando causas comuns.

O questionário fechado (Apêndice A), apresentava as opções de 'autorreconhecimento', sendo elas: homem transgênero, homem cisgênero, mulheres transgênero, mulheres cisgênero e outros, quando 'homem transgênero', 'homem cisgênero' e 'outros' foram selecionados, os questionários foram automaticamente ‘descartados’ uma vez que, a proposta do estudo é específica às mulheres.

Além desta prerrogativa, o questionário foi pensado para identificar a ‘percepção’ das profissionais quanto ao seu relacionamento com o trabalho e os ‘papéis sociais e

profissionais' das respondentes. Distribuídos sob as características: gênero, idade, estado civil, se possui filhos, satisfação com o trabalho e relações interpessoais.

Os limites demográficos consideram que a cidade de Santana de Parnaíba, enquadra-se no perfil estabelecido para a referente pesquisa, por ser uma região metropolitana, cujo desenvolvimento industrial e comercial está em ascendência, portanto considerada uma cidade em transição.

4 Análise e Interpretação dos Resultados

A pesquisa de campo foi realizada por meio da plataforma *Google Forms*, a pesquisa contava com 17 proposições de múltipla escolha (Anexo A). O questionário foi pensado para identificar a 'percepção' das profissionais quanto ao seu relacionamento com o trabalho, distribuídos sob as características de gênero, idade, estado civil, se possui filhos, satisfação com o trabalho e relações interpessoais.

Após a análise dos dados, constatamos a participação de 36 respondentes, com uma exclusão de 19,4% de indivíduos do gênero masculino.

A partir da apuração dos dados, das 29 mulheres respondentes, 55,2% sendo solteiras, 41,4% casadas e 3,4% divorciadas, conforme aponta a Figura 1:

Das respondentes, 41,4% mulheres apontaram ter filhos, 8,3% se classificam como divorciadas com filhos, seguido de 25,0% solteira com filhos; e 66,7% casadas com filhos. Essa questão demonstrou que entre as entrevistadas, solteiras e casadas sobressaíram na apuração dos resultados, conforme indica a Figura 2.

Figura 1: Estado Civil

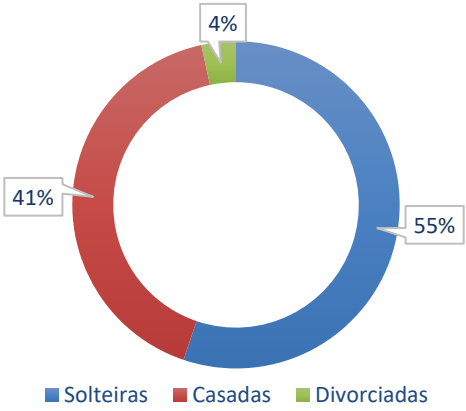
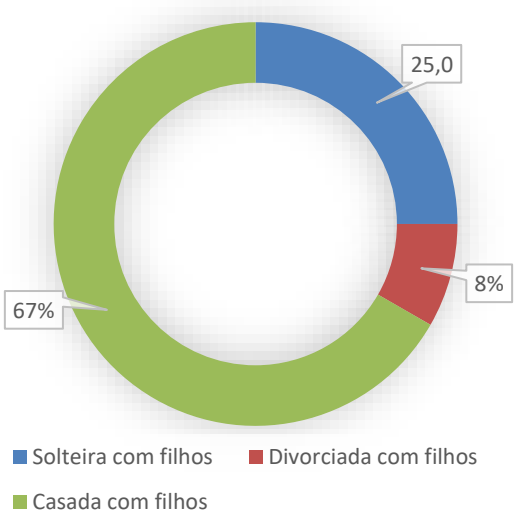
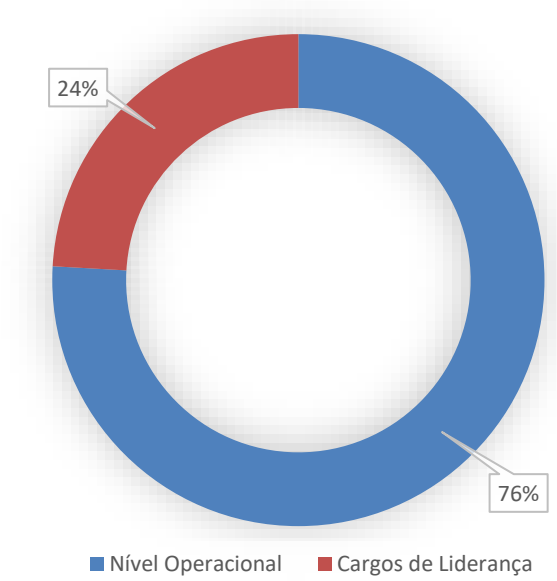


Figura 2: Distribuição sobre Filhos



Na apresentação da situação profissional (Figura 3) a pesquisa apresentou que 75,9 % das mulheres atuam no operacional e 24,1% em cargos de liderança, o que reforça inclusive uma consideração de que os cargos são tendenciados conforme o gênero.

Figura 3:Situação Profissional

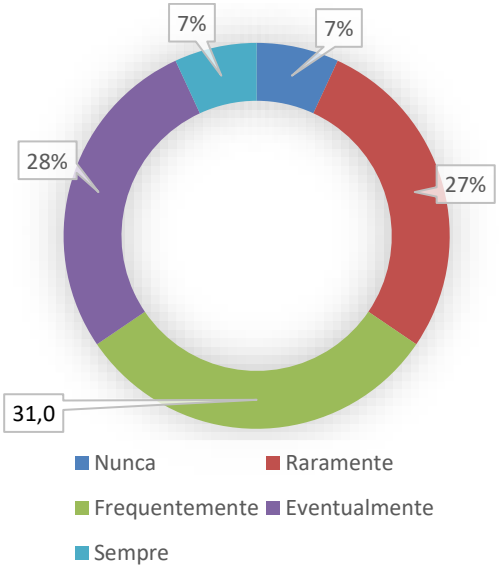


Analisando as percepções em relação ao trabalho, observa-se que diferentes estados de esgotamento são relatados pelas mulheres. Cerca de 31,0% delas afirmam sentir-se frequentemente esgotadas ao final do dia, o que é considerado uma característica negativa da jornada de trabalho.

Por outro lado, 27,6% relatam sentir-se raramente ou eventualmente esgotadas no final do dia, indicando uma ocorrência menos frequente dessa sensação de exaustão. Curiosamente, 6,9% das mulheres afirmam sempre se sentirem

esgotadas ao final do dia, apontando para um estado de exaustão constante. Esses dados podem ser investigados por meio das questões relacionadas ao estado das mulheres no ambiente de trabalho, conforme apresentado na Figura 4.

Figura 4:Distribuição sobre o esgotamento no trabalho



Os dados coletados fornecem *insights* sobre as tendências de comportamento e desempenho dos funcionários dentro da organização. Essas informações são valiosas para as empresas, pois permitem elaborar campanhas de endomarketing, estratégias de gestão de comportamento interno e medidas de prevenção e gestão do esgotamento, como programas de bem-

estar, políticas de equilíbrio entre trabalho e vida pessoal, incentivo a pausas regulares e apoio psicossocial. Isso evita os impactos negativos na produtividade, motivação e bem-estar dos colaboradores.

Essa abordagem proativa pode contribuir para a criação de um ambiente de trabalho saudável, aumentando a retenção de talentos, a produtividade e a satisfação geral no local de trabalho.

A relação entre a falta de energia para executar as tarefas do dia a dia, que é raramente observada, e a dedicação predominante das mulheres ao trabalho doméstico pode ser avaliada como um fator relevante no que diz respeito à quantidade de responsabilidades cotidianas e à possibilidade de desenvolver a Síndrome de *Burnout.*

Além disso, foi captado um depoimento da moradora do bairro Cidade São Pedro em Santana de Parnaíba, cujo nome não quis que fosse divulgado, portanto foi atribuído um nome fictício ‘Maria’, e que teve sintomas parecidos com os sintomas de pessoas que foram diagnosticadas com a Síndrome de *Burnout*.

O método usado foi a elaboração de quatro questões para que a participante respondesse com base no que foi vivenciado, conforme Figura 5.

Figura 5:Questões da Entrevista

PERGUNTAS
O que a levou ao médico?
Como foi o diagnóstico e quais foram os sintomas presenciados?
Qual processo de tratamento?
Como se sentiu após a realização do tratamento?

A respondente aqui chamada de Maria, apresenta um quadro de Síndrome de *Burnout* desde 2019, permanecendo em acompanhamento médico, antes do seu diagnostico, teve como principais sintomas: batimentos cardíacos acelerados, frio na barriga, tremor, fadiga, e estresse constante. Esses sentimentos vinham quando Maria sentia-se pressionada a exercer atividades com prazos curtos de entrega ou quando era fora de sua zona de conforto.

Ao analisar as respostas, pode-se notar que os motivos que a levaram a procurar ajuda médica foram uma intensa crise de ansiedade, ao ponto de ter que ser carregada, pois estava

incapaz de caminhar devido ao tremor. Além disso, havia choro, medo de morrer e a sensação de estar sofrendo um infarto. Em paralelo com o levantamento teórico sobre as condições de trabalho, é evidenciado que o ambiente de trabalho exerce um impacto direto na saúde mental dos colaboradores.

Na entrevista estruturada e na pesquisa realizada pelo *Google Forms*, foram analisados os sentimentos de apreensão quando lembrado da rotina de trabalho, bem como a dificuldade de desligamento da empresa após o término da jornada de trabalho, e insônia causada por pensamentos em tarefas e prazos do trabalho. Esses sentimentos podem ser observados nas seguintes falas da entrevistada Maria: "quando no serviço me sentia pressionada a exercer atividades com prazos curtos de entrega, ou quando era fora da minha zona de conforto", "algumas vezes tinha medo de ir trabalhar".

5 Conclusões

O objetivo do presente estudo foi analisar as consequências do esgotamento profissional em colaboradores, identificar as causas da Síndrome de *Burnout* e propor possíveis soluções para reduzir o número de ocorrências nas empresas, com um foco específico na

prevalência entre mulheres que atuam no mercado de trabalho. Durante a análise, foram considerados os possíveis fatores de risco e as consequências enfrentadas pelas mulheres, especialmente aquelas que lidam com a aglutinação de várias tarefas, tanto domésticas quanto profissionais.

Embora não tenhamos identificado um perfil específico com maior probabilidade de desenvolver a síndrome, estudos anteriores sugeriram que mulheres casadas e com filhos podem estar mais propensas a apresentar sinais de *Burnout*. Essa correlação pode ser atribuída à sobrecarga de responsabilidades, pois essas mulheres muitas vezes precisam conciliar múltiplos papéis, como cuidar da casa, da família e se destacar no ambiente de trabalho.

No entanto, é importante ressaltar que esses fatores não são determinantes e cada indivíduo pode vivenciar a síndrome de maneira única. Portanto, é fundamental analisar o contexto individual de cada mulher e considerar outros fatores como a cultura organizacional, o ambiente de trabalho e as demandas específicas de cada função.

Para uma abordagem mais eficaz, pesquisas futuras devem investigar outras organizações empresariais, a fim de coletar dados adicionais e comparar os resultados com empresas que já possuem uma política organizacional que demonstre preocupação e cuidado com o bem-estar das colaboradoras. Dessa forma, será possível obter uma compreensão mais completa dos fatores que contribuem para a ocorrência da Síndrome de *Burnout* entre as mulheres e identificar possíveis mudanças positivas nas organizações de trabalho.

Para promover o desenvolvimento das empresas e o bem-estar das colaboradoras, é essencial implementar campanhas de Endomarketing que engajem e conscientizem as mulheres sobre a importância da saúde mental. Além disso, é necessário contar com o auxílio contínuo de profissionais da área da saúde, a fim de identificar situações de risco à saúde mental e estabelecer um sistema de planejamento organizacional eficiente, no qual a ‘pressão por resultados’ não se torne uma característica de ambientes tóxicos de trabalho.

Em conclusão, os dados analisados indicaram que as pessoas entrevistadas estão propensas a desenvolver a Síndrome de *Burnout*, conforme evidenciado pelos seus efeitos físicos, mentais, profissionais e sociais. Para obter um entendimento mais abrangente, é necessário ampliar o estudo e obter mais dados, a fim de correlacionar a ocorrência da Síndrome de *Burnout* entre as mulheres e as possíveis mudanças positivas nas organizações de trabalho, visando manter um clima organizacional e funcional que promova o bem-estar das colaboradoras.

Referencial Bibliográfico

Acker, J. (1990). Hierarchies, Jobs, Bodies: A Theory of Gendered Organizations. Gender and Society, 4(2), 139–158. http://www.jstor.org/stable/189609

Agência IBGE. (2020). Em média, mulheres dedicam 10,4 horas por semana a mais que os homens aos afazeres domésticos ou ao cuidado de pessoas. Editora Estatísticas Sociais. São Paulo. https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27877-em-media-mulheres-dedicam-10-4-horas-por-semana-a-mais-que-os-homens-aos-afazeres-domesticos-ou-ao-cuidado-de-pessoas

Alves, M. de Abreu. (2016). Estresse no Trabalho: Entrevista cedida para o Portal Minha Vida. Psicólogas em São Paulo. https://www.marisapsicologa.com.br/estresse-no-trabalho.html#:~:text=A%20press%C3%A3o%20 do%20trabalho%20

pode,compulsivo%2C%20a%20depress%C3%A3o%2C%20etc

Beauvoir, S. (1949). O Segundo Sexo. Paris, France: Gallimard. https://edisciplinas.usp.br/pluginfile.php/3959829/mod_resource/content/1/Beauvoir.O_segundo_sexo-DIFEL.pdf

Coelho, C. dos S. (2020). Qual o nível de *Burnout* da amostra de profissionais do contexto financeiro. Associação de Politécnicos do Norte (APNOR). Instituto Politécnico de Porto. https://recipp.ipp.pt/bitstream/10400.22/17402/1/Cl%c3% a1udia_Coelho_MGO_2020.pdf

Cox, J. (2021). Porque mulheres sofrem mais de síndrome de *Burnout* do que homens. BBC News Brasil. São Paulo. https://www.bbc.com/portuguese/geral-58869558

Datasenado. (2022). Pandemia aumenta o número de brasileiros com experiência em teletrabalho. https://www12.senado.leg.br/institucional/datasenado/publicacaodatasenado?id=pandemia-aumenta-o-numero-de-brasileiros-com-experiencia-em-teletrabalho

Decreto Legislativo Nº 6 (2020). https://legislacao.presidencia.gov.br/atos/?tipo=DLG&numero=6&ano=2020&ato=b1fAzZU5EMZpWT794

França, A. C. L., & Rodrigues, A. L. (2011). Stress e trabalho: uma abordagem psicossomática. São Paulo: Atlas.

Fundação Instituto De Administração - FIA. (2020). Pesquisa Gestão de Pessoas na Crise COVID-19 Relatório Final. https://jornal.usp.br/wp-content/uploads/2020/11/Pesquisa-Gest%C3%A3o-de-Pessoas-na-Crise-de-Covid-19-ITA.pdf

Gupy. (2022). Saúde mental para colaboradores: Veja as dicas da Gupy. https://www.gupy.io/blog/saude-mental-para-colaboradores

IBGE. (2020). Indicadores IBGE: Contas nacionais trimestrais. https://biblioteca.ibge.gov.br/visualizacao/periodicos/2121/cnt_2020_4tri.pdf

International Stress Management Association - ISMA BR. (2018). Viver melhor: trabalho, stress e saúde. http://www.ismabrasil.com.br/ congressos/congresso-2018

Lima, L. P. (2022). Como superar a crise no setor de serviços em tempos de pandemia. https://www.ufrgs.br/coronaviruslitoral/como-superar-a-crise-no-setor-de-servicos/

Lopes, C. S., Menezes, P. R., Pastor-Valero, M., & Valente, M. S. S. (2016). Condições psicossociais de trabalho e *Burnout* entre bancários brasileiros: um estudo transversal. The Annals of Occupational Hygiene, 60(5), 567–580. https://doi.org/10.1093/annhyg/mew013

Mckinsey & Company. (2022). Mulheres no local de trabalho 2021. https://www.mckinsey.com/featured-insights/diversity-and-inclusion/women-in-the-workplace

Ministério Da Saúde. (2022). Síndrome de *Burnout.* https://www.gov.br/saude/pt-br/assuntos/saude-de-a-a-z/s/sindrome-de-Burnout/sindrome-de-Burnout

Ministério Público Do Estado Do Piauí. (2020). Guia Prático Sobre a Síndrome de *Burnout.* https://www.mppi.mp.br/internet/wp-content/uploads/2020/09/Ebook_Guia-pra%CC%81tico-sobre-a-Si%CC%81 ndrome-de-Burnout-2.pdf

Organização Mundial De Saúde - OMS. (2020). O impacto do COVID-19 nos profissionais de saúde e de assistência: um olhar mais atento às mortes. https://apps.who.int/iris/handle/10665/345300?search-result=true&query=Burnout&scope=&filtertype_0=author&filter_relational_operator_0=equals&filter_0=World+Health+Organization&rpp=10&sort_by=score&order=desc

Sá, V. V., de Morais, L. P., Fernandes, L. A. S., Tarlé, L. D. S. N., Verdin, M. P., de Melo Matos, M. L. & Caldeira Filho, M. L. (2022). A Síndrome de *Burnout* e os profissionais de saúde durante a pandemia de Covid-19: uma revisão narrativa. Revista Eletrônica Acervo Saúde, 15(1), e9518-e9518.

Saraiva, M. L. (2022). Como 8 empresas atuaram na pandemia para preservar o bem-estar e a saúde mental de seus colaboradores. https://forbes.com.br/carreira/2021/08/como-8-empresas-atuaram-na-pandemia-para-preservar-o-bem-estar-e-a-saude-mental-de-seus-colaboradores/

Setor Saúde. (2023). As mulheres e a Síndrome de *Burnout*. https://setorsaude.com.br/as-mulheres-e-a-sindrome-de-SÍNDROMEDE BURNOUT/

Souza, A. C. (2022). Saúde mental das mulheres: o que as empresas podem fazer. https://vocerh.abril.com.br/coluna/ana-carolina-souza/saude-mental-das-mulheres-o-que-as-empresas-podem-fazer/

Souza, P. M. (2018). Metodologia Qualitativa de Pesquisa: Possibilidades e Limitações. Revista Eletrônica Lato Sensu, 4(1), 1-16. http://www.latosensu.faccamp.br/index.php/revista/ article/view/268

Tamayo, M. R., & Tróccoli, B. T. (2002). Exaustão emocional: relações com a percepção de suporte organizacional e com as estratégias de coping no trabalho. Estudos de Psicologia (Natal), 7(1). https://doi.org/10.1590/S1413-294X2002000100005

Apêndice A: Questões aplicadas referente a Síndrome de *Burnout*

Síndrome de *Burnout*. Olá! Somos aluno(a)s do quarto semestre da Faculdade de Tecnologia de Santana de Parnaíba. Acreditamos que você pode nos ajudar na nossa pesquisa de campo; posteriormente, na relação de nossas empresas e colaboradoras, apenas respondendo dez perguntas a respeito da sua rotina de trabalho. Atenção! Este formulário tem como finalidade obter dados da Síndrome de *Burnout* [1] em mulheres no município de Santana de Parnaíba, dados estes que serão usados em nosso trabalho Programa de Integração Multidisciplinar em Tecnologia (PRIMT) e para o Trabalho de Graduação (TG), tendo proteção total de seus dados e imagem. [1]Síndrome de *Burnout* de acordo o Ministério da Saúde (2020) é um distúrbio emocional com sintomas de exaustão extrema, estresse e esgotamento físico resultante de situações de trabalho desgastante, que demandam muita competitividade e responsabilidade.

QUESTÕES	ALTERNATIVAS
Qual sua identidade de gênero?	( ) Homem Transgênero ( ) Homem Cisgênero ( ) Mulher Transgênero ( ) Mulher Cisgênero ( ) Outros
A que faixa etária você pertence?	( ) 18 – 25 ( ) 26 – 31 ( ) 32 – 39 ( ) 40 – 50
Qual seu e estado civil?	( ) Casado (a) ( ) Divorciado (a) ( ) Solteiro (a) ( ) Separado (a) ( ) Viúvo (a)

QUESTÕES	ALTERNATIVAS
Em qual setor você trabalha?	( ) Administrativo ( ) Recursos Humanos ( ) Setor comercial ( ) Setor operacional ( ) Outros
Você exerce algum cargo de liderança?	( ) Sim ( ) Não
Quantas horas você faz em sua jornada semanal?	( ) Até 30 horas semanais ( ) De 31 a 44 horas semanais ( ) Acima de 44 horas semanais
Você tem filhos?	( ) Sim ( ) Não

QUESTÕES	ALTERNATIVAS
Sinto-me decepcionado (a) com meu trabalho?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Ao final do dia de trabalho sinto-me esgotado (a)?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Quando pela manhã lembro da minha rotina de trabalho, já me sinto esgotado (a)?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre

QUESTÕES	ALTERNATIVAS
Sinto-me muito enérgico (a)/ motivado(o) no meu trabalho?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Sinto que estabelecer uma comunicação com meus colegas e clientes tem sido estressante?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Após o trabalho sinto-me sem energia para executar as tarefas do dia a dia?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre

QUESTÕES	ALTERNATIVAS
Tenho a sensação de estar conquistando muitas coisas no meu trabalho?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Sinto-me como se estivesse no limite de minhas possibilidades?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre
Consigo desligar-me da empresa por completo quando acabado minha jornada de trabalho?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre

QUESTÕES	ALTERNATIVAS
Costumo ter insônia por conta do trabalho?	( ) Nunca ( ) Raramente ( ) Frequentemente ( ) Eventualmente ( ) Sempre

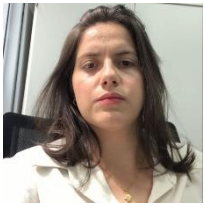
Autores deste Capítulo

Janete Almeida Carriel

Atua como Gerente Administrativa com vasta experiência em vendas e liderança de equipe. Ao longo de sua carreira, obteve grandes resultados, como o crescimento da empresa e a expansão da carteira de clientes. Ela é conhecida por sua habilidade conciliadora, buscando manter um bom relacionamento com a equipe e garantir a satisfação dos clientes. Cursou Gestão Comercial na Fatec Santana de Parnaíba em 2023 e teve o privilégio de contribuir para o desenvolvimento de um artigo científico, tornando-se um meio de compartilhar conhecimento. Inspirada por essa experiência, ela deseja continuar estudando e obter uma segunda graduação, reconhecendo a importância de se destacar no mercado de trabalho

Beatriz de Lima Cunha

Formada em Gestão Comercial, adquirindo vivência profissional na área de gestão de equipes. Hoje, busca-se o equilíbrio e defende a importância de uma vida saudável, tanto no âmbito profissional quanto pessoal. Determinada a fazer a diferença, inspira outras mulheres a encontrarem seu espaço e lutarem pelos seus direitos. A jornada está apenas começando, ansiosa para enfrentar os desafios que o futuro reserva

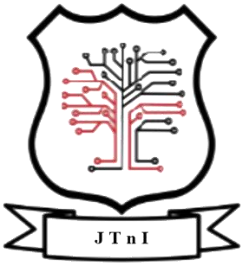


Giovanna Oliveira Pina

Escrever é sua paixão e uma forma de expressar suas ideias e desafiar perspectivas estabelecidas. Acredita que a escrita tem o poder de convidar os leitores a refletirem sobre suas experiências pessoais. Conquistou reconhecimento no Projeto Tempos de Arte Literária (TAL), obtendo o primeiro lugar no ensino médio. Além disso, ela possui certificados de empreendedorismo pelo programa Empretec e de Gerenciamento de Processos pelo Six Sigma. Cursa Gestão Comercial na Fatec Santana de Parnaíba, o que complementa seu conhecimento sobre o tema abordado no artigo científico em questão. Por meio da escrita, Giovanna almeja inspirar, provocar reflexões e promover mudanças, compartilhando seu pensamento com o mundo

Jucelaine Lopes de Oliveira

Pesquisadora e Docente do Centro Estadual de Educação Tecnológica Paula Souza, unidade FATEC/JDI. Mestre em Administração pela Faculdade Campo Limpo Paulista, especialista em gestão estratégica de Negócio e Bacharel em Administração de Recursos Humanos. A atuação profissional conta com experiência profissional gerindo operações de Distribuição e gestão de parceiros, tem como foco atual os seguintes temas: Estratégia, Inovação, Desenvolvimento sustentável, Logística e Gestão e Pessoas. Professora coordenadora da Fatec Santana de Parnaíba desde 2020



CAPÍTULO 3

Logística Reversa das Lâmpadas Compactas e Tubulares

Marcos de Oliveira Morais

Francisco Paraguai de Souza Filho

Regina Elena de Medeiros

1. Introdução

A sociedade atual produz inúmeros produtos e os consome demasiadamente e, dentre estes, destaca-se os equipamentos eletroeletrônicos. Esse consumo descontrolado e em curto prazo deve-se também à obsolescência programada devido aos rápidos avanços das informações e da tecnologia, fazendo com que um produto seja substituído, mesmo em funcionamento, por outro mais tecnológico (Rossani & Naspolini, 2017; Oliveira et al., 2017).

Em virtude do crescente consumo e do cuidado com o meio ambiente, as organizações buscam reestruturar seus sistemas logísticos, cumprindo as diretrizes legais e agregando valor à imagem corporativa. Além das questões legais, há também as pressões sociais, portanto, as empresas do comércio eletrônico têm buscado realizar a logística reversa de forma eficiente, pois seus lucros também estão vinculados ao marketing estratégico e a imagem da empresa está relacionada com a satisfação do cliente durante o

processo de comercialização (Araújo et al., 2013; Schuinsekel et al., 2017).

O conhecimento da Logística Reversa e a educação relacionada ao descarte adequado do lixo eletrônico é precário, tendo em vista que publicidades e diálogos sobre o assunto são ausentes na população, apesar de que autoridades e consumidores já estão mais atentos quando se trata de descarte de lâmpadas em relação ao meio ambiente. Por isso, é preciso estruturar sistemas que atendam as metas impostas pela legislação (Silva et, al. 2021).

Os principais problemas encontrados são a falta de informação e educação da população, a falta de preocupação com a gestão e o gerenciamento destes resíduos por parte da sociedade e a dificuldade de desmontagem de alguns equipamentos. Contudo, tais equipamentos apresentam materiais de alto valor agregado e sua reciclagem completa é importante do ponto de vista da mineração urbana e da economia circular. As cooperativas de reciclagem desempenham um papel muito importante para a economia circular deste resíduo, pois podem passar a recebê-los e desmontá-los completamente,

além de dar destino correto a todos os materiais envolvidos (Santos et, al. 2022).

No entanto, existem alguns desafios a serem enfrentados e superados, como a diversidade de materiais em um mesmo componente e/ou produto, tornando-os complexos em termos de separação e trabalhabilidade e até mesmo rastreabilidade. Além disso, o design da maioria dos equipamentos eletroeletrônicos que não é projetado para facilitar a desmontagem, reaproveitamento e consequente reciclagem dos mesmos, o que torna esta etapa um desafio (Silveira; Santos; Moraes, 2019; Tansel, 2017; Santos et al., 2020).

2. Referencial Teórico

2.1. Logística Reversa

De acordo com Leite et al (2010) a revalorização da ecológica e da logística reversa dos bens de pós consumo, é entendida como a eliminação ou mitigação desse somatório de custos dos impactos no meio ambiente provocado pela ação nociva de produtos perigosos a vida humana ou pelo

excesso desses bens, agrega-se valor ecológico ao bem de pós consumo por meio do equacionamento de sua logística reversa. De modo que se recapture o valor correspondente a esses custos, nem sempre plenamente tangível.

Logística Reversa é uma temática atual, na qual passou a ser discutida por volta da década de 90, especialmente a partir da "Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento da Rio 92". Foi neste momento em que tal tema passou a ser tratado "como uma questão de política ambiental e relacionado a proposta de sustentabilidade" (Oliveira, 2021).

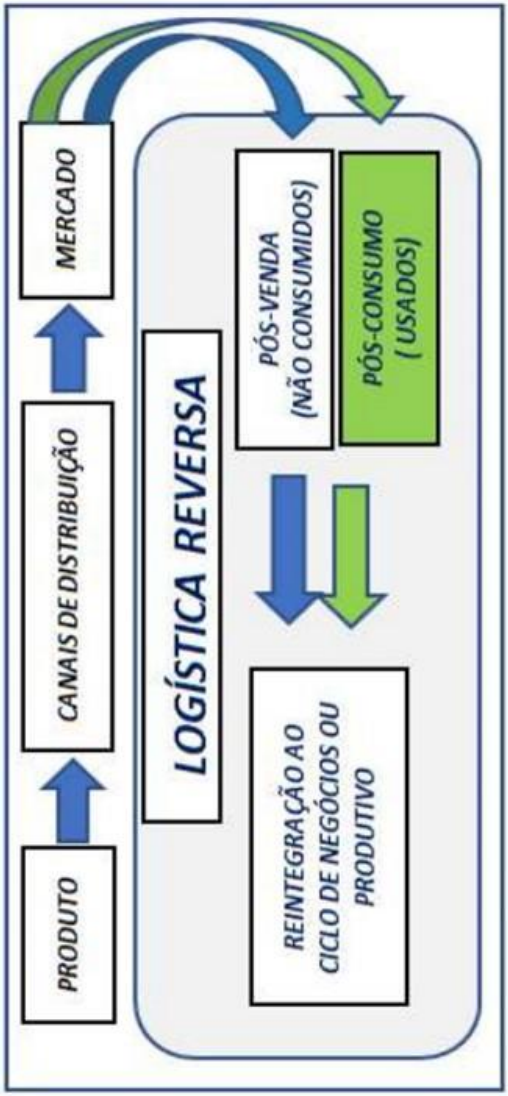
Segundo a ideia de Campos e Gourlart (2017), a logística reversa pode ser relacionada como uma poderosa estratégia competitiva, porque antes os produtos eram simplesmente descartados no meio ambiente, sendo prejudiciais aos seres humanos e ao meio ambiente. Agora passaram a ser reaproveitados e continuam no processo produtivo. Isto torna-se viável por razões econômicas e razões ecológicas, sendo assim o uso de material reciclável aumentando cada vez mais nas empresas, por consequência da sustentabilidade e legislações impostas pelo governo.

Melo Júnior et al. (2013) ressaltam que a logística reversa está ligada diretamente às questões ambientais, no que diz respeito à reciclagem, descarte e o gerenciamento de materiais contaminantes, incluindo atividades que possam gerar a redução de emissão, substituição, reciclagem, reutilização de materiais e descarte.

A logística reversa foi estabelecida como instrumento de desenvolvimento econômico e social, pela Política Nacional de Resíduos Sólidos no ano de 2010, compreendendo um conjunto de ações, procedimentos e meios destinados a viabilizar a coleta e o retorno dos resíduos sólidos ao setor empresarial após o seu consumo (Meireles E Moraes, 2020).

De acordo com Campos (2021), a rede de logística de retorno é a área de gestão de bens e materiais após a venda e consumo, devolvendo-os à sua origem, agregando-lhes valor de natureza diferente, incluindo o econômico, o ecológico, entre outros.

Figura 1: Logística Reversa baseado em Leite (2009)



A Logística Reversa pode ser concebida para atender modelos distintos de cadeias de abastecimento de materiais, podendo ser utilizado no mesmo produto, havendo integração da cadeia direta e reversa; assim como os materiais e componentes pós-consumo podem ser direcionados para outras cadeias de abastecimento diferentes da original e reutilizados para fabricar algo diferente do produto anterior (Aligleri e Lopes, 2022).

2.2. Logística Reversa para o Descarte de Lâmpadas

A logística reversa para o descarte de lâmpadas: as lâmpadas são extremamente perigosas e necessitam de uma destinação adequada após o seu consumo. Quando são descartadas incorretamente, acarretam diversos problemas tais como contaminar o meio ambiente, intoxicar os humanos e podem causar problemas físicos e neurológicos. A logística reversa se tornou fundamental e o tema vem crescendo muito no mercado de trabalho. A Política Nacional de Resíduos sólidos aprovou e com isso,

incentivou as empresas a lidarem com isso (VG Resíduos, 2018).

Segundo Vilarinho e Carvalho (2019), o crescimento do volume de resíduos sólidos gerados pela população, somados às questões socioambientais e aos custos suportados pelo Estado com o gerenciamento dos resíduos, são fatores que impulsionaram ações das autoridades públicas nesta área na última década. Como marco legal sobre gerenciamento de resíduos no Brasil, temos a Lei Federal 12.305/2010 (PNRS).

O setor de iluminação acompanha a tendência mundial da responsabilidade pós-consumo seguindo a LR, buscando tecnologias que contenham menor volume de Hg em sua composição e/ou livres dele, como exemplo as lâmpadas de LED, não gerando resíduo tóxico, podendo ser descartadas na reciclagem e aproveitando seus componentes e reduzindo custos (Apliquim, 2020).

As lâmpadas fluorescentes pós consumo são obrigadas a retornar aos seus fabricantes, para que providenciem a destinação final adequada. As lâmpadas são classificadas como resíduos perigosos, o descarte

inadequado desse material, pode causar problemas para a saúde da população e ao meio ambiente. Uma lâmpada tem a capacidade de contaminar até 15 mil litros de água ou uma piscina inteira, devido ao mercúrio encontrado em sua composição (Meireles e Moraes, 2020).

O processo de logística reversa contempla várias etapas anteriores que devem ser executadas permitindo assim que os resultados desejados sejam alcançados e as metas estabelecidas atendidas. Conforme Mansor et al (2015), O gerenciamento é o componente operacional da gestão de resíduos sólidos e inclui as etapas de coleta, transporte, tratamentos e disposição final.

3. Metodologia

A metodologia utilizada neste trabalho pode ser classificada como uma pesquisa-ação, que, segundo (Thiollent, 2014), "um tipo de pesquisa concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo no qual os pesquisadores e participantes representativos da situação ou

do problema estão envolvidos de modo cooperativo ou participativo".

A pesquisa enquadra-se como descritiva, que, segundo Gil (2002), tem por finalidade descrever as características de determinada população e identificar a relação entre as variáveis, possibilitando a construção de hipóteses, as realizações de pesquisas descritivas comumente são realizadas por pesquisadores preocupados com a prática.

Os dados coletados são referentes aos meses de Janeiro a Dezembro de 2022 perfazendo um período de 12 meses, onde os autores entendem que a amostragem para o processo de análise inicial torna-se relevante, proporcionando que se tenha uma comparação trimestral e semestral.

4. Análise e Interpretação dos Resultados

Os dados foram coletados na empresa "W" situada em São Paulo – SP, que surgiu a partir da assinatura da lei PNRS e de um acordo setorial para implementação do sistema de logística reversa de lâmpadas que contêm

mercúrio em sua composição. Em decorrência da PNRS, mais especificamente do conceito trazido de responsabilidade compartilhada pelo ciclo de vida dos produtos, o programa surgiu em novembro de 2014.

O acordo determina as diretrizes para operação da empresa "W", que prevê a redução no processo da geração de resíduos, tendo como proposta, melhorar a prática de hábitos de consumo cada vez mais sustentável e promover o aumento da reciclagem e economia circular de modo geral.

4.1. Ciclo de Destinação das Lâmpadas

Após serem recolhidas, as lâmpadas são separadas pelas tipologias tubulares e compactas. As tubulares são colocadas no britador de martelos, onde são quebradas. Após isso, passam por mais um processo para redução dos pedaços de vidro (granulometria). O material então é separado (vidro e partes metálicas) por meio de uma peneira vibratória.

As partes metálicas serão transportadas por meio de uma fosca transportadora e armazenadas em tambores para destinação final (reciclagem).

Já o vidro moído (com pó de fósforo é contendo mercúrio), é levado por uma correia transportadora até um cilindro rotativo que ajuda na separação do vidro do pó de fósforo através do atrito do vidro. É então lançada uma corrente de ar *scrubber* com o intuito de arrancar o pó de fosfórico par afora do cilindro.

Assim, o vidro limpo é recolhido e armazenado em bombonas para futura reciclagem, enquanto o pó fosfórico contendo mercúrio é direcionado para o aero ciclone, enquanto isso o ar limpo sai do ciclone e encaminhado para um filtro de mangas para reter material particulado, e em seguida para um filtro de carvão ativado, com o objetivo de reter qualquer mínima quantidade de mercúrio o ar limpo é direcionado para a chaminé do sistema de exaustão.

Todo o processo é realizado em local enclausurado e o mercúrio evaporado é retido nos filtros de carvão ativo. Posteriormente, quando saturados, tais filtros são

destinados para aterros Classe I. A Figura 2 apresenta as lâmpadas dos modelos compacta e tubular.

Figura 2: Modelos de Lâmpadas. Fonte: os autores.

Modelo Compacta

Modelo Tubular

As lâmpadas compactas são manuseadas para unidades para quebra do vidro e obtenção do bulbo para descaracterização dos componentes: metais, boquilhas e plásticos. O vidro quebrado é depositado em tambores de processamento que trabalham sob processo de exaustão. Em outro recipiente é obtido o bulbo, onde será separado as partes metálicas e outras para destinação. A Tabela 1 apresenta os resultados da coleta efetivados pela empresa no ano de 2022.

Foram coletados 450.284,40 kgs de lâmpadas compactas e 523.398,20 kgs de lâmpadas tubulares no ano somente pela empresa "W", tendo uma somatória de

973.673,60 kgs recolhidos em 2022, demonstrando que o processo de logística reversa permite proporcionar ganhos efetivos para o descarte correto deste resíduo, gerando agregar valor as necessidades ambientais assim como renda para as pessoas que trabalham nas cooperativas e empresas afim.

Tabela 1: Quantidade de Lâmpadas: Fonte: os autores.

Quantidade de Lâmpadas Coletadas em 2022			
Meses	Kg ‘s Compactas	Kg ’s Tubulares	Total Kg's
Janeiro	22.750,10	50.094,30	72.844,40
Fevereiro	21.880,10	48.351,90	70.232,00
Março	28.001,20	59.544,00	87.545,20
Abril	23.028,00	36.516,00	59.544,00
Maio	30.488,00	47.705,00	78.193,00
Junho	36.239,00	40.707,00	76.946,00
Julho	42.852,00	48.415,00	91.267,00
Agosto	48.933,00	49.740,00	98.673,00
Setembro	49.408,00	45.407,00	94.815,00
Outubro	53.543,00	37.034,00	90.577,00
Novembro	48.033,00	31.927,00	79.960,00
Dezembro	45.129,00	27.948,00	73.077,00
Total:	450.284,40	523.389,20	973.673,60

5. Conclusões

Diante dos resultados apresentados, a logística reversa para o descarte de lâmpadas apresenta um campo mais amplo para discussão, visto que há uma quantidade significativa de estudos disponíveis investigando seus supostos benefícios assim como as suas limitações. Os resultados coletados levam a demonstrar a viabilidade de utilização dessa técnica para minimizar os impactos ambientais assim como os aspectos sociais, gerando renda para as empresas que utilizam a logística reversa. A logística reversa conquista, a cada dia, uma maior participação nas empresas e também da sociedade.

Torna-se de extrema importância que se tenha uma introdução da logística reversa no cotidiano das pessoas, que também se torna necessário a estruturação de sistemas para auxílio e incentivo possibilitando criar e implementar programas coletivos para operacionalizá-la. A Política Nacional de Resíduos Sólidos passa a introduzir a divulgação desse assunto trazendo benefícios tanto para as empresas, quanto para o meio ambiente e a sociedade.

Pode-se dizer, portanto, que o objetivo deste trabalho foi alcançado, visto que foi possível compreender e visualizar os principais pontos da logística reversa de pós consumo, visando fomentar o assunto bem como a possibilidade de ampliação sobre outros temas relacionados a logística reversa e sustentabilidade nas organizações e na sociedade.

Referencial Bibliográfico

Aligleri, L., & Lopes, C. S. D. (2022). Logística Reversa de embalagens de pós-consumo: análise crítica interdisciplinar das intenções empresariais propostas no Termo de Compromisso do Recircula para cumprir a Política Nacional de Resíduos Sólidos. *Revista Brasileira de Políticas Públicas*, *12*(1).

Apliquim Brasil Recicle. (2020) Manual do Armazenamento de Lâmpadas Fluorescentes e que contém mercúrio.

Araujo, A. C. D., Matsuoka, É. M., Ung, J. E., Hilsdorf, W. D. C., & Sampaio, M. (2013). Logística reversa no comércio eletrônico: um estudo de caso. *Gestão & Produção*, *20*, 303-320.

BRASIL. Lei 12.305 (2010), Institui a Política Nacional de Resíduos Sólidos. Disp onível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/L12305.htm

Campos, A. (2017). *Logística reversa integrada: sistemas de responsabilidade pós-consumo aplicados ao ciclo de vida dos produtos*. Saraiva Educação SA.

Gil, A. C. (2002). Como elaborar projetos de pesquisa (Vol. 4, p. 175). São Paulo: Atlas.

Goulart, V. D. G., & de Campos, A. (2021). *Rede Logística de Retorno (RLR)*. Saraiva Educação SA.

Leite, M. S. A., de Lima, J. G., & Simoes, A. (2010). Mensuração dos custos em uma operação de logística reversa: o caso de uma empresa de artigos esportivos. *ABCustos*, *5*(2), 94-114.

Leite, P. R. (2009). Logística reversa. *Pearson. São Paulo*

Mansor, M. T. C. et al. (2015). Cadernos de Educação Ambiental: *Resíduos Sólidos*.

Meireles, J. F., & de Moraes, A. R. Logística Reversa De Lâmpadas Na Prática: Um Estudo de Caso no Município de Mundo Novo/MS.

Melo Júnior, T. A., Dândaro, F., Ambroseto, G., & Tabah, J. (2013). Estudo de Caso: coleta e logística reversa para lâmpadas fluorescentes no município de Franca, SP. *Revista Eletrônica em Gestão, Educação e Tecnologia Ambiental*, 2091-2101.

Moraes, V. T. D., Espinosa, D. C. R., & Lucena, L. L. (2014). Tecnologias de tratamento para resíduos de equipamentos eletroeletrônicos. *Gestão de resíduos eletroeletrônicos: uma abordagem prática para a sustentabilidade*.

Oliveira, J. D., Selva, V., de Mendonça Pimentel, R. M., & Machado, S. (2017). Resíduos eletroeletrônicos: geração, impactos ambientais e gerenciamento. *Revista Brasileira de Geografia Física*, *10*(5), 1655-1667.

Oliveira, T. G., de Mendonça Barros, M., da Costa, R. R., Rezende, D. C. V., da Cunha Rezende, S. D., Boscatti, L., ... & Rezende, A. L. D. L. S. (2021). Análise da logística reversa brasileira: a compreensão legal diante a gestão de resíduos com base no estudo da revisão da literatura. *Brazilian Journal of Development*, *7*(5), 50759-50774.

Recircula para cumprir a Política Nacional de Resíduos Sólidos. *Revista Brasileira de Políticas Públicas*, 12(1).

Rodrigues, R. C. S., Pinheiro, A. B. D., Souza, I. C., da Silva Augusto, R., & Nazaré, T. B. (2021). Logística Reversa para o Descarte se Lâmpadas. *Revista Mythos*, *15*(1), 58-72.

Rossini, V., & Naspolini, S. H. D. F. (2017). Obsolescência programada e meio ambiente: a geração de resíduos de equipamentos eletroeletrônicos. *Revista de Direito e Sustentabilidade*, *3*(1), 51-71.

Santos, E. C. A., Colling, A. V., Schaab, A., & Moraes, C. A. M. (2020). Avaliação da Influência do Design na Desmontagem de Lâmpadas LED do Tipo Bulbo Para Posterior Reciclagem. In *Forum Internacional de Resíduos Sólidos-Anais* (Vol. 11, No. 11).

Santos, E. C. A., da Silva, J. L. C., Evaldt, D. C., & Moraes, C. A. M. (2022). Beneficiamento de Lâmpadas LED Pós-Consumo Em Uma Cooperativa de Reciclagem de Resíduos Eletroeletrônicos. *MIX Sustentável*, *8*(4), 63-76.

Schuinsekel, É. O., Moura, R. C. F., & da Rosa Neto, E. (2017). Logística reversa de resíduos de equipamentos eletroeletrônicos e seus reflexos ao meio ambiente. *Revista GESTO*, *5*(3), 48-59.

Tansel, B. (2017). From electronic consumer products to e-wastes: Global outlook, waste quantities, recycling challenges. *Environment international*, *98*, 35-45.

Thiollent, M. J. M., & Colette, M. M. (2014). Pesquisa-ação, formação de professores e diversidade. Acta Scientiarum. Human and Social Sciences, 36(2), 207-216.

VG Resíduos. (2018). Como funciona a logística reversa pós-consumo de lâmpadas fluorescentes.

Vilarinho, R.; Carvalho, A. L. (2019). ConJur -Op inião: Logística reversa não é mais só uma tendência sustentável.

Autores deste Capítulo

Marcos de Oliveira Morais

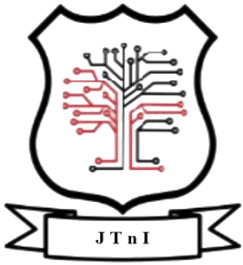
Pós Doutor em Engenharia de Produção com linha de pesquisa em gestão do conhecimento e inovação tecnológica. Qualidade e inovação. Doutor em Engenharia de Produção é Mestre em Engenharia de Produção, Pós-Graduado MBA em Gestão da Qualidade, em Engenharia de Produção, em Pedagogia Empresarial e Educação Corporativa, Formado em Gestão da Qualidade e com vasta experiência. Consultor e docente na área da Metal Mecânica, Gestão da Qualidade e Logística. Possui várias publicações científicas nacionais e internacionais. Atua como revisor das revistas Perspectivas Online, Exacta e Journal of Technology & Information. Co-autor de diversos livros

Francisco Paraguai de Souza Filho

Graduando em Administração de Empresas pelo Centro Universitário Estácio São Paulo, experiência nas áreas de Logística e *Supply Chain* em empresas de Materiais de Construção, atuando como conferente e atendimento ao fornecedor e ao público em geral. Realiza também controle de entrada e saída de materiais, além de atuar também com gestão de pessoas

Regina Elena de Medeiros

Possui graduação em Psicologia pelo Centro Universitário das Faculdades Metropolitanas Unidas, Especialização em Administração Escolar pelo Centro Universitário Ítalo Brasileiro, atualmente é Coordenadora do curso de graduação em Gestão de Recursos Humanos e Marketing, coordenadora adjunta da área de gestão e saúde, Coordenadora do curso de Especialização em Psicopedagogia e professora do Centro Universitário Estácio São Paulo. Atua como Administradora da Empresa *Alloytech* Com. Prod. Médicos e Odontológicos, respondendo pela área administrativa, comercial e financeira. Atuou como Pró-Reitora Administrativa e Acadêmica e como coordenadora de cursos técnicos em Gestão e Marketing. Tem experiência administrativa, com ênfase na área Comercial e Recursos Humanos. Atuação como Psicóloga Clínica.



CAPÍTULO 4

A Indústria 4.0 e os Aplicativos de Entrega de Alimentos

Camila França de Oliveira
Filipe Correa dos Santos Andrade
Gabrielly Nunes de Oliveira
Jéssica Aparecida Leal de Souza
Vanessa Lopes de Almeida
Marcos de Oliveira Morais

1. Introdução

Em 1957, durante a Guerra Fria, foi criada por pesquisadores militares do Estados Unidos a internet, tecnologia que permitia trocar e compartilhar informações de modo descentralizado, nascia a quarta revolução industrial, que foi batizada por Indústria 4.0, com integração de tecnologias de informação e comunicação, que permitiram alcançar novos patamares de produtividade, flexibilidade, qualidade e gerenciamento, possibilitando a geração de novas estratégias e modelos de negócio (Sacomano et. al., 2018).

As mudanças culturais ao longo dos anos, tais como: a globalização e inserção da mulher no mercado de trabalho, influenciaram no estilo de vida das pessoas inclusive nos costumes alimentares. As novas maneiras de compra e consumo possibilitaram a solicitação de alimentos virtualmente e entregues no local desejado pelo solicitante, pratica chamada de Delivery. (Magalhães, 2016).

Uma das características da modernidade é a falta de tempo e a pressa, bem como à ansiedade. A necessidade de

executar tudo de forma acelerada faz com que a alimentação também se enquadre nesse padrão. Por isso é a recorrente a busca por alternativas que possam tornar a alimentação mais prática e rápida, como *fast-foods*, serviços de *delivery*, restaurantes *self-service*, e consumo de alimentos industrializados (Magalhães, 2016).

Os serviços de entrega atualmente em domicílio (*delivery*) vêm crescendo de forma gradual no mercado, e se tornando um negócio de sucesso e vem influenciando e atingindo a cada vez mais novos consumidores, além de representar uma grande participação nos lucros da economia de um país (Silva, 2021).

Diante do exposto, o objetivo deste artigo está em verificar o crescimento da utilização de aplicativos de entrega de alimentos no auge da pandemia por Coronavírus (2020-2021), e ainda, examinar se após a flexibilização da pandemia causada pelo vírus da Convid-19, permitiu um crescimento na utilização dos aplicativos de entrega de alimentos, assim como identificar a faixa etária da população que mais utiliza os aplicativos de entrega de alimentos.

2. Referencial Teórico

2.1 O Início das Revoluções Industriais

A Revolução Industrial foi um período de grande desenvolvimento tecnológico que teve início na Inglaterra no século XVIII. O nascimento da indústria provocou mudanças importantes na economia mundial e no modo de vida da humanidade, acelerando a produção de bens e o uso dos recursos naturais (Bezerra, 2011).

Antes do surgimento da indústria, tudo era produzido de forma manual, fator que propiciava pequenas produções, e isso passava a ser inviável diante de uma população que crescia descontroladamente. Além disso, produzir mais rápido e em maior quantidade era a essência do capitalismo, que tinha como objetivo principal a obtenção de lucros (Cavalcante & Silva, 2011).

O método industrial de produção se espalhou por grande parte do hemisfério norte no século XIX e início do século XX. A adição de bens tornou- se mais barata e fácil, mas trouxe desordem à vida rural e danos ambientais. A produção mecanizada em larga escala desencadeou

mudanças nos países europeus e norte-americanos (Bezerra, 2011).

A Revolução Industrial caracteriza-se como um processo que levou à substituição de ferramentas por máquinas, à substituição da energia humana pela energia cinética e à substituição da produção artesanal pelo sistema industrial, possibilitou expandir o comércio internacional nos séculos XVI e XVII quando a riqueza da classe dominante capitalista cresceu consideravelmente. Isso permitiu acumular capital que poderia ser usado para financiar processos técnicos e os altos custos de instalações industriais (Bezerra, 2011).

2.2 As Fases das Revoluções Industriais

Nos primórdios da civilização, o ser humano usou a própria energia muscular para produzir trabalho, quando, muitas vezes, escravos eram usados para realizar tarefas repetitivas e que demandavam grande esforço (Sacomano et. al., 2018).

A primeira revolução industrial ocorreu em meados dos séculos XVIII caracterizou-se pelo aumento da

mecanização, que provocou mudanças significativas em quase todas as áreas da vida humana. Na estrutura socioeconômica, separou definitivamente o capital, representado pelos proprietários dos meios de produção, e o trabalho, representado pelos assalariados. Aboliu a antiga organização das sociedades, que era um método de produção artesanal. (Ramos, 1994).

A segunda fase da Revolução Industrial começou no final do século XIX, quando o aumento da produção de aço devido aos altos-fornos levou à produção de equipamentos e maquinários mais modernos que a madeira, uso de energia elétrica para fins industriais levou à produção (Sacomano et. al., 2018).

A terceira revolução industrial (1950-2010) foi marcada pela substituição gradual da mecânica analógica pela digital, pelo uso de microcomputadores e criação da Internet (1969) na época chamada pelo governo americano de Arpanet. Houve ainda, a crescente digitalização de arquivos e a invenção da robótica (Fante, 2021).

A quarta Revolução Industrial ou Indústria 4.0 tem seu termo usado pela primeira vez em 2011, é oriunda de

um projeto de estratégias do governo alemão votado para a tecnologia (Silveira, 2017).

Um dos pontos em comum entre as revoluções está a produção em massa que reduziu os custos de produção e, portanto, também o preço do produto para o consumidor, o que aumentou a participação da sociedade na compra de bens e serviços. Também levou à padronização de produtos, inflexibilidade para produzir de forma antidemocrática em empresas que tentam controlar todo o ciclo produtivo desde a matéria-prima até a venda dos produtos. O objetivo foi sempre produzir o mesmo produto para cada qualidade (Sacomano et. al., 2018).

2.3 Os Fundamentos da Indústria 4.0

Na quarta revolução Industrial, criada em 1957, durante a Guerra Fria entre a União Soviética e os Estados Unidos, a internet foi desenvolvida por pesquisadores militares do Estados Unidos que idealizaram um modelo que pudesse trocar e compartilhar informações de modo descentralizado, assim, um ataque russo às bases militares americanos não exporia informações sigilosas norte-

americanas, pois as mesmas estariam guardadas em diferentes locais (Sacomano et. al., 2018).

O antigo sonho de integrar os equipamentos as operações das empresas com os fornecedores através de eletrônicos tornaram cada vez mais realidade, novos softwares foram desenvolvidos com preços cada mais acessível (Sacomano et. al., 2018).

A Alemanha lançou uma Ferira de Hannover, a Plataforma Indústria 4.0 para desenvolver tecnologia e fazer com que os sistemas automatizados que controlam os equipamentos industriais pudessem se comunicar, modificando as informações de dados para que haja uma conexão otimizada entre o homem e as máquinas, plataforma, da Indústria 4.0 passou a ser divulgada em 2013, e foi relançada em 2015 como programa do governo alemão. (Hermann, Pentek & Otto, 2015; Sanders, Elangeswaran & Wulfsberg, 2016).

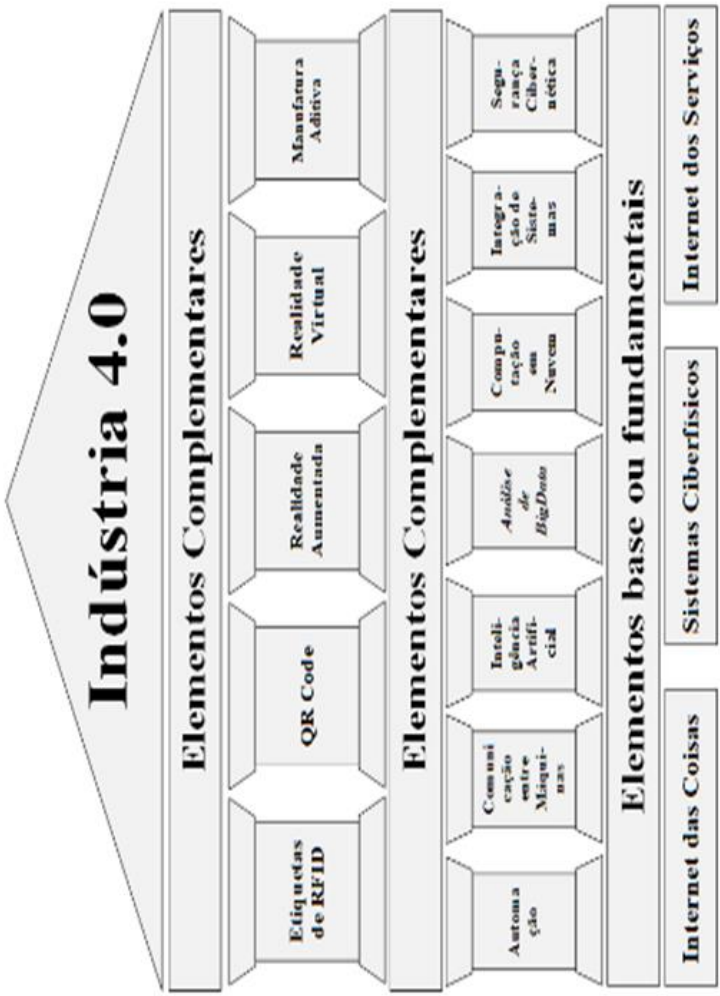
O processo envolvendo a quarta revolução industrial passa a ser irreversível visto que há uma interação e interface entre vários componentes permitindo a esta nova era uma maior complexidade, buscando cada vez mais

agilidade nos processos assim como a sua assertividade no processo decisório, essas tecnologias ainda auxiliaram na solução de problemas e melhoria na qualidade (Cheng. 2015).

A indústria 4.0 integra a tecnologia de informação e comunicação permitindo alcançar maiores produtividades, flexibilidades, qualidades e gerenciamentos, fazendo com que as novas estratégias e modelos de negócios agreguem a indústria chamando assim a Quarta Revolução Industrial (Sacomano et. al., 2018).

Sacomano *et al.* (2018) apresenta uma proposta para classificar os elementos que são a base formadora da indústria 4.0. Entende-se que não é uma formação definitiva, mas tem um caráter didático e concreto, conforme Figura 1.

Figura 1: A "Casa da Indústria 4.0" baseado em Sacomano et.al (2018).



2.4 A Transformação Digital e a Indústria 4.0

A transformação digital é inevitável e marcada por diversas quebras de paradigmas. Ao mesmo tempo em que resulta em desafios e aumento da competitividade, abre espaço para inúmeras possibilidades de criação de valor. O gigantesco avanço das tecnologias de informação e comunicação (TICs), em conjunto com novas tecnologias digitais, como a Internet das Coisas/*Internet of Things* (IoT), o *Big Data*, a Computação em Nuvem/*Cloud Computing*, a Inteligência Artificial/*Artificial Intelligence* (AI) e os sistemas Cyber-Físicos/*Cyber-Physical Systems* (CPS), sinaliza a transição de uma economia baseada emprodutos para outra baseada no fornecimento de soluções completas e personalizadas.

Nesse contexto, muitas empresas falham em criar real valor agregado para seus clientes –consequência por também falharem na gestão e no compartilhamento do conhecimento –e não conseguem recuperar recursos investidos em digitalização (Kamalaldin, Linde, Sjödin, & Parida, 2020).

O mercado se prepara nesse contexto para uma nova geração com consumidores digitais e assim são desenhadas estratégias de marketing (*bigdata*) e redes sociais. Os processos dos pedidos dos clientes se tornando automatizados programados automaticamente, podendo ter acesso as atualizações das etapas e customizar e realizar suas compras de forma flexível e remota. Os dados *bigdata* são gerados no processo industrial quanto no processo comercial, ele coleta as informações do comportamento do consumidor, após analisados são eficientes para otimizações, reduções de desperdícios, adequação à sustentabilidade e possíveis novos negócios (Sacomano et. al., 2018)

Para acessar os arquivos esses dados são armazenados ou processados em servidores que podem estar em diferentes localidades, essa troca remota ao mesmo tempo entre os servidores são identificadas como computação em nuvem. O objetivo dessa forma é tornar possível armazenar, processar e acessar os dados de qualquer lugar do mundo em que haja internet (Lira, 2020).

Poderão ser oferecidos aos clientes, ao que se chama de internet de serviços ou *Internet of Services* (IoS). Por exemplo, o seu despertador inteligente poderia tocar antes do horário, pois recebeu a informação de que o caminho que você normalmente segue para o trabalho está congestionado e requer que você acorde antecipadamente. Sugestões da inteligência artificial deverá dar apoio nas decisões lógicas e estratégicas nas organizações, mas o executivo deverá saber filtrar quando será preciso identificar a necessidade de contrariar sugestões de decisões feitas por inteligência artificial (Sacomano et. al., 2018).

2.5 Conectividade de Aplicativos e a Indústria 4.0

Atualmente o conceito de indústria 4.0 vai muito além de ser apenas industrial, vale também para as novas tecnologias que surgiram no mercado com o passar dos anos, a conectividade e inteligência artificial vem ganhando o mercado através da (Iot) e (IOS). Dentro deste aspecto podemos destacar os pilares que são: Ciber segurança, Realidade Aumentada, Big Data, Robótica Autônoma, Impressão 3D, Simulação, Integração de Sistemas,

Computação em nuvem e Internet das Coisas. (Furtado, 2017).

A conectividade realizada por exemplo através de smartphones são verdadeiros bancos de dados e fontes de informações para o desenvolvimento e criação de produtos, serviços e negócios em todas as esferas, telefonia, compras online, redes sociais, eletrônicos, comunicação, máquinas e entretenimento (Magrani, 2018).

A IoT tem o potencial de facilitar a vida humana em sua conectividade e consequentemente as empresas e indústrias foram beneficiadas com novas oportunidades, modelos de negócios e redução de custos outrora indispensáveis oferecidos através do trabalho humano, além de auxiliar na tomada de decisões e melhoria na produtividade nas áreas de varejo, agricultura e manufatura. Além destes benefícios o lado humano sofrerá grandes melhorias nas áreas de segurança, saúde, mobilidade, conectividade com social, e o empenho de energia. (Guerra, 2000).

2.6 Aplicativos de Entrega de Alimentos

As empresas de aplicativo de delivery funcionam como prestadora de serviço terceirizada, onde ela é a responsável por intermediar a ligação entre o usuário (cliente) cadastrado em sua plataforma, com produtor (Restaurante e Bar) e os entregadores (moto boys). Em todas as etapas os aplicativos de entrega incluem taxas de serviço e entrega, além de políticas de serviço para que o sistema funcione de forma adequada para todos os usuários cadastrados (Ponte, 2016).

Os aplicativos de entrega de comida (*Delivery*) estão no dia a dia da população brasileira, por conta de sua facilidade e praticidade, vale ressaltar que o Brasil é responsável por 50% do mercado de delivery alimentício na América Latina, podemos notar que como parte deste efeito bares e restaurantes que aderiram ao delivery via plataforma de aplicativo (Ponte, 2016).

Grande parte da ascensão deste mercado também está relacionada aos efeitos causados pela COVID -19 onde no ano de 2021 com parte da população ainda em isolamento social a atividade de delivery em Bares e

Restaurantes registou um crescimento de 187% movimentado aproximadamente R$ 35 bilhões segundo a Abrasel (Massa, 2022).

Entre os principais aplicativos de entrega temos o *Rappi*, James, Uber *Eats*, *Appetit Delivery*, porém devemos destacar o maior aplicativo de entregas e líder de mercado que é responsável por atender 80% do mercado brasileiro o I food presente em milhares de cidades no Brasil e também na América Latina como Argentina, Colômbia e México com 270 mil restaurantes parceiros, 160 mil entregadores e 60 milhões de entregas em março de 2021 (iFood, 2022).

3. Metodologia

O presente trabalho é de natureza qualitativa (Martins, & Theóphilo, 2016) e o emprego da metodologia de pesquisa bibliográfica, realizada pelo levantamento da dados em fontes secundárias, a qual compreendeu consultas em livros particulares, artigos científicos, bibliotecas, sites de universidades revisando os bancos de teses, dissertações e monografias, que segundo, busca proporcionar maior familiaridade com o problema, buscando torná-lo mais

explícito, desta forma o desenvolvimento de novas metodologias, assim como novos conhecimentos que podem facilitar a compreensão da evolução tecnológica, viabilizando seu potencial tecnológico e utilização passa a ser de extrema relevância para o crescimento profissional e das organizações (Gil, 2008).

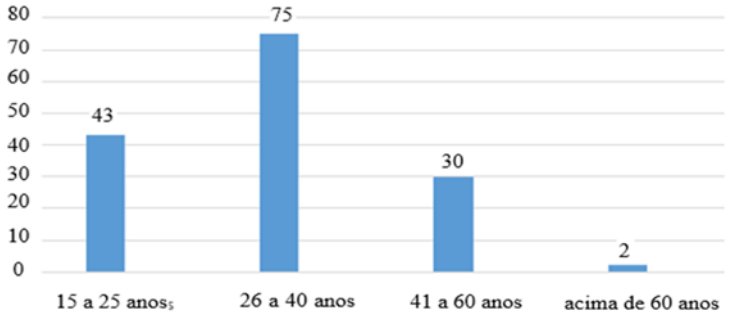
Foi aplicado um questionário online entre os dias 13 e 27 de outubro de 2022, divulgado por meio de *WhatsApp*, e os dados foram compilados da plataforma Microsoft *forms*. Ao todo foram obtidas 150 respostas anônimas, formalizadas por 6 perguntas direcionadas.

4. Análise e Interpretação dos Resultados

Nesta seção são apresentados os resultados obtidos por meio da pesquisa realizada para a análise do trabalho conforme apresentados na metodologia. Foram analisadas as respostas referentes a como os entrevistados utilizam os aplicativos para realização de suas compras de alimentos.

Um dos pontos relevantes para os autores está relacionado a idade dos respondentes, possibilitando assim um melhor escopo conforme apresentado na Figura 2.

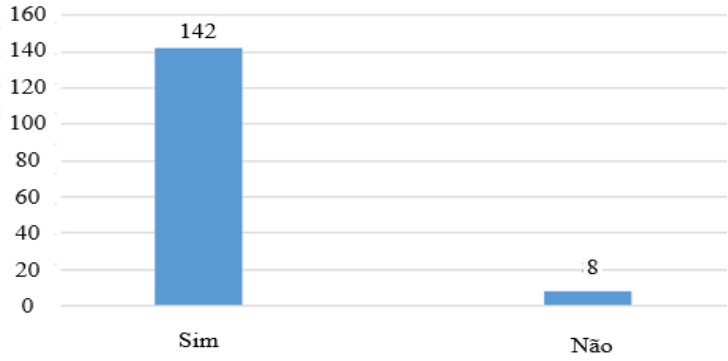
Figura 2: Faixa etária dos respondentes



A Figura 2 divide a faixa etária dos respondentes onde de 15 a 25 anos temos 43 respondentes ou 29%, entre 26 a 40 anos temos 75 respondentes o que representa 50%, já entre 41 a 60 anos são 30 respondentes ou seja 20%, e finalizando respondentes acima de 60 anos temos 2 respondentes ou 1%.

A Figura 3 apresenta o cenário da pesquisa com 150 respondentes indicando quantos destes utilizam aplicativos para a compra de alimentos denominado como *delivery*.

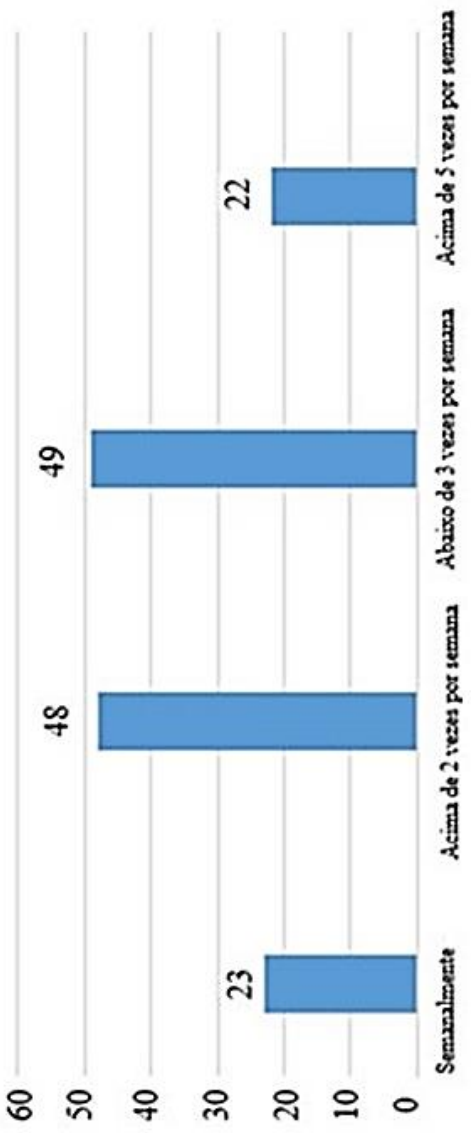
Figura 3: Utilização de aplicativos de alimentos



Dentre os respondentes pesquisados 142 pessoas ou 95% afirmaram que já utilizaram algum tipo de aplicativo para a compra de alimentos *on line* ou denominado de *delivery*, já 8 respondentes ou 5% indicaram que nunca utilizam estes aplicativos para a realização de compras.

No Gráfico 3 é apresentado a frequência em que os respondentes utilizam os aplicativos de entrega de alimentos, ressaltando que foram retirados os 8 respondentes que na Figura 4 sinalizaram que não utilizam este tipo de modalidade para realizar compras de alimentos, sendo assim os dados que passam a ser analisados 142 respondentes.

Figura 4: Frequência de utilização dos aplicativos


60
50
40
30
20
10
0
23
48
49
22
Semanalmente
Acima de 2 vezes por semana
Abaixo de 3 vezes por semana
Acima de 5 vezes por semana

Na Figura 5 são apresentadas as frequências do uso de aplicativos de *delivery* e observamos um equilíbrio entre as pessoas, que utilizam o serviço abaixo de 3 vezes ao mês com 49 respondentes ou seja 35% e pessoas que utilizam o serviço acima de 2 vezes durante a semana de 48 pessoas o que representa 34%. Também foram apresentados equilíbrios entre as pessoas que utilizam semanalmente 23 respondentes ou seja 16% e as pessoas que utilizam mais de 5 vezes o aplicativo por mês 22 pessoas o que representa 15%.

Observa-se também que a grande maioria dos entrevistados utilizam o aplicativo *iFood* 113 respondentes ou 77%, sendo líder de mercado neste segmento segundo a pesquisa analisada. Em segundo ponto os aplicativos dos próprios estabelecimentos com 22 respondentes o que representa 16% dos entrevistados, já o aplicativo *Rappi* teve 5 respondentes que utilizam este aplicativo ou seja 3,5% e o aplicativo Zé *delivery* teve 2 usuários ou 1,5%.

A Figura 6 aponta em qual momento se ampliou a utilização dos aplicativos de alimentos segundo os respondentes.

Figura 5: Aplicativos mais utilizados

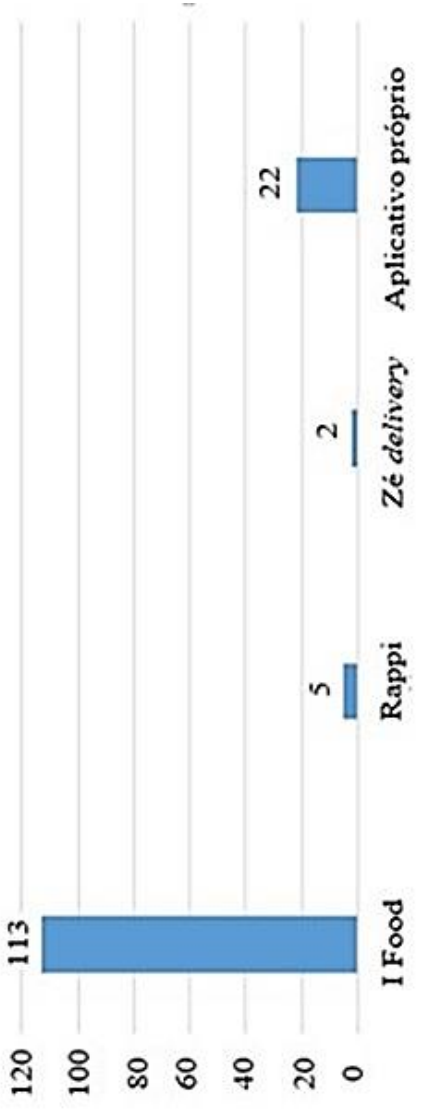
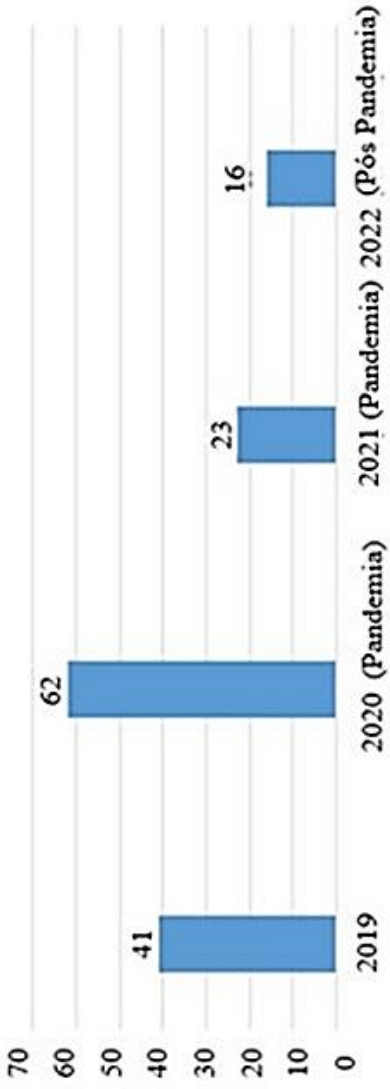


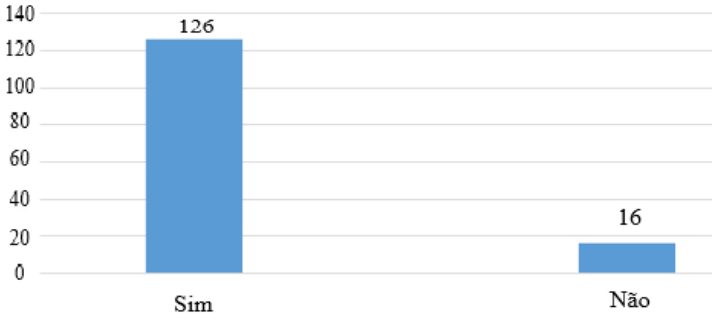
Figura 6: Ano de início da utilização dos aplicativos



Conforme apresentado em 2019, 41 pessoas ou 29% já utilizavam algum tipo de aplicativo antes da pandemia, porém se somarmos 2020 e 2021 período de maiores restrições referentes a pandemia temos 85 respondentes ou 60% que iniciaram a utilização dos aplicativos de entregas de alimentos e apenas 16 pessoas ou 11% iniciaram este processo em 2022 chamado de pós pandemia.

Na Figura 7 para reforçar a ideia e a importância dos aplicativos foi perguntado aos respondentes entre os anos de 2020 e 2021 se houve uma maior utilização por meio deste serviço.

Figura 7: Frequência da utilização dos aplicativos



Entre os entrevistados 126 ou 88% afirmaram que utilizaram com maior frequência os aplicativos de *delivery* e apenas 16 ou 12% responderam negativamente, sendo assim é importante destacar que as restrições decorrentes da pandemia favoreceram os números apresentados.

5. Conclusões

A quarta revolução industrial ou a denominada indústria 4.0 passa a ser um processo irreversível que afeta todos os segmentos organizacionais. Na pesquisa realizada sobre a utilização dos aplicativos de entregas de comida *delivery* tornou-se possível visualizar está aplicação, além disso buscou-se mapear quais as faixas etárias, frequência de utilização e empresas envolvidas neste processo.

Embora ainda com muitos desafios a serem encarados a integração de tecnologias da informação e comunicação, que permitiram alcançar novos patamares de produtividade, flexibilidade, qualidade e gerenciamento, possibilitando a geração de novas estratégias e modelos de negócios.

No período de isolamento por causa do coronavírus que ocorreu nos anos de 2020 e 2021, contribuíram e aceleraram a tendência do comportamento do consumidor em estar mais conectado e na busca de alternativas tecnológicas.

Toda esta evolução corrobora para que se tenha cada vez mais interfaces entre a tecnologia e as pessoas, o que agrega também para as organizações de uma forma geral, visto que também há uma interface entre a sociedade e as organizações. Portanto aumentam as oportunidades e o mercado da visibilidade para quem quer apostar nesse tipo de negócio.

Referencial Bibliográfico

Bezerra, J. (2011). Biografia e resumo da Revolução Industrial. Toda Matéria. Disponível em: https://www.todamateria.com.br/revolucao-industrial/. Acesso em: Acesso em 02 de novembro de 2022.

Cavalcante, Z. V., & da Silva, M. L. S. (2011). A importância da revolução industrial no mundo da tecnologia.

Cheng, C. (2015). *Semantic degrees for industrie 4.0 engineering: deciding on the degree of semantic formalization to select appropriate technologies. In: European software engineering conference and the acm sigsoft symposium on the foundations of software engineering*, 10, Bergamo.

Silva, M. R. G. (2021). O crescimento das empresas de delivery no contexto da pandemia.

Fante, B. Z., & de Souza, V. V. C. (2021). A 4ª revolução industrial e seus impactos no futuro dos meios de trabalho. *etic-encontro de iniciação científica-issn 21-76-8498*, *17*(17).

Furtado, J. et al. (2017). Indústria 4.0: a quarta revolução industrial e os desafios para a indústria e para o desenvolvimento brasileiro.

Gil, A. C. (2008). Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas.

Guerra, J. H. L. (2000). Utilização do computador no processo de ensino-aprendizagem: uma aplicação em planejamento e controle da produção. *São Carlos: USP-Universidade de São Paulo*.

Hermann, M., Pentek, T., & Otto, B. (2015). Design principles for industrie 4.0 scenarios: a literature review. Technische Universität Dortmund, Dortmund, 45.

iFood. Institucional Ifood (2022). Disponível em: https://institucional.ifood.com.br/ ifood/. Acesso em: 07.out.2022.

Kamalaldin, A., Linde, L., Sjödin, D., & Parida, V. (2020). Transforming provider-customer relationships in digital

servitization: A relational view on digitalization. Industrial Marketing Management, 89, 306-325.

Lira, G. D. L. *Indústria 4.0: os impactos das tecnologias habilitadoras nas estratégias de operações* (Doctoral dissertation, Universidade de São Paulo).

Magalhães, E. D. S. (2016). A compressão do tempo e a formação de novos hábitos alimentares: reveses e possibilidades.

Magrani, E. (2018). *A internet das coisas*. Editora FGV.

Martins, G. de A., & Theóphilo, C. R. (2016). Metodologia da Investigação Científica Para Ciências Sociais Aplicadas (3ªed). Atlas.

Ponte Neto, E. D. S. (2016). I Food: um estudo sobre o comportamento de compra do consumidor.

Ramos, C. (1994). Pedagogia da qualidade total. Qualitymark Editora Ltda.

Sacomano, J. B., Gonçalves, R. F., Bonilla, S. H., da Silva, M. T., & Sátyro, W. C. (2018). Indústria 4.0. Editora Blucher.

Sanders, A., Elangeswaran, C., & Wulfsberg, J. P. (2016). Industry 4.0 implies lean manufacturing: Research activities in industry 4.0 function as enablers for lean manufacturing. Journal of Industrial Engineering and Management (JIEM), 9(3), 811-833.

Silveira, C. B. (2017). O que é indústria 4.0 e como ela vai impactar o mundo. Citisystens. Disponível em https://www.citisystems.com.br/industria-4-0

Autores deste Capítulo

Filipe Correa dos Santos Andrade

Bacharel em Administração, experiência em atendimento a clientes e ao público em geral, conhecimento na área de ensino superior em atividades administrativas desde a controle e logística de avaliações, participando da implementação de um novo sistema de avaliação, controles de KPI internas, atua na área de *learning management system*.

Gabrielly Nunes de Oliveira

Bacharel em Administração, com experiência nas áreas de contabilidade, compras, jurídico e Administração, com maior conhecimento nas atividades de administração, compras e facilites, desde avaliação comercial, controle de estoque, controle de viagens corporativas, pagamentos e treinamento de estagiário. Atualmente estou atuando na área de compras na empresa Casio Brasil.

Jéssica Aparecida Leal de Souza

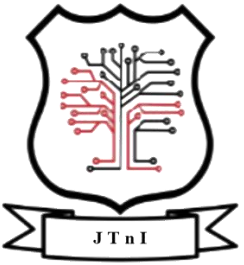
Bacharel em Administração, experiência em atendimento a clientes e ao público em geral, amplo conhecimento nas atividades administrativas desde avaliação de contratos, controle de entrada e saída de correspondências e estoque, sugestões de melhorias e reporte à gestão para soluções de conflitos. Atua na área comercial de Tecnologia Forense Digital.

Vanessa Lopes de Almeida

Mestre em Ciências Sociais / Antropologia pela PUC/SP. Bacharel em Direito e em Serviço Social e licencianda em Filosofia pela pela Universidade de Santo Amaro (UNISA/SP). Atuou como assistente social, na implantação de Centro de Convivência para Idosos, Coordenadora e técnica de CRAS / CREAS, sustentabilidade empresarial, desenvolvimento de projetos socioambientais em empresa de grande porte Na academia desde 2011 ministrando aulas na Graduação nos Cursos de Serviço Social, Administração, Ciências Contábeis, Direito, Gestão Pública, Economia e Gastronomia. Na Pós-Graduação nos Cursos de Gestão de Projetos Sociais, MBA em Gestão Pública. Entre os principais interesses na pesquisa, destacam-se os estudos sobre gênero, violência e violação de direito e envelhecimento

Marcos de Oliveira Morais

Pós Doutor em Engenharia de Produção com linha de pesquisa em gestão do conhecimento e inovação tecnológica. Qualidade e inovação. Doutor em Engenharia de Produção é Mestre em Engenharia de Produção, Pós-Graduado MBA em Gestão da Qualidade, em Engenharia de Produção, em Pedagogia Empresarial e Educação Corporativa, Formado em Gestão da Qualidade e com vasta experiência. Consultor e docente na área da Metal Mecânica, Gestão da Qualidade e Logística. Possui várias publicações científicas nacionais e internacionais. Atua como revisor das revistas Perspectivas Online, Exacta e Journal of Technology & Information. Co-autor de diversos livros



CAPÍTULO 5

Segurança da Informação e Proteção dos Dados: Aplicação Web

Elson Santos da Costa

Wiliam Carlos Galvão

1 Introdução

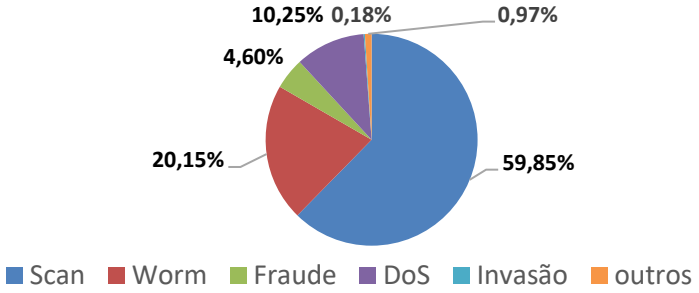
Atualmente, as empresas compreenderam que não basta ter um produto que contenha qualidade e preço. É preciso ter algo além. Isso significa conhecer bem seu cliente, entender seus gostos, suas necessidades, trazê-lo para mais perto e torná-lo mais do que um cliente, um parceiro que venha agregar valor ao produto ou serviço, oferecendo experiências que venham fidelizar o cliente com a marca (Kotler & Keller, 2012).

De acordo com Kotler, Hermawan e Iwan (2021), o avanço da tecnologia trouxe consigo facilidades e agilidade nos processos, tornando-se um aliado para as empresas no sentido de compreender, quase que em tempo real, as necessidades de seus clientes. Essa compreensão permite o suporte na criação de campanhas direcionadas para atrair e fidelizar esses clientes.

A segurança dos dados é uma grande preocupação, no ano de 2021, houve um aumento de 950% de ataques cibernéticos em relação há 2020 (Fortinet, 2022).

No Brasil em 2020 a CERT.br, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil em seu relatório final, indica um aumento nos números de incidentes, demonstrado na figura 1, São dados preocupantes que indicam alto risco de roubos ou acessos não autorizados à dados sigilosos (Cert.br, 2022).

Figura 1 – Incidentes Reportados



A Figura 1 demonstra os principais incidentes e a respectiva proporção relatados no período de janeiro de 2020 à dezembro de 2020.

O relatório de segurança Fortinet (2022) cita que o Brasil foi o segundo país da América Latina a sofrer mais ataques cibernéticos na ordem de 88,5 bilhões. Este maior

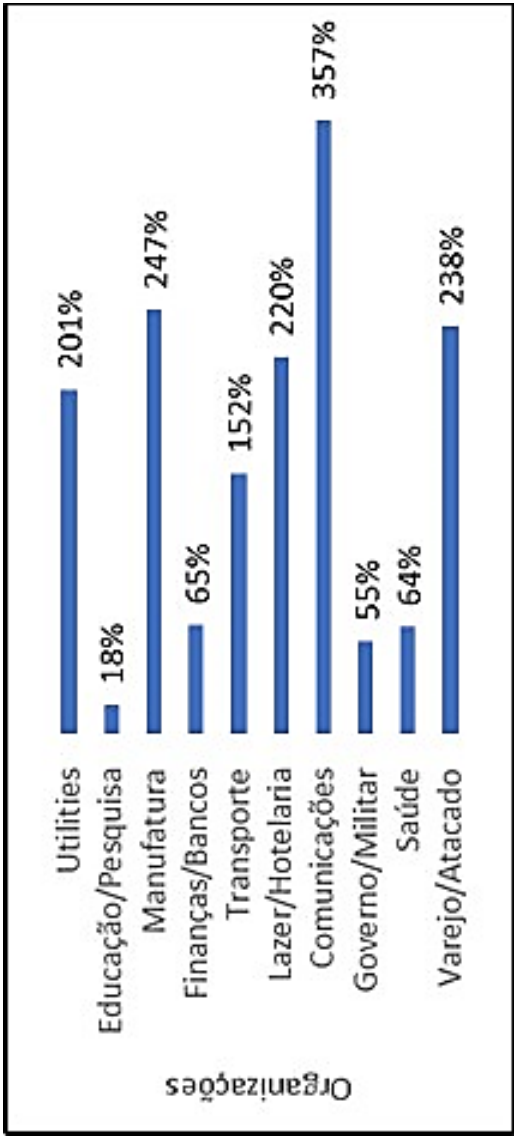
volume tem ligação direta pelo aumento do trabalho remoto, impulsionado pela pandemia.

No Brasil, houve um aumento na ordem de 77% de ataques às organizações, no período de 2020 a 2021 (Check Point Research, 2021). A Figura 2 indica os ataques separadas por organizações.

Apesar da alta de ataques, as empresas precisam entender e alinhar suas estratégias em conjunto com as tecnologias na implementação de táticas e operações de marketing para atrair clientes, oferecendo mais que apenas produtos ou serviços, desta forma terão clientes fiéis a marca (Kotler; Hermawan; Iwan, 2021).

Neste contexto, este artigo busca responder à **Q**uestão de **P**esquisa (**QP**): "Os dados manuseados nas aplicações *web* estão seguros contra-ataques cibernéticos e vazamentos de informações?". Os objetivos são: (1) Apresentar métodos de segurança para mitigar os riscos; (2) Discutir sua eficiência.

Figura 2 – Incidentes Reportados



2 Referencial Teórico

2.1 International Organization for Standardization

InternationalOrganization for Standardization (ISO), possui sede na Suíça desde a sua criação no ano de 1946, 160 países são associados a ISO, sendo representados pelos seus órgãos de normalização (INMETRO, 2022).

O objetivo da organização Internacional de Normalização é criar normas que incentivam as boas práticas de gestão, avanço tecnológico e propagar conhecimentos para manter um padrão a ser seguido e assim facilitar o comércio mundial (INMETRO, 2022).

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2022). As normas ISO são critérios estabelecidos entre os membros associados que visam padronizar as ações, atividades e processos com o objetivo de melhorar eficiência, reduzir falhas na produção, aumentar a qualidade de produtos e serviços e garantir a segurança dos sistemas de acordo com os princípios de Confidencialidade, Integridade e Disponibilidade (CIA) (ISO, 2022).

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2022). A ABNT representa o Brasil na organização ISO e é uma instituição privada sem fins lucrativos. Além disso, a ABNT participa da Comissão Pan-Americana de Normas Técnicas (COPANT) e é membro da Comissão Eletrotécnica Internacional (IEC) (ABNT, 2022).

A ABNT trabalha na certificação de produtos e desenvolve estudos, pesquisas para atender as necessidades das empresas brasileiras para melhorias nos processos, qualidade, melhoria de eficiência e diminuição dos impactos ambientais (ISO, 2022).

2.2 Ciberataques

Os ciberataques consiste em obter acessos, roubar ou danificar arquivos que possuam algum tipo de valor, estes ataques podem ocorrem em organizações privadas, públicas ou até com pessoas físicas, se utilizando de conhecimento técnicos avançados de programação e lógica (Carvalho, 2005).

Os 8 primeiros meses do ano de 2021, houve um aumento de 23% de ataques no Brasil, identificando uma tendência de aumento em relação ao ano anterior, colocando o país como um dos focos de crimes virtuais (KASPERSKY, 2021).

Esse é um dado preocupante, que coloca em xeque a segurança de sistemas críticos, podendo causar milhões de reais em prejuízos quando o ataque obtém sucesso, um caso famoso que ocorreu no ano de 2021, foi com a grande empresa JBS em sua filial dos Estados Unidos, que teve seus dados sequestrados através do ataque tipo *Ransoware*, criptografando seus servidores, segundo a empresa, informa que seu departamento de TI atuou para restabelecer seus servidores e sistemas (JBS, 2021).

2.3 Segurança da Informação

De acordo com Silva (2009), a Segurança da Informação envolve a criação de um documento contendo medidas a serem implementadas para proteger as informações e sistemas de informações. O objetivo é

garantir a integridade, disponibilidade, não repúdio, autenticidade e confidencialidade dessas informações.

A Autenticidade, de acordo com Silva (2009), refere-se à garantia de que a informação ou usuário é genuíno, permitindo a identificação do sistema ou usuário e aumentando a proteção contra acessos não autorizados e fraudes.

De acordo com Carvalho (2005), o pilar de segurança da Disponibilidade assegura que a informação ou sistema esteja prontamente acessível em qualquer momento solicitado.

Segundo Silva (2009), o princípio de Não-Repúdio desempenha um papel crucial ao garantir que uma ação concluída não possa ser negada, o que proporciona confiabilidade às informações obtidas por meio de transações eletrônicas. Esse princípio é especialmente relevante para aplicações web envolvidas no comércio eletrônico.

A Integridade garante que a informação esteja na sua forma original quando for armazenada ou enviada,

protegendo contra modificações não autorizadas (IBM, 2021).

A Confidencialidade permite que a informação ou sistema deve ser acessado somente por pessoas autorizadas, permitindo segregar os níveis de acesso de acordo com sua necessidade (IBM, 2021).

2.4 Open Web Application Security Project

Open Web Application Security Project (OWASP) é uma entidade privada sem fins lucrativos que tem por objetivo pesquisar e desenvolver melhorias de segurança dos softwares (OWASP, 2022).

A organização OWASP tem um projeto onde, são analisados vários trabalhos de desenvolvimento de softwares para encontrar vulnerabilidades e ranqueá-las, é criado um documento com recomendações para os processos de desenvolvimento para mitigar os riscos de segurança, estes dados analisados é elaborador por especialistas em segurança da informação e organizações que contribuem com a entidade (OWASP, 2022).

A lista Top 10 OWASP apresentada na Tabela 1 tem sua última edição lançada em 2021 e apresentou as vulnerabilidades na Tabela 1.

Tabela 1 – *TOP* 10 OWASP – Baseado em Owasp (2022)

#	Vulnerabilidades Encontradas
A01	Controle de acesso quebrado
A02	Falhas de criptografias
A03	Injeção
A04	Design inseguro
A05	Configuração incorreta de segurança
A06	Componentes vulneráveis e desatualizados
A07	Falhas de identificação e autenticação
A08	Falhas de software e de integridade dados
A09	Falhas de registro e monitoramento de segurança
A10	Falsificação de solicitação (SSRF)

3 Metodologia

Este artigo utilizou, conforme Tabela 2, a metodologia Estudo de Caso, pois proporcionou expor de forma prática o problema para retratar de forma real soluções adequadas por abordar especificações técnicas e desenvolvimento (YIN, 2014).

Tabela 2 – Características da Pesquisa

Item	Conteúdo	Autor (a)
QP	Os dados que transitam nas aplicações web estão seguros contra-ataques cibernéticos e vazamentos de informações?	
Natureza	Qualitativo	Martins & Theóphilo (2009)
Metodologia	Estudo de Caso	Yin (2014)

3.1 Procedimentos Para Desenvolvimento do Ambiente

Os procedimentos seguirão da seguinte forma:

Etapa 1: Criar ambiente. No portal Microsoft criar o ambiente de teste CRM Dynamics;

Etapa 2: Teste de Vulnerabilidade. Realizar o teste de vulnerabilidade utilizando a ferramenta OWASP ZAP;

Etapa 3: Avaliar os resultados. Através dos resultados obtidos pela ferramenta de teste, identificar as falhas através da avaliação dos dados;

Etapa 4: A partir da Questão de Pesquisa, validar as propostas;

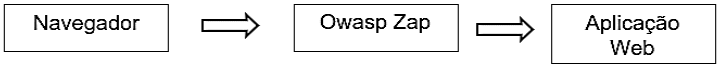
Etapa 5: Análise dos Resultados.

3.2 Desenvolvendo Ambiente de Teste

A ferramenta utilizada para realizar análise de vulnerabilidade é a OWASP ***Z**AP **A**TTACK **P**ROXY* (ZAP), é um software para scanear aplicações web de código aberto muito utilizado para verificar vulnerabilidades, trabalha entre o navegador e *web application*, se colocando em uma posição conhecida como *man-in-the-middle*, desta forma ele irá inspecionar as mensagens trocadas entre navegador e aplicação, modificar o conteúdo e encaminhar para o destino e analisar o comportamento da aplicação (OWASP, 2022).

Na Figura 3 é possível identificar como a ferramenta Owasp Zap trabalha para coletar as informações e realizar o teste de vulnerabilidade conforme Figura 3.

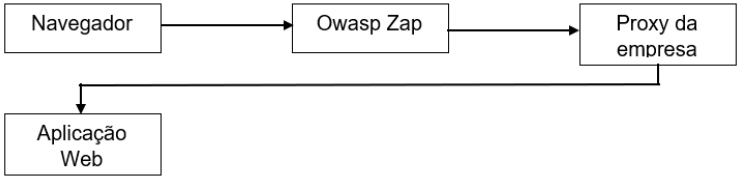
Figura 3: Owasp Zap Sem Proxy



Fonte – Realizado pelo próprio autor

A Figura 4 ilustra de forma sequencial o funcionamento da ferramenta Owasp ZAP.

Figura 4: Owasp Zap Com Proxy



De acordo com Dynamics Cloud (2022), o ambiente de teste selecionado foi o CRM Microsoft Dynamics 365, uma solução baseada em nuvem. Nesse contexto, a segurança do ambiente é responsabilidade da Microsoft, que implementa medidas como firewalls, regras de segurança para acesso aos servidores e atualizações regulares, entre outros aspectos.

No ambiente *CRM* é possível realizar qualquer ação, adicionar ou remover usuários de grupo, criar bancos de dados no ambiente *Microsoftdataverse*, gerenciar recurso

criados no ambiente e definir políticas de prevenção contra perdas de dados (MICROSOFT, 2022).

Realizado a criação do ambiente CRM:

Ambiente CRM endereço: https://org89ca8cb4.crm2.dynamics.com/ (Ambiente *trial* para teste);

- Configurado os componentes: O ambiente possui uma solução de nome “Treinamento” e um aplicativo Alocação de Equipamentos de TI para teste;
- Aplicado as configurações de segurança (Criar, atualizar, visualizar e exclusão) – Esta etapa foi criado um grupo de nome: Alocação de Equipamentos para definir os níveis.

A Figura 5 representa os níveis de acessos aos recursos do ambiente, é possível classificar para cada componente a forma de como o usuário que possuir no seu perfil o grupo Alocação de Equipamentos o grau de permissões que no *Dynamics* são classificados pelas chaves representadas por círculos pintados conforme Figura 5.

As chaves possuem os valores:

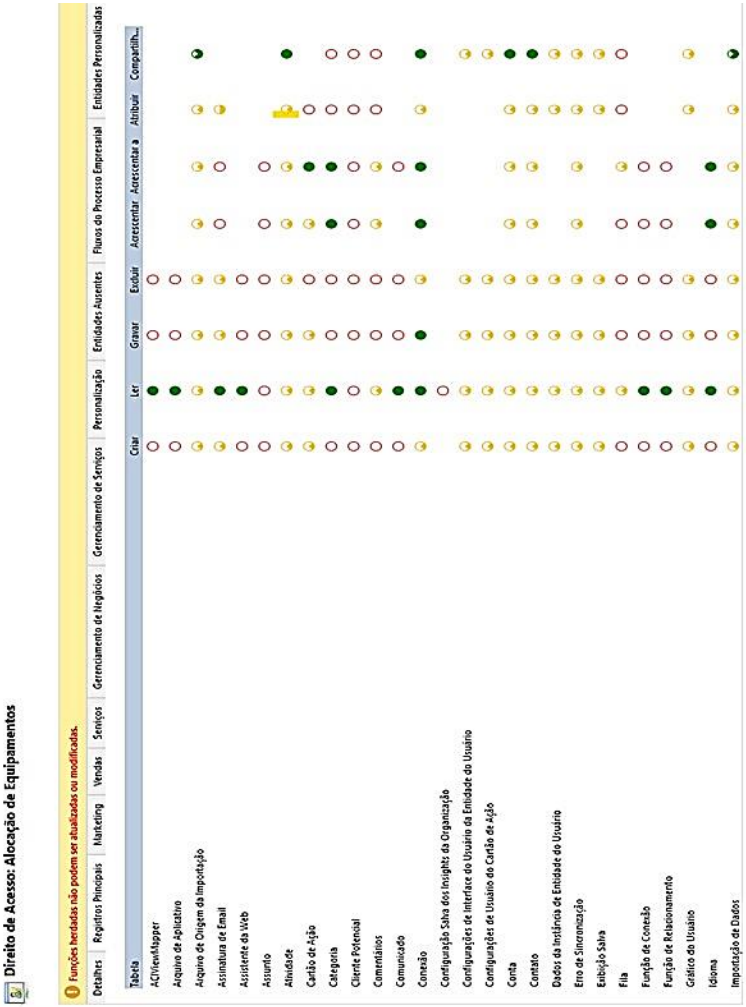
- Usuário: Esta chave indica que somente o usuário que criou o registro poderá atualizá-lo;

- Unidade de Negócio: Os usuários que pertence a unidade de negócio onde o registro foi criado poderá atualizá-lo;

- Divisão Primárias, secundárias: Os usuários poderão atualizar os registros de Unidades de Negócios e usuários que estiverem abaixo dela;

- Organização, esta chave indica que terá acesso irrestrito para manusear o registro conforme sua necessidade.

Figura 5: Direitos de Acesso



Para o armazenamento dos dados será utilizado o *Microsoft Dataverse*, é uma solução baseada em nuvem para ser o repositório central dos dados, ele permite escalar recursos conforme necessidade (MICROSOFT, 2022).

Foram criadas três tabelas no *Microsoft Dynamics* como demonstra a Figura 6, estas tabelas são denominadas como entidades.

O ambiente possui um aplicativo *Model Driven* chamado de Alocação de Equipamentos de TI para que os dados das alocações sejam armazenados e gerados relatórios demonstrados na Figura 7. Na Figura 8 podemos visualizar sua interface e os campos preenchidos com informações de vários clientes compostos por nome do cliente, equipamento alocado, período e valores.

Figura 6 – Tabelas *Microsoft Dynamics*

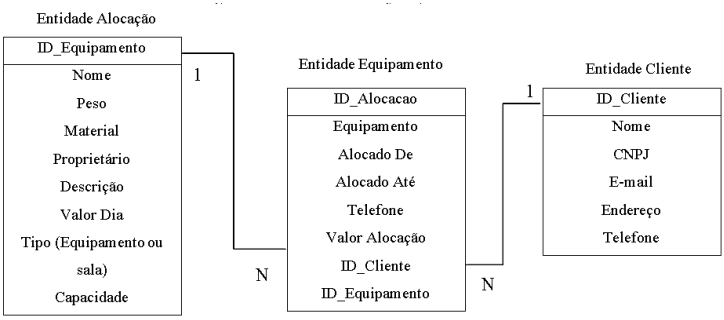


Figura 7 – Descrição das Entidades Criadas

Alocação de Equipamentos TI > **Tabelas**

Tabela	Nome	Tipo	Gerenciado
Alocação	smt_alocacao	Standard	Não
Cliente	smt_cliente	Standard	Não
Equipamento	smt_equipamento	Standard	Não

Figura 8 – Aplicativo Model Driven Alocação de Equipamentos de TI

Foram criados dados fictícios para a aplicação observado na Tabela 3, os testes de vulnerabilidades serão realizados neste ambiente.

Tabela 3 – Configuração básica do ambiente

Ambiente	Tipo	Banco de Dados
Treinamento	*SubscriptionBasedTrial*	5 GB

3.3 Programa de Recompensas para a Localização de Bugs da Microsoft MSRC

A *Microsoft* possui um programa de recompensas onde incentivam pesquisadores, profissionais da tecnologia a descobrirem vulnerabilidades nos seus produtos, serviços ou dispositivos da *Microsoft*. Se o relatório de vulnerabilidades enviado afetar um produto ou serviços e esteja alinhada ao programa de recompensa, será premiado com valores que podem chegar até US*$ 250.000*. (MICROSOFT MSRC, 2022)

4 Análise e Interpretação dos Resultados

4.1 Teste de Vulnerabilidade – Resultado

Realizado teste de vulnerabilidade no ambiente *CRM Trial* com a ferramenta Owasp zap para verificar as principais vulnerabilidades mais encontradas nas aplicações que estão descritas na Tabela 1 – Capítulo 2.4.

Os alertas gerados são classificados por cores:

- Cor vermelha: Alta;
- Cor Amarelo escuro: Médio;
- Cor Amarelo Claro: Baixo;
- Cor Azul: Informativo;
- Cor Verde: Falso Positivo.

De acordo com OWASP ZAP (2022), a categorização é realizada pelo aplicativo, com base nas referências fornecidas pelo OWASP, CVE e CWE, as quais são apresentadas diretamente no aplicativo OWASP ZAP.

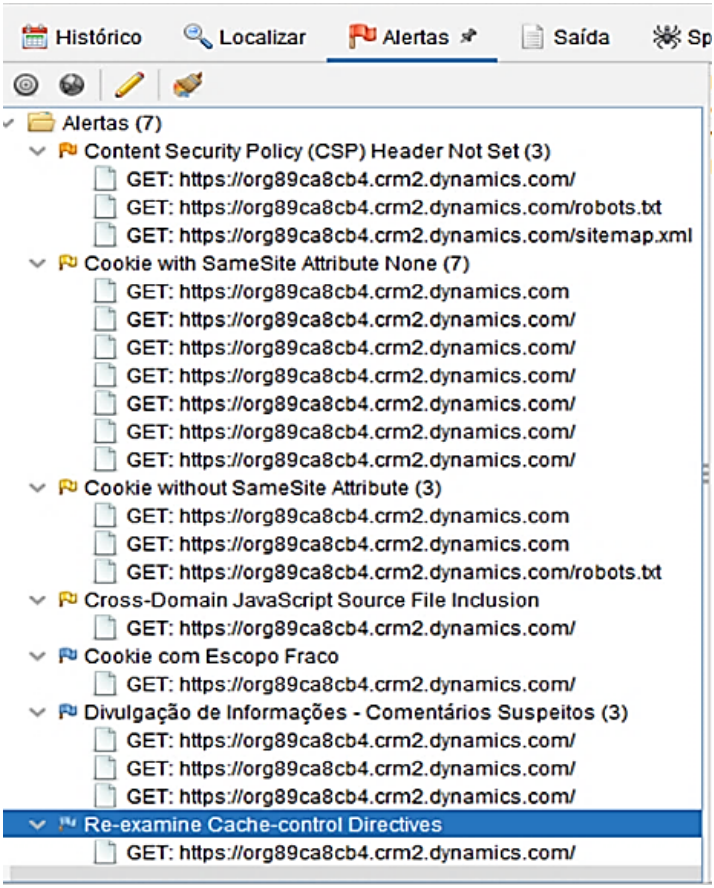
Foram encontradas 7 alertas nos testes realizados, onde:

- 1 Cor Amarela escura: Médio;
- 3 Cor Amarela claro: Baixo;
- 3 Cor Azul: Informativo.

Conforme mencionado pela OWASP ZAP (2022), é importante destacar que, embora a categoria de cor azul seja informativa, se não for corrigida, pode representar uma brecha em que hackers podem explorar para realizar ataques que causam danos significativos à organização. Essa classificação de vulnerabilidade é claramente apresentada na lista Owasp Top 10.

A Figura 9 lista os alertas gerados pelo teste, categorizando por riscos sendo identificados com bandeiras coloridas que indicam a sua classificação. Clicando nos alertas será aberto uma tela com as informações do risco encontrado, descrição e soluções.

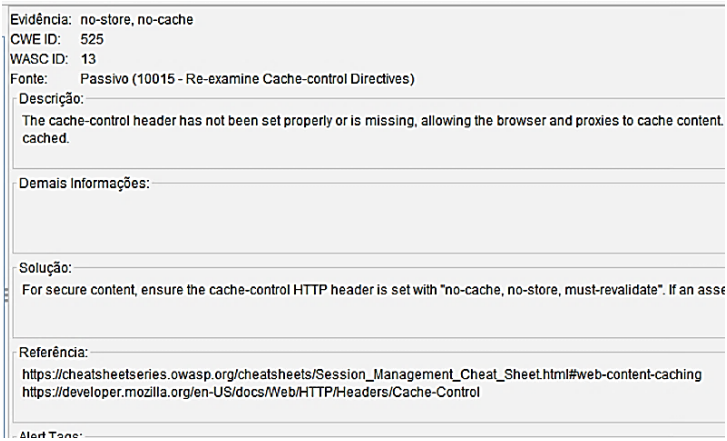
Figura 9 – Tela de Resultado



Segundo OWASP ZAP. (2022), a Figura 10 apresenta as informações ao clicar no alerta, com informações sobre a vulnerabilidade encontrada e um breve

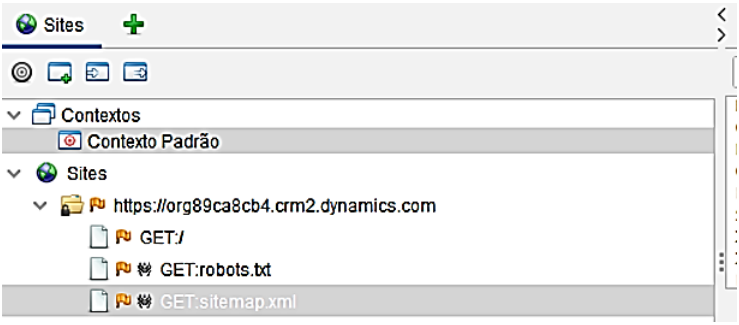
relato de como corrigir o problema, ao pesquisar o código CWE (2022) é possível obter mais detalhes do risco bem como a solução no máximo detalhe.

Figura 10 – Tela de Resultado



A Figura 11 faz parte dos resultados encontrados. No entanto, esta tela informa os itens testados, no caso deste estudo, a página da aplicação web e scripts que podem ser utilizados em conjunto de categorias e *templates* (OWASP ZAP, 2022).

Figura 11 – Tela de Resultado



Os resultados encontrados no aplicativo Owasp zap foram tabulados com informações que que identificam qual o nível de alerta conforme Tabela 4, vulnerabilidade, descrição e a possível solução.

O teste de vulnerabilidade demonstra que, por mais que a aplicação seja bem projetada, bem estruturada e desenvolvida, sempre há pontos que podem se tornar vulneráveis. Importante entender que o teste de vulnerabilidade é uma parte da estratégia para se manter o ambiente seguro. É preciso instituir o gerenciamento de vulnerabilidades para conhecer melhor pontos de melhoria.

Tabela 4: Resultado teste de Vulnerabilidade

Tag Alerta **Classificação Top 10** **CWE ID**	**Vulnerabilidade Descrição**	**Solução**
Amarelo Escuro 5 693	*Security Misconfiguration* Forma de configuração incorreta	Certificar seu servidor *web*, esteja configurado para definir o cabeçalho *Content-Security-Policy*, para obter o suporte ideal ao navegador: "*Content-Security-Policy*" para Chrome 25+, *Firefox* 23+ e *Safari* 7 +, etc.
Amarelo Claro 1 1275	*Broken Access Control* Cookie com o atributo *SameSite*definido como "*none*", dessa maneira é possível realizar ataques por falsificação de solicitação entre sites, inclusão de script entre sites etc.	Definir atributo *SameSite* com o valor:*Iax* ou *atrict.*
Azul 8 565	*Software and Data Integrity Failures* Cookie com escopo de domínio Pai.	Sempre definir o escopo dos cookies para FQDN

Tag Alerta Classificação Top 10 CWE ID	Vulnerabilidade Descrição	Solução
Azul 1 200	. *Broken Access Control* Comentários suspeitos que podem ajudar um invasor	Remover todos os comentários que retornem informações que possam ajudar o invasor.

4.2 Gerenciamento de Vulnerabilidade

Segundo o ITEAM (2020), a vulnerabilidade é considerada um ponto de acesso potencial para invasões, acesso não autorizado e vazamento de dados quando descoberta por hackers. Essa vulnerabilidade pode ter origem na infraestrutura, desenvolvimento da aplicação ou banco de dados.

O gerenciamento de vulnerabilidade tem por objetivo criar processos para identificar as vulnerabilidades, classificar e indicar a solução adequada para correção dos itens elencados como vulneráveis (MICROSOFT, 2022).

A ISO 27002 é uma norma que fornece diretrizes de Segurança da Informação com práticas para gerenciamento de segurança, controles para ambientes críticos para desenvolvimento de processos para identificação e gerenciamento de riscos e vulnerabilidades (ISSO, 2022).

O teste indica como primeiro passo, conhecer os pontos falhos, desta forma a empresa terá meios para desenvolver processos internos para melhorias contínuas, terá conhecimento dos ativos, possuindo um maior controle para avaliação das vulnerabilidades (MICROSOFT, 2022).

4.3 Discussão

Os resultados dos testes indicam que é importante ter um gerenciamento de vulnerabilidades das aplicações web, desta forma os dados que lá trafegam sempre estarão seguros e com o mínimo de risco para ataques e vazamentos de dados.

Muito importante ter um processo preventivo de melhoria contínua, sempre baseado nas melhores práticas de gestão de segurança da informação em conformidade com o que é praticado no mercado e regulamentado por entidades regulamentadoras (ISO - STANDARDS, 2022).

Conforme a ISO - STANDARDS (2022), a norma ISO 15408 desempenha um papel importante ao auxiliar os desenvolvedores na construção de aplicações seguras. Ela descreve os conceitos necessários para garantir a segurança dos sistemas, possibilitando uma avaliação mais detalhada.

Diante das questões que implicam na segurança da informação, o teste de vulnerabilidade demonstra que não podemos ficar satisfeitos com a segurança já aplicada mesmo que nunca tenham tido um ataque ou vazamentos, pelo contrário, sempre haverá pontos frágeis, muito importante estar atentos com as novas tecnologias e tendências na segurança da informação.

5 Conclusões

Segundo o Ministério da Cidadania (2022), a Lei Geral de Proteção de Dados (LGPD) foi instituída com o

objetivo de salvaguardar a liberdade, privacidade e formação da personalidade de cada indivíduo. A LGPD oferece orientação tanto para empresas, governo e outras entidades sobre a maneira adequada de coletar, tratar, armazenar e manipular dados por meio de um conjunto de medidas que delineiam responsabilidades, penalidades e direitos das partes envolvidas.

Neste contexto, faz se necessário trabalhar para manter o ambiente seguro para estar aderente a Lei, bem como ter um ambiente seguro para aplicações onde, é desenvolvido um ciclo de melhoria por meio do Gerenciamento de Vulnerabilidades avaliando seus ativos para entender o perfil de risco de cada recurso.

Qualquer software que seja mal desenvolvido possui vulnerabilidades que serão exploradas em algum momento. As aplicações web, são visadas por estarem disponíveis ao público, logo, implementar de maneira segura é fundamental. Além disto, há riscos das informações coletadas pela empresa de serem acessadas, vazadas, comprometendo todo o serviço realizado por ela. Caso haja o incidente, põem em risco a credibilidade e

mostra para seus usuários, clientes a falta de gestão e competência da empresa em gerir com segurança o seu ambiente.

A utilização da ferramenta de escaneamento OWASP ZAP é parte de uma estratégia maior, o software encontra as vulnerabilidades para serem solucionadas, no entanto, é importante trabalhar para identificar a causa raiz que permitiu que esta vulnerabilidade ocorresse.

O gerenciamento de vulnerabilidade vem de encontro com esta proposta, conhecendo seus ativos e recursos, poderá de forma proativa reduzir os pontos vulneráveis. No entanto, este gerenciamento de vulnerabilidade, deve estar acompanhado com uma política de segurança da informação, que contemple processos, procedimentos, responsabilidades das áreas bem como as ações que serão tomadas, pontos focais quando um incidente ocorrer.

A ISO 27002 é um ótimo ponto de partida para as organizações implementarem Sistema de Gerenciamento de Segurança da informação (SGSI), com diretrizes e procedimentos auxiliando as organizações com as melhores

soluções de acordo com os ambientes de riscos, porte e estratégias.

Em conjunto com o gerenciamento de vulnerabilidade, Políticas de Segurança, processos para avaliações de segurança, equipe bem treinada, o risco de algum ataque prosperar será mínimo, portanto, manter um ciclo que revise todos os processos em um ciclo de melhoria contínua, possibilita que as aplicações *web* seja sim, seguras e possa garantir os três principais pilares, Disponibilidade, integridade e Autenticidade.

Como contribuição futura será elaborado uma cartilha de boas práticas especificamente para modelos aplicados ao contexto do estudo.

Referências Bibliográficas

ABNT - Brasil. ISO - Membros. Recuperado em 3 de junho de 2022, de https://www.iso.org/member/1579.html

Carvalho, L. G. de. (2005). Segurança de Redes (2ª ed.). Editora Ciência Moderna.

CERT.br. (2022). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Recuperado em 28 de agosto de 2022, de https://www.cert.br/

Check Point Research. (2022). Cyber Attack Trends: 2022 Mid-Year Report. Recuperado em 20 de junho de 2022, de https://research.checkpoint.com/category/threat-intelligence-reports/

CWE. (2022). CWE - Common Weakness Enumeration. Recuperado em 4 de junho de 2022, de https://cwe.mitre.org/index.html

Dynamics Cloud. (2022). Microsoft Dynamics 365 Cloud. Recuperado em 29 de abril de 2022, de https://dynamics.microsoft.com/pt-br/cloud-migration/

Fortinet. (2022). Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. Segurança. Recuperado em 2 de abril de 2022, de https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021

IBM. (2021). Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação. Segurança da Informação. Recuperado em 10 de setembro de 2022, de https://service.com.br/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao/

INMETRO. O que é ISO? Governo. Recuperado em 3 de junho de 2022, de http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp

ISO - International Organization for Standardization. ISO - Standards. Normalização. Recuperado em 3 de junho de 2022, de https://www.iso.org/home.html

Iteam. (2022). Vulnerabilidade de segurança e quais são as mais comuns. Segurança da Informação. Recuperado em 17 de setembro de 2022, de https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/

JBS. JBS USA E PILGRIM'S ANUNCIAM RESOLUÇÃO DE ATAQUE CIBERNÉTICO. Privado. Recuperado em 6 de dezembro de 2022, de https://ri.jbs.com.br/arquivos-cvm/avisos-comunicados-e-fatos-relevantes/

Kaspersky. (2021). O Panorama de Ameaças 2021 da Kaspersky. Recuperado em 24 de abril de 2022, de https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/

Kotler, P., & Keller, K. L. (2012). Marketing Estratégico Para Instituições Educacionais (12ª ed.). Pearson - Prentice Hall.

Kotler, P., Hermawan, K., & Iwan, S. (2021). Marketing 5.0: Tecnologia para a humanidade. Editora Sextante.

Martins, G. de A., & Theóphilo, C. R. (2009). Metodologia da investigação científica para ciências sociais aplicadas.

Microsoft. 365. O que é o Dynamics 365? CRM. Recuperado em 22 de abril de 2022, de https://dynamics.microsoft.com/pt-br/what-is-dynamics365/

Microsoft. Gerenciar permissões e administração para o Dataverse. Recuperado em 29 de abril de 2022, de https://docs.microsoft.com/pt-br/learn/modules/get-started-security-roles/

Microsoft. O que é o Gerenciamento de Vulnerabilidades? Tecnologia. Recuperado em 29 de abril de 2022, de https://www.microsoft.com/pt-br/security/business/security-101/what-is-vulnerability-management

Ministério da Cidadania – Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado em 20 de junho de 2022, de https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd

Open Web Application Security Project. OWASP. Fundação. Recuperado em 20 de junho de 2022, de https://owasp.org/

OWASP ZAP. OWASP - Zap Attack Proxy (ZAP). Cibersegurança. Recuperado em 3 de setembro de 2022, de https://www.zaproxy.org/

OWASP. OWASP Top Ten. Segurança da Informação. Recuperado em 20 de junho de 2022, de https://owasp.org/www-project-top-ten/

Silva, L. H. R. da. (2009). Tecnologia em Redes de Computadores - Uso de GPO's na Segurança de Domínios Corporativos. Ciência Moderna.

Yin, R. K. (2014). Estudo de Caso. Planejamento e Métodos (5ª ed.). Bookman.

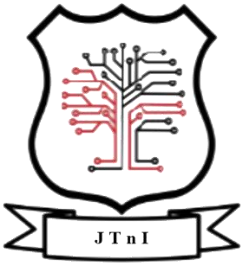
Autores deste Capítulo

Elson Santos da Costa

Tecnólogo em Segurança da Informação pela FATEC Santana de Parnaíba e Bacharel em Ciência da Computação pela UNIP. Possui formação técnica em SQL SERVER pela Escola de Tecnologia Impacta, Web Design pelo SENAI Mariano Ferraz, Power BI e Javascript pela Escola de Treinamento Hashtag Treinamentos. Possui aperfeiçoamento em Perícia Forense Computacional, Auditoria, Engenharia de software e Python realizado pela FATEC. Atuou como Analista de Suporte N2 e N3 e atualmente trabalha em uma consultoria CRM na área de Suporte e Desenvolvimento utilizando C#, Javascript, Html e css. Publicou seu primeiro artigo sobre segurança da informação pela revista *Journal Of Technology & Information.*

Wiliam Carlos Galvão

Doutor em Agronomia, Energia na Agricultura pela UNESP com linha de pesquisa em processamento de imagens e sinais e veículo aéreo não tripulado, Mestre em Agronomia, Energia na Agricultura pela UNESP com linha de pesquisa em Sistemas de gestão de recursos para o agronegócio. Especialista em Desenvolvimento de Sistemas para Ambiente Web, Segurança Cibernética e Forense Computacional. Graduando em Sistemas de Informação pela USC, Licenciado em Matemática, técnico em processamento e eletrônica. Possui aperfeiçoamento em Ciência de Dados, Arquiteto *Cloud Computing* e *Business Intelligence*. Publicou artigos em revistas e congressos nacionais e internacionais. É revisor das revistas *Journal of Technology & Information* e FatecSeg.



CAPÍTULO 6

Ransomware: A Evolução dos Ataques na Contemporaneidade e seus Desafios para a Segurança Digital

Stephany Victoria Nascimento da Silva

Irapuan Glória Júnior

1. Introdução

Ao longo dos anos, os crimes cibernéticos têm chamado cada vez mais a atenção da mídia. Isso devido ao seu crescimento rápido e as táticas de engenharia social empregadas para fazer suas vítimas. Entre eles, um dos mais incidentes nas organizações do Brasil e do mundo está o *Ransomware*, que por ter seu público-alvo voltado às empresas, é um dos que mais causa prejuízos financeiros no mundo (Biancamano, 2021)

O *Ransomware* é um tipo de *malware* que sequestra os arquivos de um computador, exigindo um pagamento para liberá-los. Por meio de técnicas sofisticadas de engenharia social, exploração de vulnerabilidades em sistemas operacionais e aplicativos, e uso de criptografia avançada, os cibercriminosos têm sido capazes de lançar ataques *Ransomware* cada vez mais perigosos e disseminados, incluindo a propagação por meio de *e-mails* de *phishing*, *downloads* de *software* malicioso,

vulnerabilidades em sistemas operacionais e aplicativos, entre outras práticas fraudulentas (Inside, 2023)

As tendências nas empresas de utilizar o formato de trabalho remoto e o aumento da digitalização de processos têm proporcionado novas oportunidades para os criminosos propagarem o *Ransomware*, resultando em consequências graves para empresas e indivíduos, incluindo perda de dados, tempo de inatividade, custos de recuperação e danos à reputação. Algumas das variantes mais conhecidas de *Ransomware* incluem o *WannaCry*, o *Petya*, o *Locky*, e o *Ryuk* (Report, 2022).

Diante desse cenário, torna-se imprescindível compreender a evolução do *Ransomware* ao longo dos anos, desde suas primeiras aparições até as variantes mais recentes, com o objetivo de desenvolver estratégias de defesa mais eficazes contra esse tipo de ameaça e até mesmo prever tendências futuras (Souza, 2023). Nesse sentido, o presente artigo possui como questão de pesquisa: "Quais os tipos de *Ransomware* identificados?". Os objetivos do presente estudo são: (1) Identificar quais os

tipos de *Ransomware* descritos na literatura (2) Apresentar um diagrama de identificação a partir do comportamento do ataque.

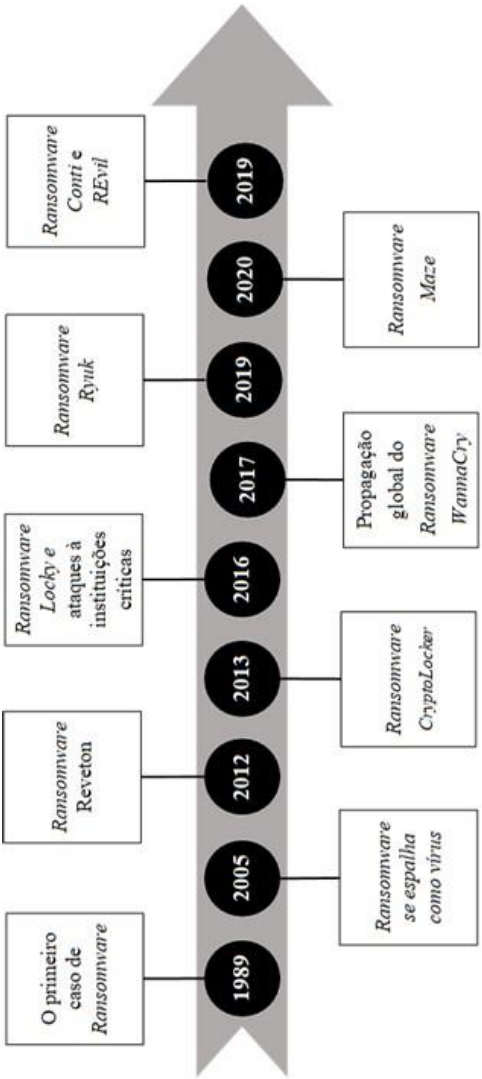
2. Referencial Teórico

2.1. Ransomware

Entender o fenômeno criminógeno, que representa as origens de um crime, é essencial para a sua compreensão, assim como suas condicionantes e possibilita a análise e definição de possíveis tendências, para viabilizar seu combate e prevenção (Souza, 2018).

A escala evolutiva do *Ransomware* (Figura 1) iniciou em 1989 com a primeira versão do vírus que foi criado pelo Doutor em biologia Joseph Popp de Harvard, e disseminado por meio de uma tática de Engenharia Social (Prabhu & Van Wagoner, 2023)

Figura 1 – Linha do tempo da evolução do Ransomware baseado em McAffe (2021)



O ataque consistiu em enviar um disco nomeado AIDS, acrônico para *Acquired Immunodeficiency Syndrome* (Prabhu & Van Wagoner, 2023), para uma lista de participantes de uma confraternização da Organização Mundial de Saúde (OMS) sobre a doença, fazendo mais de 20.000 pessoas serem vítimas de sequestro de dados por acreditarem se tratar de pesquisas médicas (Mujezinovic, 2019).

Por meio de seu primeiro caso, é possível estabelecer como inicia o fluxo de infecção do *Ransomware*, por uma estratégia social, convencendo suas vítimas de que o arquivo malicioso se trata de algo de seu interesse e não por meio de uma força técnica (Guedes, 2021).

A atuação do *Ransomware* AIDS, conforme Figura 6, inicia com o envio de um dispositivo até a vítima (Etapa 1) que insere no computador e acessa o arquivo infectado (Etapa 2). Após o acesso, é realizada a instalação do *malware* (Etapa 3), e quando perfizer a

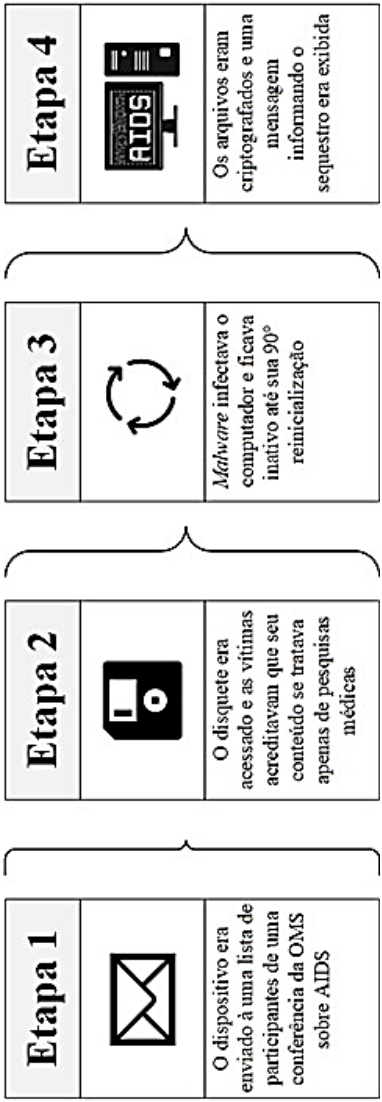
nonagésima inicialização do sistema operacional (Etapa 4), o vírus criptografa os dados do computador e a visualização do sistema era substituída por um alerta de solicitação de pagamento para a corporação *PC Cyborg* pela liberação dos dados (Kelly, 2021).

Especialistas da segurança da informação conseguiram rastrear o autor facilmente, revertendo o processo e permitindo o rastreamento e prisão do autor dos crimes. Isso foi possível devido ao fato que a criptografia ser realizada através de chaves simétricas (Kelly, 2021).

Apesar de demonstrar aptidão suficiente para arquitetar o vírus e sua forma de propagação, Popp foi julgado inapto mentalmente para responder por seus atos (Lessing, 2020).

O ataque interrompeu a operação de várias instituições e organizações médicas, no qual algumas vítimas entraram em pânico e apagaram seus *hard-drivers*, perdendo dados de pesquisas de valores imensuráveis e insubstituíveis (Mujezinovic, 2021).

Figura 6 – Esquema de Infecção do AIDS Baseado em Kelly (2020)



Diferente das vítimas, cuja percepção da realidade acontece imediatamente e suas consequências podem ser inúmeras visto que estes casos podem acarretar demissões nas empresas afetadas, a. Isso ocorre porque as empresas podem sofrer perda de dados, interrupção de negócios e danos à reputação, o que pode afetar sua situação financeira e consequentemente a capacidade de manter funcionários, levando à necessidade de cortes de custos. Em alguns casos a demissão pode ocorrer até mesmo pela culpabilização do funcionário que foi enganado pelos criminosos e acabou servindo como "porta de entrada" (Bertolluci, 2019).

Algumas das consequências psicológicas de um ataque de *Ransomware* incluem ansiedade devido à pressão de tomar decisões rapidamente, raiva e irritação decorrentes da sensação de injustiça, perda de confiança e habilidades tecnológicas resultante da perda de acesso a informações importantes, e depressão devido ao impacto significativo na vida das vítimas. Além disso, algumas vítimas podem desenvolver sintomas de estresse pós-traumático, como *flashbacks*, pesadelos e evitação de situações relacionadas ao ataque (Laccelva, 2021).

Wilhem, a primeira vítima de *Ransomware* conseguiu contornar a situação e começou a receber ligações de instituições e organizações médicas perguntando como ele o fez. Devido à sua experiência, ele atualmente trabalha como profissional de Segurança da Informação (CNN, 2021).

Apesar de sua investigação ter sido consideravelmente rápida e o autor encontrado, a história do *Ransomware* não acabou por aí. Como principais exemplos, em 2005, o *Ransomware* começou a se espalhar pela internet como um vírus. Já em 2012, o *Ransomware Reveton* se mostrou uma versão mais evoluída e sofisticada ao se disfarçar como uma mensagem de aplicação da lei (Lemos, 2017).

Em 2013, o *Ransomware* CryptoLocker se espalhou rapidamente por e-mail e exigia o pagamento em Bitcoin, dificultando a investigação da transação, tática que é utilizada até os dias atuais. Já em 2016, o *Ransomware* Locky se tornou uma das formas mais populares, atingindo hospitais e outras instituições críticas pois a venda de seus

dados possui grande retorno financeiro. Em 2017, o *Ransomware WannaCry* se espalhou globalmente, infectando mais de 200.000 computadores em 150 países (FireEye, 2018).

Em 2019, o *Ransomware Ryuk* se tornou cada vez mais sofisticado e direcionado a grandes empresas. Em 2020, o *Ransomware Maze* se tornou ainda mais direcionado e perigoso ao infiltrar os arquivos do usuário e ameaçar divulgá-los publicamente. E a partir de 2021, o *Ransomware* continua sendo uma ameaça significativa com ataques como o *Ransomware* Conti e REvil, enquanto surge o aparecimento de grupos de *Ransomware*, que trabalhando desta forma se tornam mais organizados e profissionais (McAffe, 2021).

Na evolução e história do *Ransomware* foi possível separá-lo em categorias e tipos mais incidentes. Primeiramente é necessário compreender que é frequente haver confusão ao considerar o *Ransomware* como um vírus comum. Tal equívoco ocorre devido a uma imagem ultrapassada que muitas pessoas têm, segundo a qual todo

malware é um vírus genérico, pois este é o tipo de malware mais conhecido e difundido, graças à sua habilidade de se replicar e incidência no dia a dia da população (AVG, 2022).

Um malware é uma categoria formada por programas desenvolvidos para prejudicar um computador (PagBank, 2023). Portanto, *Ransomwares*, cavalos de tróias, *spywares*, *adwares*, entre outros, são todos pertencentes às famílias de malwares (Ximenes, 2022).

Os meios mais utilizados para infecção de *Ransomware* utilizam táticas de Engenharia Social, como por exemplo, convencendo o usuário a baixar um arquivo infectado, convencendo-o que na verdade, seja algo de seu interesse (AVG, 2021).

Isso ocorre principalmente via e-mail, convencendo o usuário de que o arquivo malicioso enviado à ele é referente a algum site que este fez inscrição, ou até mesmo em corporações fingindo que é algum comando de um superior na cadeia hierárquica da empresa (Srinivas, 2021).

Existem também, infecções por *Malvertising*, que envolve a incorporação de *malware* em anúncios em sites populares, e kits de *exploit*, que são ferramentas de *hacking* que exploram vulnerabilidades em software desatualizado. Além disso, alguns sites maliciosos aproveitam navegadores desatualizados para baixar *malwares* em segundo plano (Rivera, 2023).

2.2. Incidência Global e Nacional

Em relação aos ataques cibernéticos as maiores vítimas estão nos setores empresariais, sobretudo no setor de Varejo. Baseado nas estatísticas, é possível constatar que o índice está direcionado ao segmento do comércio varejista representando 11% acima da média dos ataques observados em outros setores, e tem levado os agentes varejistas a não encararem a ação de ciberataque de *Ransomware* como uma simples hipótese, mas sim um fato eminente (Inside, 2022).

O setor que registrou a segunda maior incidência de ataques foi o governamental, devido ao fato de que estas realizam a coleta e o armazenamento de vastas quantidades de informações, que compreendem dados de cidadãos

individuais que podem ser comercializados na *deep web*. Ademais, há o perigo de utilização de dados militares e de segurança nacional por organizações terroristas (Inside, 2023).

Apesar de não lidarem com dados financeiros ou bancários, a indústria da saúde não está a salvo. No ano de 2022, o setor da saúde sofreu o terceiro maior número de ataques por *Ransomware*. As informações contidas no histórico médico de um paciente podem ter um valor de até 50 vezes mais do que dados bancários no mercado negro da internet. Isso se deve à durabilidade dos dados e à capacidade de cometer fraudes mais lucrativas, como seguros de vida, ao invés de simples compras e empréstimos *online* (Pacete, 2022).

No cenário global, o ano de 2017 passou por três grandes ataques de *Ransomware*. Em maio, o *WannaCry* afetou cerca de 200 mil computadores em mais de 150 países, com prejuízo estimado em US$ 1 bilhão. No final de junho, mais um ataque global foi realizado, desta vez chamado *Petya*, que impactou mais de 12 mil

computadores, encriptando *hard-drives* e os tornando inúteis. Por fim, em outubro, e com menor alcance, o *Bad Rabbit* afetou sistemas de aeroportos, metrôs e empresas de países como Rússia, Ucrânia, Turquia e Alemanha (Kapersky 2017).

O WannaCry surgiu porque a Agência de Segurança Nacional dos Estados Unidos desenvolveu uma exploração chamada *EternalBlue*, que se torna uma vulnerabilidade presente na implementação do protocolo *Server Message Block* (SMB) da Microsoft. Esta vulnerabilidade pode ser explorada devido ao fato de que muitas versões do Sistema Operacional *Windows* não manipulam pacotes especialmente criados corretamente, desta forma, um invasor pode criar pacotes especiais enviados ao dispositivo de destino, desencadeando uma exploração que pode ser usada para realizar ataques de *malware* no computador da vítima (Burdova, 2020).

A Microsoft lançou uma atualização para correção desta vulnerabilidade meses antes do ocorrido, porém como não foi divulgada a importância da instalação, muitos

usuários acabaram não realizando-a, o que permitiu o grande alcance do *WannaCry* (Root, 2022).

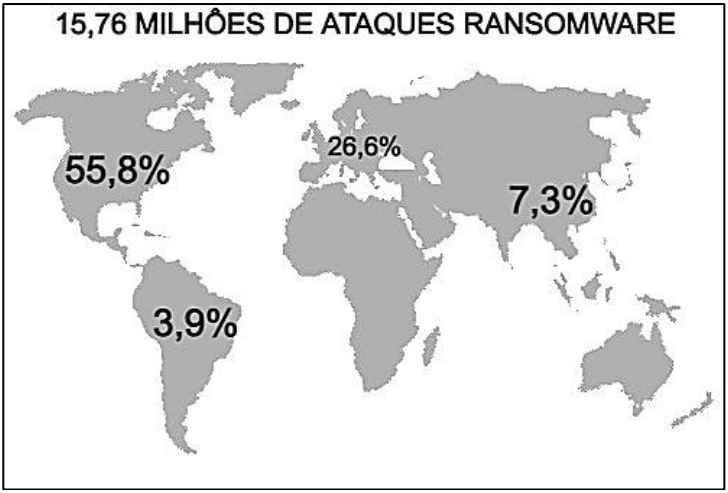
No ano de 2019 houve um aumento de 60% em relação ao ano anterior. Esses ataques, diferente de 2017, foram principalmente concentrados em municípios, e pelo menos 174 instituições municipais, com mais de 3.000 suborganizações foram atacadas (Kapersky,2019).

Um dos casos conhecidos pela mídia de infecção de *Ransomware* em 2019, foi do *malware Bitpaymer* que vitimou várias empresas espanholas e uma rádio (Chieco, 2019). As empresas conseguiram reverter o problema e mitigar seus impactos sem pagar aos criminosos. Dessa forma o *Bitpaymer* modificou seu código de acordo com estes aprendizados, evoluiu e atualmente é conhecido como *FriedEx* (Poslušný, 2021).

O ano de 2022 foi marcado com um grande acréscimo de ataques *Ransomware* (Figura 3) visto que estes quase dobraram comparado ao ano anterior. A américa do norte foi a maior vítima, com 55,9% dos ataques, em segundo lugar ficou a Europa com 26,6% dos

ataques, seguida pela Ásia com 7,3% e por último a América do Sul com 3,9% (Abranet,2023).

Figura 3 – Ataques *Ransomware* em 2022 divididos por continente baseado em Abranet (2023)



No Brasil, os ataques *Ransomware* começaram a tomar conta do mercado a partir de 2018, quando um *malware* brasileiro chamado *Cry Brazil* (Figura 4) chamou a atenção de pesquisadores, criptografando dados de usuários brasileiros e tendo como principal característica a troca do papel de parede do Windows com uma mensagem

em português pedindo resgate para liberar o acesso dos documentos armazenados (Perrone, 2018).

Figura 4 - Papel de Parede Cry Brazil baseado em Perrone (2018)

A versão do *Ransomware Cry Brazil* não fez nenhuma grande empresa de vítima, seu foco foi principalmente usuários comuns. Este foi apenas o início de um cenário que colocaria o Brasil no *ranking* mundial como um dos países mais afetados pelo vírus no mundo (Perrone, 2018).

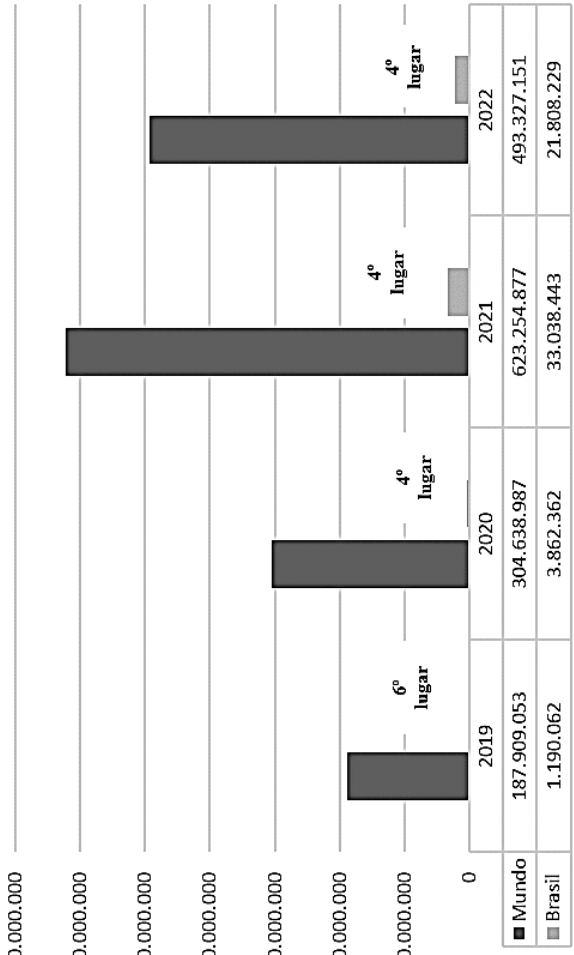
Em 2020, o Brasil sofreu o total de 187.909.053 ataques (Figura 5) ocupando o 6° lugar no ranking de países

mais afetados por *Ransomware* no mundo (Report, 2021). Em 2022 essa marca ultrapassou o número de 21.808.229 ataques, consolidando o país no 4 lugar deste ranking, visto que este já o ocupava desde 2020 (SonicWall, 2023).

O ano de 2021, além de trazer o Brasil para o quarto lugar no ranking global de ataques *Ransomware*, também foi marcado pela vitimização de duas grandes empresas brasileiras: As lojas Renner, do ramo de vestuários e a CVC, do mercado de turismo, trouxeram visibilidade à problemática de Segurança da Informação (Pacete, 2021).

O ataque sofrido pela Renner foi um grande marco na segurança da informação nacional, pois graças a sua repercussão, o assunto ganhou visibilidade (Gaidargi, 2021). A empresa divulgou um comunicado informando que havia ocorrido um ataque cibernético em seu ambiente de TI e que este causou indisponibilidade em parte de seus sistemas e operação. Esta também ressaltou que rapidamente acionou os protocolos e procedimentos existentes de controle e segurança para bloquear o ataque e minimizar eventuais impactos (Upx, 2021).

Figura 5 – Ataques *Ransomware* no Brasil baseado em SonicWall (2023)



O caso da empresa de viagens CVC também é outro caso importante para a segurança da informação nacional pois diferente da Renner, apenas conseguiu obter o reestabelecimento normal das operações 10 dias após o ataque cibernético (ABC, 2019).

Consequente deste cenário cerca de 850 lojistas da CVC informaram dúvidas e inseguranças relatadas por clientes que compraram na empresa antes da invasão cibernética, e demonstraram preocupação, se seus dados de cartões e pessoais, estavam seguros após a invasão ou se foram violados, comprometidos ou vendidos pelos criminosos. Apesar de a empresa não ter exposto os prejuízos causados durante esse período de interrupção, estima-se que este foi extremamente alto, visto que o prejuízo aumenta de acordo com o tempo que a organização fica fora do ar (Branco, 2021).

Para evitar estes cenários é extremamente importante que nas organizações sejam disseminadas formas de prevenção através da conscientização e treinamento de funcionários. É importante que eles estejam cientes dos

riscos associados ao *Ransomware* e saibam como identificar e evitar possíveis ameaças. Além disso, é fundamental manter os sistemas operacionais e aplicativos atualizados e utilizar programas de antivírus e *anti-malware* (Kapersky, 2022)

É importante que existam backups e estes sejam armazenados em locais seguros e que os procedimentos de recuperação de dados sejam testados regularmente. Caso a empresa seja vítima de um ataque de *Ransomware*, é fundamental ter um plano de contingência para mitigar os danos (McAfee, 2023).

Em resumo, a prevenção e mitigação de ataques de *Ransomware* em empresas exigem uma abordagem holística, envolvendo a conscientização dos funcionários, a atualização de sistemas e aplicativos, o backup regular de dados e a criação de um plano de contingência eficaz. A implementação dessas medidas pode ajudar a reduzir significativamente o risco de ataques de *Ransomware* e minimizar os danos em caso de ocorrência (Paiva, 2023).

Em 2020 foi identificado que o fato de que as empresas não pagaram o resgate, não torna o trabalho dos criminosos em vão, já que há uma nova abordagem híbrida onde a tática de leiloar informações roubadas foi adotada. Os criminosos se unem em organizações tipo cartel para realização destas atividades e compartilhamento de seu conhecimento (Grustniy, 2021).

2.3. *Ransomware* e a Legislação

Uma grande problemática relacionada aos *Ransomwares* é que estes são extremamente rentáveis para seus autores. Das organizações afetadas por ataques cibernéticos no país, 92% delas possuíam uma apólice de seguro cibernético. Além disso, o estudo constatou que 93% das seguradoras estavam dispostas a pagar o resgate exigido pelos criminosos para descriptografar os arquivos comprometidos. É importante ressaltar que sete em cada 10 organizações conseguiram recuperar o acesso aos seus dados após efetuarem o pagamento do resgate exigido pelos criminosos (Auler & Justo, 2022)

Além disso, o pagamento aos criminosos encoraja os hackers a criarem mais ataques desse tipo. Mesmo que a vítima não pague, estes ainda ganham dinheiro com a venda de dados na internet, prática que inclui até mesmo organização em cartéis (Elsad, 2022).

O principal problema em relação aos ataques *Ramsomware* é a dificuldade em punir seus autores. Em muitos casos, os responsáveis operam em países onde as leis são mais brandas em relação a crimes cibernéticos. Em outros casos, utilizam técnicas para dificultar a identificação da origem do ataque, como o uso de redes virtuais privadas e a utilização de criptomoedas para receber o pagamento do resgate (Finelli, 2016).

Além disso, muitas vezes os órgãos de investigação não possuem recursos suficientes para realizar uma investigação efetiva e identificar os responsáveis pelo ataque. Como resultado, muitos casos de ataques *Ransomware* acabam ficando impunes, o que incentiva ainda mais sua prática (Biales, 2020).

Outro fator que dificulta a punição dos autores de ataques *Ransomware* é a falta de cooperação entre países em relação a crimes cibernéticos. Como o ataque pode ter origem em um país e o resgate ser pago em outro, é necessário que haja uma cooperação internacional para que seja possível identificar os responsáveis e aplicar as leis de cada país (Garcez, 2022)

Portanto, a dificuldade na punição dos autores de ataques *Ransomware* é um grande desafio para as autoridades e empresas de segurança cibernética. É preciso investir em tecnologias e recursos para identificar e punir esses criminosos, além de buscar uma maior cooperação internacional para combater esse tipo de crime de forma efetiva (Lemos, 2020).

No Brasil, não existe uma lei específica que trate exclusivamente do crime de *Ransomware.* No entanto, algumas legislações podem ser aplicadas para punir os responsáveis por essa prática criminosa (Schettini, 2022).

Em território brasileiro, a legislação de combate a crimes cibernéticos é composta, principalmente, pela Lei nº

12.737/2012, também conhecida como Lei Carolina Dieckmann, e pela Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Ambas as leis trazem dispositivos que visam a prevenção e repressão de atividades ilícitas no ambiente virtual (Araujo, 2023).

O Código Penal Brasileiro prevê sanções criminais para quem produz, oferece, distribui, vende ou difunde programa de computador com o intuito de causar dano à integridade de dados, programas ou sistemas de computador, sem autorização ou consentimento do titular. Essa conduta pode ser enquadrada no artigo 154-A do Código Penal, que trata do crime de invasão de dispositivo informático (Cabette, 2014).

Além disso, a LGPD estabelece normas para proteção de dados pessoais, o que inclui a prevenção de vazamento ou sequestro de informações sensíveis. Dessa forma, empresas e organizações que não implementam medidas adequadas de segurança cibernética podem ser responsabilizadas por eventuais danos causados aos titulares de dados (Nones, 2022).

Por fim, é importante mencionar que o Brasil é signatário da Convenção de Budapeste sobre o Cibercrime, tratado internacional que estabelece cooperação entre países no combate a crimes cometidos no ambiente virtual. Através dessa convenção, é possível aprimorar a troca de informações e a investigação de casos de *Ransomware* que transcendem as fronteiras nacionais (Berbert, 2021).

3. Metodologia

A metodologia aplicada foi estudo de caso (YIN, 2021), pois o estudo tem como objetivo, entender as experiências de profissionais de Segurança da Informação com *Ransomware*, lições aprendidas e estratégias de mitigação apoiadas atualmente por estes. Na Tabela 1 são apresentadas as características utilizadas para a realização do estudo.

Tabela 1 – Características do Estudo

Item	Descrição	Autor(es)
Questão de Pesquisa	"As ações de prevenção, contenção e recuperação conhecidas por profissionais da área de Segurança da Informação evoluíram junto com o Ransomware?"	
Natureza	- Qualitativa	GIL (2022)
Metodologia	- Análise Bibliográfica	ECO (1997)
Coleta de Dados	- Análise documental	TEÓPHILO; MARTINS (2016)
Unidade de análise	- Artigos, publicações e notícias relacionadas à ataques *Ransomware*	

3.1. Processo Metodológico

As etapas desta pesquisa, conforme Figura 6, são:

- **Passo 1: Definir o tema e a questão de pesquisa.** O tema de pesquisa foi definido e uma questão de pesquisa clara foi formulada;

- **Passo 2: Realizar revisão bibliográfica inicial.** Foi realizada uma pesquisa inicial em bases de dados acadêmicas, bibliotecas e outras fontes confiáveis para obter uma visão geral do estado atual do conhecimento sobre o tema;

- **Passo 3: Selecionar as fontes relevantes.** As fontes bibliográficas foram avaliadas e selecionadas com base em sua relevância para o tema de pesquisa;

- **Passo 4: Ler e analisar as fontes selecionadas.** As fontes selecionadas foram lidas atentamente e analisadas, fazendo anotações sobre os principais conceitos, argumentos, metodologias e resultados apresentados;

- **Passo 5: Organizar as informações.** As informações obtidas das fontes bibliográficas foram organizadas de acordo com uma estrutura lógica ou esquema previamente definido; e

- **Passo 6: Escrever o artigo.** Com base na estrutura organizada e nas informações

Figura 6 - Procedimentos Metodológicos

4. Análise e Interpretação dos Resultados

4.1. Identificação do Tipo de Ransomware

A partir da literatura foi possível identificar os tipos de *Ransomwares: Crypto malware* (Burdova, 2022), *Locker* (Moura,2022), *Scareware* (Ramos, 2021), *Doxware* (Klusaité,2022) *Spora* (Mekauskas, 2020), *Petya* (Belcic, 2017) e *Reveton* (Lessing, 2020) e seu modo de infecção conforme apresentado na Figura 7.

Os *Ransomwares* podem ser divididos em quatro categorias principais (Figura): O *Crypto Ransomware* criptografa arquivos da vítima, o dispositivo continua funcionando normalmente, porém estes arquivos não podem ser abertos (Meskauskas, 2021). O *Locker Ransomware* que não realiza criptografia, mas bloqueia funções básicas do dispositivo como não permitir o acesso a área de trabalho ou bloquear parcialmente o teclado (Moura, 2022).

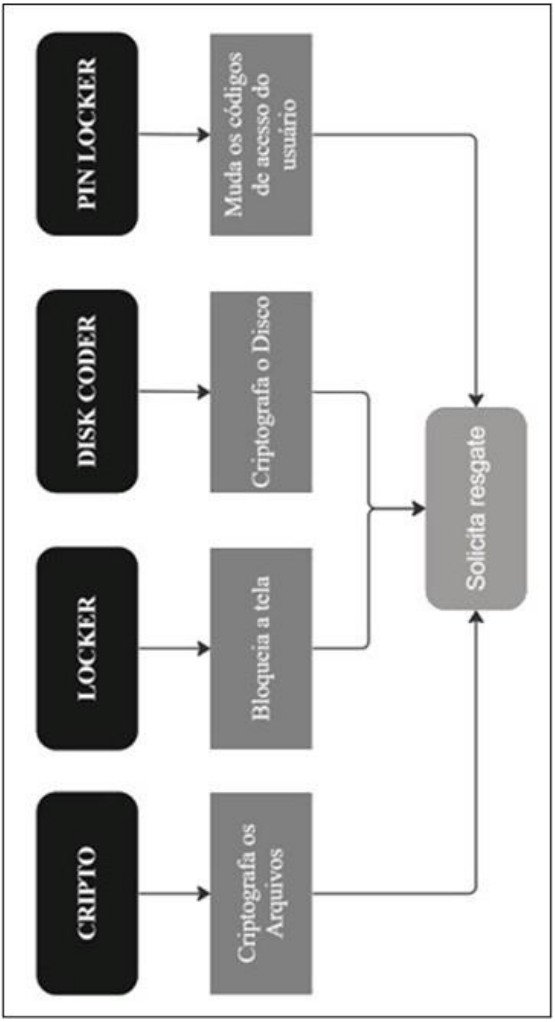
Em relação ao "*disk coder*" criptografa os arquivos no disco rígido da vítima impedindo o acesso aos dados.

Esse tipo de *Ransomware* pode se espalhar por toda a rede da vítima, criptografando arquivos em outros dispositivos conectados. Esse tipo de *Ransomware* é mais comumente encontrado em computadores de mesa e laptops (Cossetti, 2023).

Desde seu surgimento era comum o pensamento da existência de *Ransomwares* somente em computadores, mas estes já evoluíram e se sofisticaram, atualmente o *Ransomware "Pin Locker"* bloqueia a tela do dispositivo com um código PIN, e é comum em dispositivos móveis (Osborne, 2015).

A variante de *Ramsomware Locker* infecta os computadores das vítimas através de arquivos baixados da internet - geralmente versões piratas de jogos. Quando infiltrado e executado com sucesso, este encripta os arquivos do computador e estabelece um prazo de 72 horas para resgate. Caso este prazo não seja cumprido o malware apaga as Cópias Shadow Volume tornando a recuperação dos arquivos impossível (Moura, 2022).

Figura 7 – Principais Tipos de Ransomware baseado em Moura (2022) e AVG (2021)



Já o *ScareWare* tem como intuito manipular o usuário através do medo. Este exibe uma mensagem na tela se passando por um antivírus informando falsamente a vítima de que há algo errado em seu dispositivo e que é necessária a instalação de uma aplicação para resolução do problema. Essa aplicação na verdade é um malware que pode acessar as informações pessoais, financeiras e de navegação da vítima (Ramos, 2021).

Uma das variantes mais temidas é o *DoxWare* pois este chantageia o usuário ameaçando-o a expor seus arquivos e informações confidenciais publicamente. Geralmente infecta redes e computadores através de *phishing* com links e anexos maliciosos ou através de sites que contém códigos capazes de explorar vulnerabilidades de segurança não corrigidas no sistema de um visitante (Klusaitė, 2022).

O Spora é um *Ramsomware* que trabalha através do *JavaScript.* Um executável é enviado por e-mail para a vítima que baixa e o executa, desta forma uma pasta é extraída e um documento em *JavaScript* chamado

("closed.js") é colocado no sistema de pasta "%temp%". A pasta em *JavaScript* extrai outro executável com nome aleatório que sai encriptando as pastas da vítima. O Spora não necessita de internet para trabalhar (Meskauskas, 2020).

Um dos *Malwares* mais difíceis de remediar é o *Petya*, que criptografa o guia de referência rápida do computador para cada arquivo em seu HD (MFT) fazendo com que o computador não consiga inicializar ou funcionar normalmente. Em um computador Windows, ele infecta o MBR que é responsável por carregar o sistema operacional. Desta forma, o *Malware* obriga o computador a reinicializar enquanto criptografa o MFT, a partir disto o computador não consegue acessar nada do disco rígido, nem o próprio sistema operacional (Belcic, 2019)

O *Ramsomware* Reveton ficou famoso por se apresentar como agências policiais e governamentais, sendo personalizado para cada país. Este bloqueava a tela e exigia que os usuários pagassem uma "multa" sob ameaça de prisão (Lessing, 2020).

Por fim, os tipos *Cerber* e *Locky* são malwares que conseguem criptografar grande variedade de arquivos específicos, geralmente mídias e documentos que o usuário mais acessa, enquanto o *Locky* pode alterar o código-fonte do computador, o que o torna inutilizável (Avast, 2020).

O *Ransomware* está em constante evolução, atualmente até mesmo sistemas operacionais como MacOS e Linux já possuem variantes de *Ransomware* adaptadas para si - Assim como os dispositivos *Android* (Avelino, 2023).

Este *Malware* é difundido principalmente por quadrilhas, que se organizam, desenvolvem e realizam os ataques, em um levantamento realizado pela Microsoft, foi estimado que existam pelo menos 100 destas em todo o mundo (Brasiline, 2023). Este mercado é organizado e bem sofisticado porque é bastante lucrativo, uma pesquisa da Tren Micro estima que a Indústria de *Ransomware* já fatura mais de US$ 400 milhões ao ano (Advisor, 2023).

Tabela 2 - Tipos e Características mais comuns de *Ransomware*

Variantes	Características
Crypto malware	Explora uma vulnerabilidade do Windows, deixando a máquina exposta para criptografar os arquivos e pedir resgates (Burdova, 2022).
Locker	Infecta o SO impossibilitando acesso a todos os arquivos e aplicativos (Moura, 2022).
Scareware	Age como um antivírus falso afirmando ter encontrado problemas e solicitando dinheiro para resolver, enchendo a tela de mensagens *pop-up* (Ramos, 2021).
Doxware	Ameaça publicar as informações do usuário on-line caso o resgate não seja pago (Klusaitė, 2022).
Spora	Infecta o sistema através de *phishing*, agindo incialmente como um usuário administrador, mostrando uma janela pop-up que não some até que o usuário a aceite (Meskauskas, 2020).
Petya	Impede o acesso a todo o disco rígido, criptografando a tabela de arquivos mestre (Belcic, 2017).
Reveton	Bloqueia as telas em vez de criptografar os arquivos (LESSING, 2020).
Cerber e Locky	Pesquisam e criptografam tipos específicos de arquivos, geralmente documentos e arquivos de mídia (AVAST, 2021).

As quadrilhas de *Ransomware* também oferecem na *dark web* o chamado *Ransomware as a Service* (RaaS), ou *Ransomware* como Serviço, que permitem que criminosos cibernéticos sem habilidades técnicas consigam comprar esses kits, que possuem suporte 24 horas e 7 dias por semana, e fazer vítimas sem mesmo precisar desenvolver o *Malware* (Padeiro, 2023).

De acordo com uma pesquisa realizada pelo Relatório Anual de Defesa Cibernética/*Cyber Defense Report* (CDR), cerca de 78% das empresas que foram vítimas de *Ransomware*, mesmo conseguindo mitigar a situação, enfrentaram consequências de ameaças adicionais, como vazamento de dados, notificação à mídia ou outros tipos de ataques conjuntos como por exemplo, *DDoS* (Advisor, 2023).

4.2. Identificação do Tipo de Ransomware

A possibilidade de identificação do tipo de ataque *Ransomware* pode auxiliar os analistas de Tecnologia da Informação (Ramos, 2021; Moura, 2022; Advisor, 2023; Avelino, 2023), desta forma, a partir do referencial teórico foi elaborado um *Framework* de Identificação de *Ransomware* (Figura 8).

Os detalhamentos dos fluxos foram apresentados nas Figuras 9 a 13.

4.3. Discussões

É possível inferir que como o crime cibernético não requer ação ou esforço físico e os criminosos não sofrem consequências em suas vidas pessoais, pode reduzir a percepção da gravidade de suas ações (Schreiber, 2022).

Figura 8 – *Framework* de Identificação de *Ransomware*

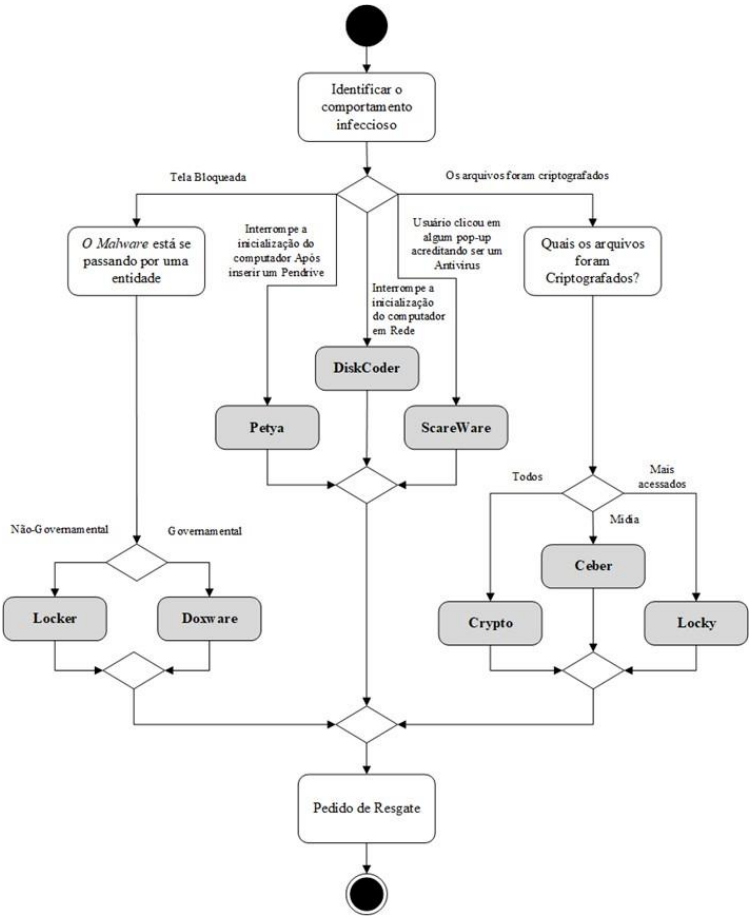


Figura 9 – Detalhamento do Fluxo Decisório Superior

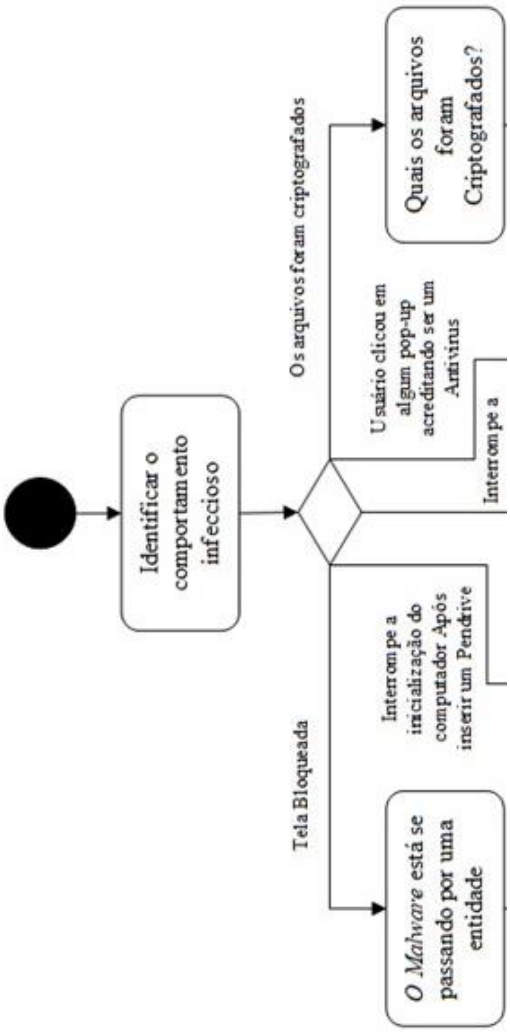


Figura 10 – Detalhamento do Fluxo Esquerdo

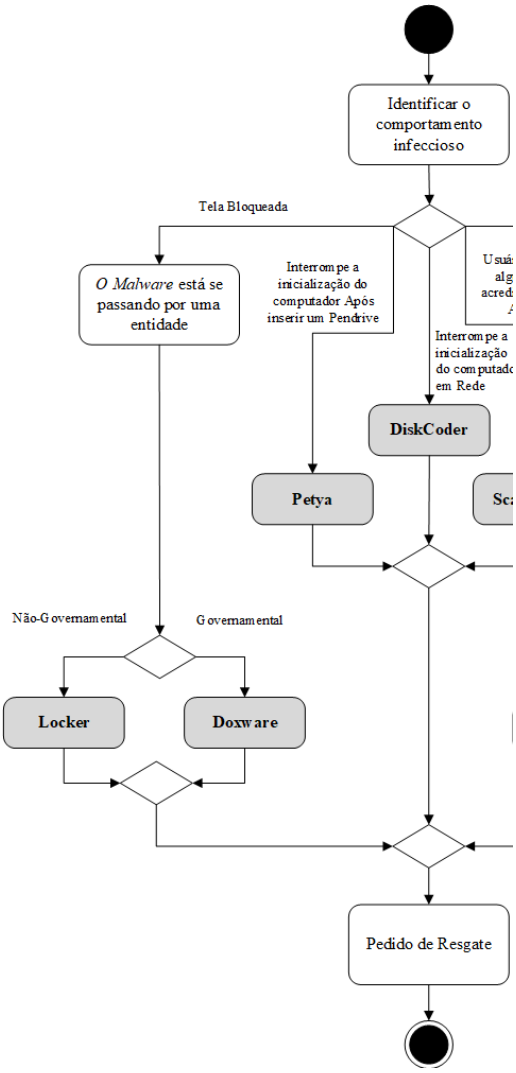


Figura 11 – Detalhamento do Fluxo Direito

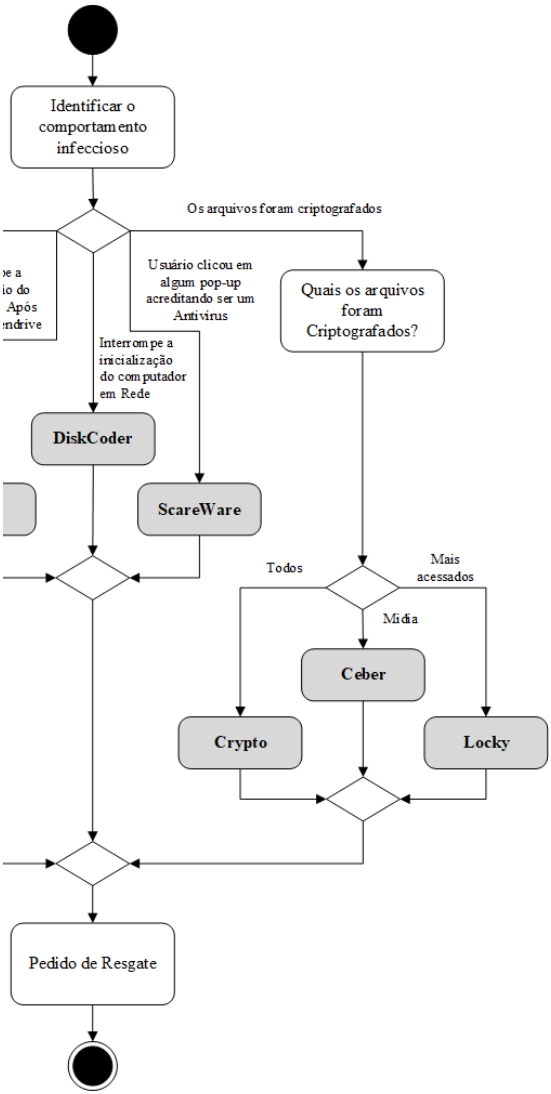


Figura 12 – Detalhamento do Fluxo Inferior Esquerdo

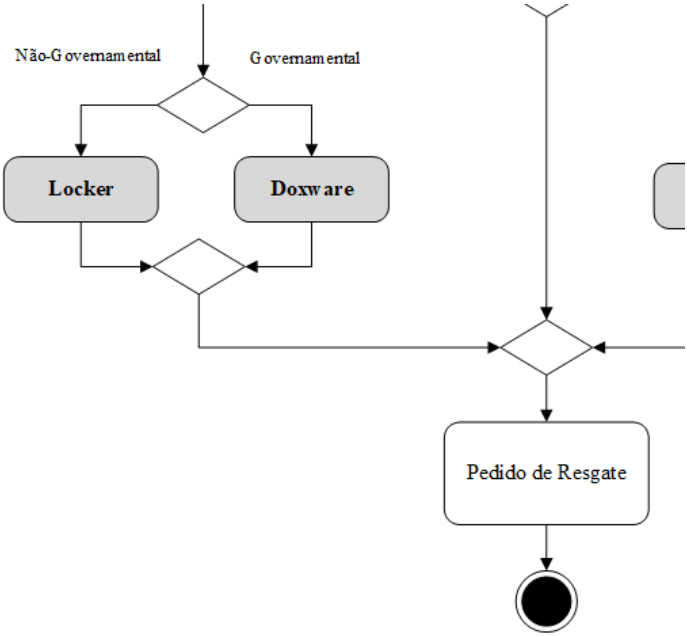
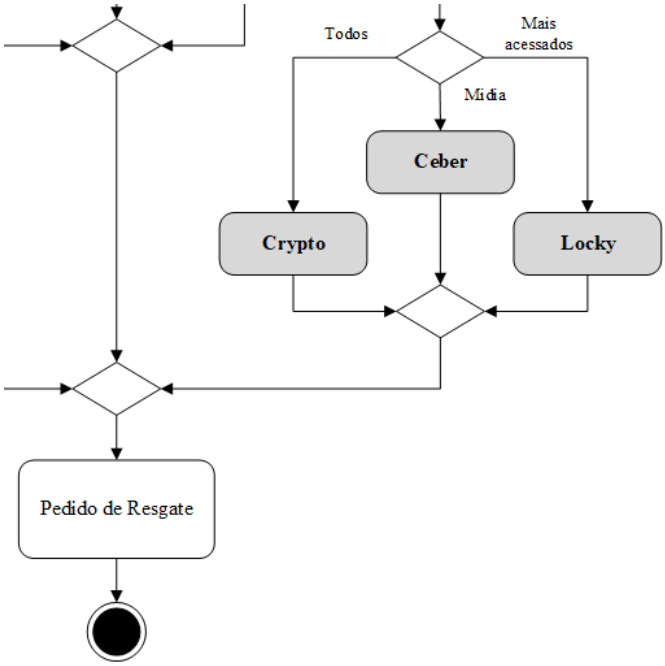


Figura 13 – Detalhamento do Fluxo Inferior Direito



5. Conclusões

O mercado do *Ransomware* tem crescido cada vez mais e consequentemente se tornado mais lucrativo para os criminosos, o que ocasiona grande investimento de tempo e dinheiro destes para aprimorar as tecnologias cada vez mais.

As empresas e usuários devem seguir a evolução da criminologia, evoluindo também seus métodos de proteção. É importante investir em métodos de resposta e continuidade à *Ransomware*, mas é muito mais importante que isso investir em conscientização e prevenção. Pois mesmo conseguindo mitigar a ameaça, uma vez que este infecta o computador pode trazer outros tipos de ataque ou ocasionar vazamento de dados.

Decorrente da vergonha ou até mesmo medo ocasionado por um ataque *Ransomware*, grande parte das empresas não divulgam detalhes sobre o ocorrido, mas é importante que isso seja feito para que profissionais de segurança fora desta possam estudar e entender possíveis

novas variantes de *Ransomware* ou evoluções e mudanças de comportamento das variantes já existentes.

A contribuição para a teoria está em apresentar as formas de ataques dos principais tipos de *Ransomware*. A contribuição para a prática é alertar os gestores e gerentes de segurança da informação das formas de ataques.

Referencial Bibliográfico

ABC, Diário do (2021). Ataque cibernético prejudica vendas da CVC há cinco dias, SP. Editora Redação. Disponível em: https://www.dgabc.com.br/ Noticia/3781374/ataque-cibernetico-prejudica-vendas-da-cvc-ha-cinco-dias

Abranet (2023) Ataques *Ransomwares* Continuam Sendo os Preferidos dos Criminosos, SP. Editora Convergência Digital. Disponível em: https://www.abranet.org.br/Noticias/ Ataques-ransomware-continuam-sendo-os-preferidos-dos-criminosos4212.html?UserActiveTemplate=site#ZCd5kHvMLIU.

Advisor, CISO (2023). Cerca de 4 em cada 5 ataques de *Ransomware* têm outras ameaças. BR. Disponível em: https://www.cisoadvisor.com.br/cerca-de-4-em-cada-5-ataques-de-Ransomware-contem-outras-ameacas/

Advisor, CISO (2023). Indústria de *Ransomwar*e já fatura mais de US$ 400 milhões ao ano. BR. Disponível em: https://www.cisoadvisor.com.br/ industria-de-Ransomware-movimenta-mais-de-us-400-mi-ao-ano

Araujo, J (2023). Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. DF. Disponível em: https://www12.senado.leg.br/radio /1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Portanto%2C%20desde%20mar%C3%A7o%20de%202023,dispositivos%20inform%C3%A1ticos%20para%20instalar%20vulnerabilidades

Auler, F & Justo, G (2022). Ataques à propriedade virtual e o seguro cyber. SP. Disponível em: https://www.conjur.com.br/2022-jul-07/seguros-contemporaneos-ataques-propriedade-virtual-seguro-cyber

Avast (2020). *Ransomware Cerber*: Tudo que você precisa saber. Disponível em: https://www.avast.com/pt-br/c-cerber.

Avelino, Y. (2023). *RustBucket*: crackers estariam visando Macs com novo malware. PE. Disponível em: https://macmagazine.com.br/ post/2023/05/05/rustbucket-crackers-estariam-visando-macs-com-novo-malware

AVG (2021). Guia de Proteção e Remoção de *Ransomware*. Disponível em: https://www.avg.com/pt/signal/what-is-Ransomware.

Belcic, I. (2019*). Ransomware Petya:* Como funciona e como se proteger. AVAST. Disponível em: https://www.avast.com/pt-br/c-petya

Berbert. L. (2021). Contra cibercrimes, Brasil passa a ser signatário da Convenção de Budapeste. SP. Disponível em: https://www.telesintese.com.br/brasil-assina-convencao-contra-cibercrimes.

Bertolucci, G. (2019). *Ransomware* causa demissão de 300 funcionários de empresa, MG. Disponível em: https://livecoins.com.br/Ransomware-causa-demissao-300-funcionarios-empresa.

Biancamano, P (2021). 5 prejuízos que um ataque *Ransomware* pode causar a sua empresa. RJ. Disponível em: https://www.psafe.com/blog/5-prejuizos-que-um-ataque-Ransomware-pode-causar-a-sua-empresa/.

Branco, D. (2021). CVC segue com prejuízos em vendas devido a ataque de *Ransomware*. Canaltech. Disponível em: https://canaltech.com.br/ seguranca/cvc-segue-com-prejuizos-em-vendas-devido-a-ataque-de-Ransomware-198352

Brasiline (2023). Microsoft diz rastrear mais de 100 quadrilhas de *Ransomware*. BR. Disponível em: https://brasiline.com.br/blog/microsoft-diz-rastrear-mais-de-100-quadrilhas-de-Ransomware/

Burdova, C. (2022). What Is Eternal Blue and Why Is the MS17-010 Exploit Still Relevant?. London, United Kingdom. Disponível em: https://www.avast.com/c-eternalblue.

Cabette, E (2014). Crime de Invasão de Dispositivo Informático (artigo 154 - A, CP). SP. https://www.jusbrasil.com.br/artigos/crime-de-invasao-de-dispositivo-informatico-artigo-154-a-cp/153070617.

Chieco, B (2019). Everis sofre ataque de *Ransomware.* Disponível em: https://www.mentebinaria.com.br/noticias/portal-mente-bin%C3%A1ria/everis-sofre-ataque-de-Ransomware-r182/.

CNN Brasil (2021). A bizarra história do inventor do *Ransomware;* vírus deixou parte dos EUA sem gás. Disponível em: https://www.cnnbrasil.com.br/economia/a-bizarra-historia-do-inventor-do-Ransomware-virus-deixou-parte-dos-eua-sem-gas/#:~:text= Willems%20esperava%20ver%20pesquisas%20m%C3%A9dicas,dos%20EUA%20na%20semana%20passada.

Cossetti, M. (2023). O que é um *Ransomware*?. RJ. TECNOBLOG. Disponível em: https://tecnoblog.net/responde/o-que-e-um-Ransomware/

Elsad, A. (2022). Threat Assessment: Black Basta Ransomware. USA. Disponível em: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-Ransomware/

Finelli, A. (2016). Por que o *Ransomware* ainda lidera o ranking de ataques?. SP. Conteudo Editorial. Disponível em: https://www.securityreport.com.br/por-que-o-Ransomware-ainda-lidera-o-ranking-de-ataques/

FireEye (2018). Global Ransomware Study, USA. Disponível em: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-global-Ransomware-study.pdf.

Gaidargi, J. (2021). Renner é vítima de *Ransomware* – E se fosse você? SP. Disponível em: https://www.infonova.com.br/seguranca/renner-ransonware-consequencias-solucoes/.

Garcez, J. (2022). Breves Anotações Sobre a Cooperação Jurídica Internacional na Convenção de Budapeste e a Investigação e Persecução de Crimes Cibernéticos. RO. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/58147/breves-anotaes-sobre-a-cooperao-jurdica-internacional-na-conveno-de-budapeste-e-a-investigao-e-persecuo-de-crimes-cibernticos .

Grustniy, L. (2021). A saga do *Ransomware*. RU. Kapersky. Disponível em: https://www.kaspersky.com.br/blog/history-of-Ransomware/17280/.

Guedes, M. (2021). O que é Engenharia Social?, SP. Disponível em: https://www.treinaweb.com.br/blog/o-que-e-engenharia-social.

Inside, TI (2023). Setor Financeiro é o segundo mais atingido por ataque de *Ransomwares*. SP. Disponível em: https://tiinside.com.br/ 06/04/2023/setor-financeiro-e-o-segundo-mais-atingido-por-ataque-de-Ransomwares/.

Inside, TI. (2022). Varejo é o setor mais atacado por *Ransomware*, segundo pesquisa da Sophos. BR. Disponível em: https://tiinside.com.br/ 25/11/2022/cinco-dicas-da-sophos-para-compras-seguras/.

Kapersky (2017). História do Ano de 2017 da Kaspersky Lab: mais de um quarto dos ataques de *Ransomware* visa empresas. SP. Disponível em: https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-more-than-a-quarter-of-Ransomware-attacks-target-companies-in-2017.

Kapersky (2019). *Ransowmare* e cidades: mais de 170 ataques em 2019. SP. Disponível em: https://www.kaspersky.com.br/about/press-releases/2019_ransowmare-e-cidades-mais-de-170-ataques-em-2019 .

Kapersky (2023). Proteção contra *Ransomware*: como manter seus dados seguros em 2023. SP. Disponível em: https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-Ransomware .

Kelly, M. (2021). The bizarre story of the inventor of Ransomware, USA. CNN Business. Disponível em: https://edition.cnn.com/2021/05/16/tech/ Ransomware-joseph-popp/index.html.

Klusaitė, L (2022). *Ransomware:* o que é e como se proteger?. NordVPN. Disponível em: https://nordvpn.com/pt-br/blog/o-que-e-Ransomware/

Laccelva, F. (2021). Os 10 distúrbios psicológicos mais comuns e suas características, SP. Disponível em: https://blog.fepo.com.br/psicologia/os-10-disturbios-psicologicos-mais-comuns-e-suas-caracteristica/.

Lemos, R. (2017). *Ransomware:* O Sequestrador de Dados, RS. Disponível em: https://www.linkedin.com/pulse/Ransomware-o-sequestrador-de-dados-vinicius-m-s-lemos/?originalSubdomain=pt.

Lemos, R. (2020). Ataque ao STJ é sinal de alerta. SP. Folha de São Paulo. Disponível em: https://itsrio.org/pt/artigos/ataque-ao-stj-e-sinal-de-alerta/

Lessing, M. (2020). Case Study: AIDS Trojan Ransomware, USA. Studios Editor. Disponível em: https://www.sdxcentral.com/security/definitions/what-is-Ransomware/case-study-aids-trojan-Ransomware/.

Lessing, M. (2020). Case Study: Reveton Ransomware. USA. Disponível em: https://www.sdxcentral.com/security/definitions/what-is-Ransomware/ case-study-reveton-Ransomware/

McAfee (2022). O que é *Ransomware*?. CA, USA. Disponível em: https://www.mcafee.com/blogs/pt-br/internet-security/8-dicas-para-ficar-protegido-contra-ataques-de-Ransomware/.

McAffe (2021). Threats Report, USA. Disponível em: https://www.mcafee.com/enterprise/en-us/threat-center/threat-reports.html.

Mekauskas, T. (2020). Ransomware Spora. Disponível em: https://www.pcrisk.pt/guias-de-remocao/8473-spora-Ransomware

Meskauskas, T. (2021). Vírus Locker. Lituânia. Disponível em: www.pcrisk.pt/guias-de-remocao/7918-locker-virus.

Moura, B. (2022). Os 14 tipos de *Ransomware* mais perigosos da web. RJ. Disponível em: https://www.psafe.com/blog/os-14-tipos-de-Ransomware-mais-perigosos-da-web/.

Moura, B. (2022). Ransomware Locker: o que é e como evitar. SP. TECNOBLOG. Disponível em: https://www.psafe.com/blog/Ransomware-locker-o-que-e-e-como-evitar/

Mujezinovic, D. (2021) AIDS Trojan: The Story Behind the First Ever Ransomware Attack. Disponível em: https://www.makeuseof.com/aids-trojan-the-first-Ransomware-attack-in-history/.

Nones, F. (2022). LGPD: o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing e vendas. SP. Disponível em: https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/

Osborne, C. (2015). Lockerpin Ransomware steals PINs, locks Android devices permenantly. USA. Disponível em: https://www.zdnet.com/article/ lockerpin-Ransomware-steals-pins-locks-android-devices-permenantly/

Pacete, L (2022). Dados de saúde valem mais que informações financeiras na dark web. Dísponível em:https://forbes.com.br/forbes-tech/2022/06/dados-de-saude-chegam-a-valer-mais-que-informacoes-financeiras-na-dark-web/.

Pacete, L. (2021). 5 ataques cibernéticos no Brasil em 2021 que geraram alerta. SP. Forbes. Disponível em: https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/.

Padeiro (2023) Ransomware As A Service (RaaS) Explained How It Works & Examples, USA. Crowdstrike. Disponível em: https://www.crowdstrike.com/cybersecurity-101/Ransomware/ransom ware-as-a-service-raas/.

PagBank (2023). Malware: saiba o que é e como proteger seus dados!. SP. Disponível em: https://blog.pagseguro.uol.com.br/o-que-e-malware/.

Paiva, C. (2023). Cibersegurança existe responsabilidade e diigencia coletivas. MG. Disponível em: https://www.diariodoaco.com.br/noticia/0106554-opiniao-ciberseguranca-exige-responsabilidade-e-diligencia-coletivas.

Perrone, G. (2018). Cry Brazil: Ransomware sequestra PCs de brasileiros; saiba se proteger, RJ. Disponível em: https://sbackup.online/cry-brazil-Ransomware-sequestra-pcs-de-brasileiros-saiba-se-proteger/.

Poslušný, M (2020). O Ransomware Bitpaymer foi um trabalho dos criadores do Dridex. RJ. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjMv8eRyfX_AhUKrJUCHf_YAMAQFnoECBAQAQ&url=https%3A%2F%2Fwww.welivesecurity.com%2Fbr%2F2018%2F01%2F31%2Ffriedex-o-Ransomware-bitpaymer-foi-um-trabalho-dos-criadores-do-dridex%2F&usg=AOvVaw1kyot0hs4SuvyOJG7FXLDb&opi=89978449.

Prabhu, S. R., & van Wagoner, N (2023). Human Immunodeficiency Virus Infection and Acquired Immunodeficiency Syndrome (HIV/AIDS): An Overview. Sexually Transmissible Oral Diseases, 51.

Ramos, G. (2021). O que é scareware? Entenda o programa malicioso que 'causa medo'. RJ. Disponível em https://www.techtudo.com.br/listas/2021/03/o-que-e-scareware-entenda-o-programa-malicioso-que-causa-medo.ghtml.

Report, Security (2022). Brasil foi o 5º país com mais ataques cibernéticos em 2021. SP. Conteúdo Editorial. Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.ZCisl3vMLIU

Report, Security (2022). Brasil foi o 5º país com mais ataques cibernéticos em 2021. SP. Conteúdo Editorial. Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.ZCisl3vMLIU.

Rivera, J. (2023). How Big Tech enables cybercriminals via 'malvertising'. TO. TORONTO SUN. Disponível em: https://torontosun.com/ opinion/columnists/rivera-how-big-tech-enables-cybercriminals-via-malvertising

Root, E. (2022). As crônicas do WannaCry. Kapersky. Disponível em: https://www.kaspersky.com.br/blog/wannacry-history-lessons/19960/.

Schettini, B. (2022). O crime de invasão de dispositivos informáticos (notebooks, netbooks, tablets, smartphones, etc.). JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/o-crime-de-invasao-de-dispositivos-informaticos-notebooks-netbooks-tablets-smartphones-etc/1630463264

Schreiber, A. (2022) O Direito em Tempos de Ciberguerra, RJ. O Globo. Disponível em: https://blogs.oglobo.globo.com/fumus-boni-iuris/post/anderson-schreiber-o-direito-em-tempos-de-ciberguerra.html

Sonicwall. 2023 Cyber Threat Report, CA (USA): Editora SONICWALL. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf.

Souza (2018) Criminologia - origem e evolução. JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/criminologia-origem-e-evolucao/600948002#:~:text=Com%20inicio%20no%20s%C3%A9culo%20XVIII,etiologia%2C%20para%20explicar%20o%20crime.

Srinivas, R (2021). How Cybercriminals Use Phishing Kits, USA. CISO MAG. Disponível em: https://cisomag.com/how-cybercriminals-use-phishing-kits/.

UPX (2021). Ransomware: entenda o caso que abalou a Renner e conheça os diferentes tipos de ciberataques. Disponível em: https://upx.com/ post/Ransomware-renner/.

Ximenes, L (2022). O que é malware? Conheça os tipos mais comuns. Disponível em: https://www.hardware.com.br/artigos/o-que-e-malware-conheca-os-tipos-mais-comuns/#:~:text=Malware%20%C3%A9%20todo%20software%20malicioso,nessa%20categoria%20hoje%20em%20dia.

Autores deste Capítulo

Stephany Victoria Nascimento da Silva

Entusiasta da área de Segurança da Informação. Graduada em Segurança da Informação pela Fatec Santana de Parnaíba e experiência prática. Atua em Gestão de Continuidade de Negócios, onde desenvolve estratégias e implementa medidas para garantir a resiliência e proteção das organizações em face de ameaças cibernéticas. Possui interesse especial em pesquisa e tendências da criminologia digital, combinando expertise técnica e uma abordagem proativa, sua paixão pela compreensão dos aspectos criminológicos no mundo digital impulsiona seu trabalho, permitindo que identifique e analise os padrões e comportamentos dos criminosos cibernéticos. Seu objetivo é contribuir para a proteção da informação e conscientizar sobre os desafios e riscos enfrentados no ambiente digital dedicando-se a enfrentar os desafios emergentes na segurança cibernética

Irapuan Glória Júnior

Pós-doutor e doutor em Engenharia da Produção, mestre em Administração em Gestão de Projetos, com foco em Projetos de TI. É pós-graduado em consultoria em Internet, Administração Pública, Marketing e *Cybersecurity*. Graduado em Análise e Desenvolvimento de Sistemas. Entusiasta em pesquisa e inovação. Autor de 5 livros e publicou diversos artigos científicos no Brasil e no mundo. É revisor de diversos periódicos e editor do *Journal of Technology & Information.* Atua como coordenador de Segurança da Informação na Fatec Santana de Parnaíba. Atuou como coordenador de projetos em empresas como Carrefour, Chipek, Telefônica e New Design.

APÊNDICE

O Símbolo do JTnI

Irapuan Glória Júnior

Marcos de Oliveira Morais

1 Introdução

Fundado em 01/09/2021 o *Journal of Technology & Information* foi criado com o intuído de fomentar a pesquisa científica nas diversas áreas do conhecimento, idealizada por dois pesquisadores que trazem para o escopo da revista o compartilhamento de temas relevantes e atuais.

A nossa logomarca foi idealizada de forma a apresentar o aspecto tecnológico, com todo o movimento cibernético atual, e a representação da árvore com suas raízes profundas e frutos, resultando em uma árvore do conhecimento digital.

A árvore encontra-se protegida por um escudo, digno de uma fortaleza, da solidez e firmeza em todos os momentos.

Assim, o símbolo sempre nos lembra do compromisso de propagar os frutos do conhecimento de maneira sólida, robusta e firme, para que os leitores possam usufruir do conhecimento apresentado.

Irapuan Glória Júnior

Marcos de Oliveira Morais


Team
Success
IDEA