Malwares e Crackers: Uma Análise Bibliográfica sobre Segurança em Redes de Computadores

Waynner Fernandes Rodrigues Pessoa

PROJETO DE CONCLUSÃO DE CURSO

Data de Depósito: 20/11/2023

Assinatura: _____

Malwares e Crackers: Uma Análise Bibliográfica sobre Segurança em Redes de Computadores

Waynner Fernandes Rodrigues Pessoa

Willyan Michel Ferreira

Monografia apresentada ao Centro Universitário de Formiga - UNIFOR, como requisito parcial para obtenção do título de bacharel em Ciência da Computação, sob a orientação do Prof Willyan Michel Ferreira.

Unifor-MG - Formiga
20 de novembro de 2023

À minha família, amigos e todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia.

Agradecimentos

Aos meus pais, por nunca ter medido esforços para me proporcionar um ensino de qualidade durante todo o meu período escolar.

Ao meu orientador, Willyan que conduziu o trabalho com paciência e dedicação, sempre disponível a compartilhar todo o seu conhecimento.

Às pessoas com quem convivi a longo desses anos de curso, em especial a minha namorada, Ana Clara, que me incentivou e que certamente tive impacto na minha formação acadêmica, e compreendeu a minha ausência enquanto eu me dedicava à realização deste trabalho.

Aos meus colegas de curso, cm quem convivi intensamente durante os últimos anos, pelo companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando.

"A tragédia não é quando um homem morre. A tragédia é o que morre dentro de um homem quando ele está vivo."

Albert Schweitzer

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

CPF - *Cadastro de Pessoa Física*
CRAMM - *CCTA Risk Analysis and Management Method*
DDoS - *Distributed Denial of Service*
GDPR - *General Data Protection Regulation/Regulamentação Geral de Proteção de Dados*
IA - *Inteligencia Artificial*
IaaS - *Infrastructure as a Service*
IDS - *Intrusion Detection System*
IoT - *Internet of Things*
IP - *Internet Protocol*
IPS - *Intrusion Prevention System*
ISO - *International Organization for Standardization*
LGPD - *Lei Geral de Proteção de Dados*
MTTR - *mean time to repare*
NIST - *National Institute of Standards and Technology*
OCTAVE - *Operationally Critical Threat, Asset and Vulnerability Evaluation*
PaaS - *Platform as a Service*
RG - *Registro Geral*
SaaS - *Software as a Service*
SASE - *Secure Access Service Edge*
SGs - *Smart Grids*
SGSI - *Sistema de Gestão de Segurança da Informação*
SSO - *Single Sign-on*
TI - *Tecnologia da Informação*

Resumo

PESSOA, W. F. R. *Segurança da Informação.* Monografia (Graduação) — Centro Universitário de Formiga – UNIFOR-MG – Formiga, 2023.

Este estudo abrange a vital importância da segurança da informação na era digital, explorando princípios, desafios e estratégias essenciais para proteger dados em um mundo cada vez mais conectado. Ele contextualiza a evolução dessa segurança, destacando a necessidade crescente de proteger informações confidenciais e garantir a integridade, disponibilidade e autenticidade dos dados. Analisa uma gama de ameaças cibernéticas atuais, como *malware*, *phishing* e ataques de negação de serviço (DDoS), oferecendo estudos de caso para evidenciar suas consequências e a importância de estratégias proativas para mitigá-las. Explora detalhadamente estratégias de proteção, como *firewalls*, criptografia e autenticação de dois fatores, incluindo exemplos de implementações bem-sucedidas. Discute a conformidade com regulamentações, como GDPR, LGPD e ISO 27001, enfatizando a importância de políticas de segurança robustas. Aborda a gestão de riscos, destacando a necessidade de planos de contingência e recuperação de desastres. Por fim, explora as tendências futuras, como inteligência artificial e internet das coisas, e seus impactos na segurança da informação, ressaltando desafios emergentes e a necessidade contínua de adaptação das estratégias de proteção de dados.

Palavras-chave: Segurança da Informação, Proteção de Dados, Cibersegurança, Princípios de Segurança, Ameaças Cibernéticas.

Abstract

PESSOA, W. F. R. *Segurança da Informação.* Monografia (Graduacao) — Centro universitario de Formiga – Unifor-mg – Formiga-MG, 2023.

This study covers the vital importance of information security in the digital age, exploring essential principles, challenges, and strategies to safeguard data in an increasingly connected world. It contextualizes the evolution of this security, emphasizing the growing need to protect confidential information and ensure the integrity, availability, and authenticity of data. It analyzes a range of current cyber threats such as malware, phishing, and denial-of-service attacks (DDoS), offering case studies to illustrate their consequences and the importance of proactive strategies to mitigate them. It extensively explores protection strategies like firewalls, encryption, and two-factor authentication, including examples of successful implementations. It discusses compliance with regulations such as GDPR, LGPD, and ISO 27001, highlighting the importance of robust security policies. It addresses risk management, emphasizing the need for contingency plans and disaster recovery. Lastly, it delves into future trends like artificial intelligence and the Internet of Things, and their impacts on information security, highlighting emerging challenges and the continuous need to adapt data protection strategies.

Keywords: Information Security, Data Protection, Cybersecurity, Security Principles, Cyber Threats.

Capítulo

1

Introdução

No cenário contemporâneo, segundo Andress (2014) a segurança da informação é um elemento fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados em qualquer organização. Com o avanço exponencial da tecnologia e a interconexão global, as ameaças cibernéticas têm se tornado mais sofisticadas e persistentes, desafiando constantemente as estratégias de proteção de dados.

Diante disso se viu importante a produção dessa revisão bibliográfica para buscar e explorar as falhas da segurança da informação, analisando metodologias, desafios e tendências atuais nesse campo crucial. Desde os princípios fundamentais da criptografia e autenticação até os recentes avanços em inteligência artificial aplicada à detecção de ameaças, esta revisão busca fornecer uma visão panorâmica das abordagens mais relevantes e eficazes para proteger sistemas, redes e informações sensíveis.

Ao longo deste estudo, serão examinados trabalhos acadêmicos, pesquisas, padrões industriais e práticas recomendadas, com o intuito de mapear o panorama atual da segurança da informação. Serão também destacados os desafios emergentes, como a crescente sofisticação de ataques de *malware*, *phishing* e engenharia social e a necessidade de políticas robustas de governança de dados.

De acordo com Skopik, Settanni e Fiedler (2016) a compreensão aprofundada desses tópicos é essencial para o desenvolvimento de estratégias proativas e eficazes de segurança da informação, a fim de guardar ativos digitais e preservar a confiança dos usuários, em um ambiente cada vez mais interconectado e vulnerável a ameaças cibernéticas.

1.1 Objetivos

Objetivo Geral:

Produzir uma revisão bibliográfica com o intuito de explorar as tendências, desafios e avanços

atuais na área de segurança da informação, investigando as principais estratégias, tecnologias e melhores práticas utilizadas para proteger sistemas, dados e informações sensíveis contra ameaças cibernéticas, visando oferecer uma compreensão abrangente do panorama atual e suas implicações para a proteção digital em diversos setores.

Objetivos Específicos:

O estudo tem como foco conscientizar os usuários e se manterem informados sobre proteger seus dados, ele visa entender melhor os perigos dos ataques de *malware*, os ataques DDoS, assim como explicar sobre as inteligências artificiais e como elas podem ajudar os usuários a se protegerem contra possíveis ataques, além disso informar os usuários de como a segurança da informação está diretamente ligada com os aspectos humanos, e quais os desafios enfrentados para manterem seus dados seguros em um mundo que está se tornando cada vez mais tecnológico.

1.2 Justificativa

Nos últimos anos, o campo da segurança cibernética tem enfrentado desafios crescentes, impulsionados pelas constantes evoluções tecnológicas e ameaças cada vez mais sofisticadas.

O Brasil possui aproximadamente 214 milhões de habitantes, segundo Santos (2022) 81% da população brasileira possui acesso a internet, de acordo com ele em 2022 65% dos ataques e vazamentos de dados envolvem o roubo de identidade, como número de CPF e RG.

Devido a falta de informação e de conhecimento dos usuários, a segurança se torna uma tarefa difícil, pois por consequência dessa falta de informação as senhas se tornam mais fáceis de serem decifradas por invasores. Em 2021 aproximadamente 530 milhões de usuários do Facebook tiveram seus dados roubados, entre os dados que os invasores tiveram acesso estão número de CPF, nome de usuário e senha dos usuários. (ROSA, 2021)

Essa revisão bibliográfica se torna um pilar fundamental nesse contexto dinâmico, oferecendo uma oportunidade única para compreender o estado atual das práticas, tecnologias e desafios presentes na segurança da informação. O principal objetivo desta revisão é não apenas atualizar o conhecimento, mas também identificar tendências emergentes e inovações recentes neste campo em constante transformação.

Além de sua contribuição para a pesquisa, esta revisão busca educar e conscientizar um público amplo sobre os desafios e as melhores práticas de segurança da informação, garantindo a disseminação de informações valiosas para profissionais, acadêmicos e interessados neste campo em constante evolução.

1.3 Estrutura da Monografia

Essa revisão bibliográfica foi dividida em 4 capítulos.

No primeiro capítulo está presente a introdução, onde é introduzido o objetivo geral e o objetivo específico, juntamente com a justificativa para o desenvolvimento dessa revisão bibliográfica.

No segundo capítulo está de fato a revisão bibliográfica, contendo os tópicos principais para

a segurança da informação. É nesse capítulo que estão os tipos de ataques, como o ser humano está diretamente ligado com a segurança da informação, assim como as forma de se proteger e identificar os possíveis ataques que pode surgir contra o usuário.

No terceiro capítulo está presente a discussão, onde é apresentado as dificuldades enfrentadas durante a realização dessa revisão, assim como também uma comparação entre dois tópicos presentes na revisão.

No quarto e último capítulo foi apresentado os resultados dessa revisão, é nesse tópico que está sendo informado a quantidade de artigos pesquisados, a quantidade de artigos que foram realmente utilizado, os países em que os artigos foram publicados, e por fim a conclusão da presente revisão.

Capítulo

2

Revisão Bibliográfica

2.1 Conceitos fundamentais de Segurança da informação

A segurança da informação é um conjunto de práticas que visam a proteção de informações e dados pessoais de empresas e pessoas, está juntamente ligada a Lei Geral de Proteção de Dados[1]. A LGPD é uma lei que foi criada para proteger os direitos de liberdade e de privacidade dos usuários que utilizam a internet e outros meios digitais, a quebra dessa lei pode resultar em multas simples.

Embora a segurança seja considerada uma necessidade fundamental nas empresas, as abordagens sobre o nível adequado variam substancialmente entre as organizações. Muitas vezes, o investimento em segurança é encarado como um custo sem benefícios claros para o negócio, levando à busca pela minimização desses custos. Para atingir esse objetivo, é crucial implementar estratégias de segurança voltadas para a proteção do que é considerado essencial.(CONCEIÇÃO, 2019)

A norma ISO 27001, ao estabelecer diretrizes para a criação, implementação, manutenção e melhoria contínua de sistemas de gerenciamento de segurança da informação, destaca os 3 princípios da segurança da informação, que são eles:(ISO, 2022)

- **Confidencialidade:** Esse pilar está ligado diretamente com a proteção dos dados, permitindo o acesso a determinados dados somente por pessoas autorizadas.
- **Integridade:** É nesse pilar que deve garantir que as informações não possam ser alteradas por pessoas sem autorização, assim mantendo as informações verdadeiras.
- **Disponibilidade:** Permite que os dados sejam acessados quando precisar, mas mantendo os princípios dos demais pilares.

[1] A LGPD tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

2.1.1 Confidencialidade

A importância da confidencialidade, também referida como exclusividade, transcende a simples restrição de acesso a informações específicas. Trata-se de um princípio fundamental no âmbito da segurança da informação, essencial para resguardar dados sensíveis em diversos contextos. No cenário empresarial, executivos enfrentam a constante necessidade de proteger os planos estratégicos de suas organizações contra a espionagem competitiva, assegurando que informações cruciais permaneçam restritas aos colaboradores autorizados.(HINTZBERGEN et al., 2018)

A confidencialidade é um princípio fundamental na segurança da informação, com raízes profundamente ancoradas em uma mentalidade militar que preconiza uma autoridade hierárquica estrita e controle rigoroso sobre aqueles que têm acesso à informação, de acordo com uma necessidade específica de conhecimento.(CAMP, 1999)

Além disso, a confidencialidade estende-se ao âmbito pessoal, onde indivíduos estão cada vez mais preocupados com a segurança de seus registros financeiros. A garantia de que apenas pessoas autorizadas tenham acesso a essas informações é crucial para evitar possíveis violações de privacidade e proteger os dados pessoais contra usos indevidos.(HINTZBERGEN et al., 2018)

No contexto da segurança cibernética, a confidencialidade não é uma medida estática; ao contrário, é uma salvaguarda dinâmica que deve persistir em todas as etapas do processamento de dados. Isso abrange desde o armazenamento seguro em sistemas e dispositivos de rede até a transmissão segura e a chegada segura ao destino. A implementação eficaz desse princípio contribui para a construção de uma rede robusta de proteção contra ameaças cibernéticas, garantindo a integridade e a confidencialidade dos dados em todos os momentos.(HINTZBERGEN et al., 2018)

2.1.2 Integridade dos Dados

Integridade na segurança da informação refere-se à garantia de que os dados permaneçam precisos, não alterados e confiáveis ao longo de seu ciclo de vida. Este aspecto essencial da segurança da informação assegura que as informações estejam protegidas contra modificações ou adulterações não autorizadas. O princípio da integridade é crucial para manter a confiança nos dados, especialmente em ambientes nos quais a precisão da informação é fundamental.(SAMONAS; COSS, 2014)

Na segurança da informação, a integridade é frequentemente alcançada por meio da implementação de diversas salvaguardas e controles. Estes podem incluir técnicas de criptografia, assinaturas digitais, controles de acesso e trilhas de auditoria. A criptografia ajuda a proteger os dados contra alterações durante a transmissão, enquanto as assinaturas digitais fornecem um meio de verificar a autenticidade e integridade de uma mensagem ou documento. Controles de acesso restringem permissões para modificar dados, e trilhas de auditoria permitem o rastreamento de alterações, assegurando a responsabilização.(YEE; ZOLKIPLI, 2021)

Preservar a integridade da informação é vital em diversos setores, incluindo finanças, saúde e governo, onde a precisão dos dados é crucial para tomada de decisões e conformidade regu-

latória. As organizações devem estabelecer e aplicar políticas e procedimentos que priorizem a integridade dos dados para evitar alterações não autorizadas e manter a confiabilidade dos ativos de informação.(SAMONAS; COSS, 2014)

2.1.3 Disponibilidade das Informações

Disponibilidade na segurança da informação diz respeito à garantia de que os dados e sistemas de informação estejam acessíveis e utilizáveis quando necessário. Esse aspecto da segurança foca em prevenir e minimizar interrupções nos serviços de informação, assegurando que usuários autorizados possam acessar de forma confiável os recursos de informação necessários.(LIMA; FERREIRA; PEIXOTO, 2022)

Para manter a disponibilidade, as medidas de segurança da informação frequentemente incluem estratégias como sistemas redundantes, procedimentos de backup e recuperação, e um design de infraestrutura robusto. Sistemas redundantes oferecem caminhos alternativos para dados no caso de falha de um sistema, minimizando o tempo de inatividade. Procedimentos de backup e recuperação envolvem a cópia regular de dados e processos para restaurar informações rapidamente em caso de perda ou falha do sistema. O design robusto da infraestrutura considera fatores como escalabilidade e confiabilidade, garantindo que os sistemas de informação possam lidar com diferentes níveis de demanda sem comprometer o desempenho.(SILVA et al., 2011)

Assegurar a disponibilidade da informação é crucial para a continuidade dos negócios, eficiência operacional e satisfação do usuário. As organizações devem avaliar os riscos potenciais e implementar medidas proativas para mitigar o impacto de eventos como falhas de hardware, ataques cibernéticos ou desastres naturais que poderiam interromper o acesso à informação. Ao priorizar a disponibilidade em suas práticas de segurança da informação, as organizações conseguem manter a funcionalidade de seus sistemas e serviços, mesmo em circunstâncias desafiadoras.(LIMA; FERREIRA; PEIXOTO, 2022)

2.2 Ameaças à Segurança da Informação

Com a crescente sofisticação das tecnologias e a proliferação de dispositivos de conexão à internet, como notebooks, smartphones e tablets e *IPads*, o uso de redes sociais não seguras e têm contribuído para um aumento significativo nas ameaças a segurança. Uma ameaça adicional aos sistemas de segurança da informação é representada pelo chamado risco interno. Essas tendências emergentes abrem espaços para que os cibercriminosos explorarem novas oportunidades.(GAMA, 2021)

O desafio internacional enfrentado por governos, organizações e empresas é fornecer medidas de cibersegurança preventivas e protetoras adequadas para todos os tipos de informações e serviços, em um cenário onde as fronteiras digitais transcendem as fronteiras físicas. Consequentemente, há uma crescente inclinação para uma abordagem internacional coordenada, visando regulamentar, controlar, combater e processar cibercriminosos.(ELMRABIT; YANG; YANG, 2015)

No entanto, a natureza intrinsecamente aberta e desimpedida do ciberespaço apresenta um dilema, pois a essência da cibersegurança colide com a natureza incontrolável do ambiente

digital.(ALDAAJEH et al., 2022)

Segundo Sen et al. (2013) existem diversos tipos de ataques que os invasores usam para coletar informações de forma ilegal, na Tabela 2.1 estão listados os tipos de ataques assim como também uma breve descrição do objetivo de cada um.

Tabela 2.1: Tipos de Ataques

Tipo	**Descrição**
Malware	Dispositivo que se infiltra na máquina e rouba as informações.
Phishing	É uma forma de conseguir informações sigilosas como senhas de cartões ligando para a pessoa e se passando por um funcionário do banco.
Engenharia Social	Induz o usuário a enviar dados confidenciais, e infectar os computadores com *malwares*.
Ataques DDoS	É um ataque que provoca uma sobrecarga no sistema fazendo com que ele fique indisponível.

Fonte: (SEN et al., 2013)

2.2.1 Crackers

Os crackers, no mundo da informática, segundo Taewee (2011) são indivíduos habilidosos que utilizam seus conhecimentos em programação e sistemas para invadir redes, quebrar senhas e acessar informações sensíveis de maneira ilegal. Diferentemente dos hackers, que podem empregar suas habilidades para aprimorar a segurança digital, os crackers têm motivações maliciosas. Eles exploram vulnerabilidades em sistemas, causando danos, roubo de dados e interrupções em serviços online.

De acordo com Richet (2013) essas ações ilícitas incluem invasões a redes corporativas, roubo de informações pessoais e financeiras, disseminação de *malware* e realização de ataques cibernéticos. O objetivo dos crackers muitas vezes é financeiro, mas também podem ser motivados por desafios técnicos ou simplesmente por causar estragos.

É essencial distinguir entre *crackers* e *hackers* éticos ou *white hat hackers*, que trabalham para fortalecer a segurança cibernética, identificando e corrigindo vulnerabilidades antes que sejam exploradas por indivíduos mal-intencionados. Enquanto os crackers representam uma ameaça à segurança digital, os hackers éticos desempenham um papel fundamental na proteção de sistemas e dados.(EPSTEIN; TANCER, 1996)

2.2.2 Malware

Nos últimos anos, a sociedade como um todo incorporou o uso da Internet em sua rotina diária. Essa integração se tornou praticamente indispensável, uma vez que quase todas as atividades, desde interações sociais até transações bancárias online, dependem da conectividade digital. No entanto, à medida que a Internet cresceu rapidamente, os criminosos também migraram para esse ambiente virtual, abandonando, em parte, o cenário físico.(ASLAN; SAMET, 2020)

Os criminosos cibernéticos, em sua maioria, recorrem ao uso de softwares maliciosos para executar ataques virtuais nos dispositivos das vítimas. O termo geral para qualquer software que intencionalmente introduza cargas maliciosas em máquinas-alvo, como computadores, smartphones e redes, é *malware*. Esse espectro abrange uma variedade de ameaças, como vírus, *worms*, cavalos de Troia, *rootkits* e *ransomware*, cada um projetado com propósitos específicos.(YE et al., 2017)

A complexidade do cenário de cibersegurança é agravada pelo fato de que a classificação de *malware* se torna uma tarefa desafiadora. Algumas instâncias de *malware* apresentam características de várias classes simultaneamente, tornando a identificação e resposta mais difícil para os profissionais de segurança digital. Esse ambiente dinâmico exige constantes atualizações nas estratégias de defesa, uma vez que os criminosos digitais continuam a aprimorar suas táticas e técnicas para contornar as medidas tradicionais de segurança. O desafio reside não apenas em entender as nuances de cada tipo de *malware*, mas também em antecipar as evoluções e combinações que surgem constantemente no cenário cibernético em rápida mudança.(ASLAN; SAMET, 2020)

O *malware* de nova geração tem a capacidade de executar suas atividades evasivas, contornando facilmente softwares de proteção que operam em modo *kernel*, incluindo *firewalls* e antivírus. Enquanto o *malware* tradicional frequentemente consiste em um único processo sem grandes artifícios para ocultação, o *malware* de nova geração adota uma abordagem mais sofisticada. Utilizando múltiplos processos simultaneamente, sejam eles já existentes ou recém-criados, esse tipo de *malware* emprega técnicas de ofuscação para ocultar sua presença e garantir persistência no sistema.(ASLAN; SAMET, 2020)

O aspecto distintivo do *malware* de nova geração é sua capacidade de lançar ataques mais destrutivos e sofisticados, incluindo ataques direcionados e persistentes que transcendem as capacidades do *malware* tradicional. Durante esses ataques, é comum a utilização de mais de um tipo de *malware*, ampliando a gama de ameaças enfrentadas pelos sistemas de segurança. Essa evolução marca uma mudança significativa no panorama da cibersegurança, demandando estratégias avançadas e proativas para detecção e mitigação eficazes diante dessa nova geração de ameaças digitais.(TAHIR, 2018)

Há também variações de *malwares*, cada uma delas possui uma funcionalidade específica. Algumas delas são:(YE et al., 2017)

- **Ransomware:** Ganha acesso à máquina e posteriormente é exigido um resgate da vítima, para eliminar a ameaça das máquinas;
- **Spyware:** É um software destinado a coletar dados das máquinas infectadas;
- **Adware:** Tem como objetivo gerar receita aos seus desenvolvedores através de anúncios na internet como spam;
- **Worms:** São *malwares* que exploram de falhas da rede para se propagar em vários computadores, assim abrindo portas para outros tipos de *malware*;

- **Cavalo de troia:** É um *malware* que se disfarça de legitimo e infiltra nas máquinas para espionar e roubar dados;
- **Botnets:** Usam de outros *malwares* para infectar uma máquina e acessá-la remotamente.

A Figura 2.1 representa como é feito um ataque de *malware*, ele é realizado da seguinte forma, o usuário baixa algum arquivo em seu computador, junto com esse arquivo baixado está o arquivo infectado, após isso o criminoso consegue acessar as informações do usuário, depois de conseguir o acesso todas as informações são criptografadas e uma quantia em dinheiro é solicitada para liberar as mesmas.

Figura 2.1: Malware

Fonte: https://infob.com.br/o-que-e-ransomware/

2.2.3 Phishing

O *phishing*, é uma prática na qual os criminosos utilizam artimanhas para obter informações sensíveis, como senhas, números de cartão de crédito e dados bancários. Esse método enganoso frequentemente se manifesta por meio de e-mails, mensagens de texto, redes sociais ou até mesmo chamadas telefônicas, onde os golpistas se fazem passar por entidades confiáveis.(RAMZAN, 2010)

Este tipo de fraude, um dos mais antigos e conhecidos na internet, pode resultar em diversos danos para as vítimas, como roubo de identidade, perda financeira, invasão de contas, infecção por *malware*, chantagem e extorsão. Assim, é imperativo adotar medidas para reconhecer e evitar golpes de *phishing*.(HONG, 2012)

O uso de ferramentas de segurança, como software antivírus, é essencial, proporcionando uma camada adicional de proteção contra ameaças online. A educação contínua sobre práticas seguras na internet e treinamentos de conscientização são peças-chave na defesa contra

o *phishing*, capacitando os usuários a discernir e responder adequadamente a tentativas de fraude.(HONG, 2012)

É importante ressaltar que, além das medidas preventivas, a denúncia de tentativas de *phishing* é uma prática útil para ajudar na identificação e mitigação desses ataques. Apesar das leis existentes contra o *phishing*, a natureza global da internet exige esforços coordenados para fazer valer essas regulamentações.(RAMZAN, 2010)

Aqui estão alguns aspectos abrangentes sobre o *phishing*:

- **Engenharia Social:** O *phishing* muitas vezes utiliza técnicas de engenharia social para manipular psicologicamente as vítimas. Os atacantes criam mensagens persuasivas, aproveitando-se de contextos emocionais, autoridade percebida ou urgência para induzir as vítimas a agirem contra seu próprio interesse.(ALEROUD; ZHOU, 2017)

- **E-mails e Mensagens Falsas:** Os cibercriminosos enviam e-mails ou mensagens de texto fraudulentos que aparentam ser de fontes confiáveis, como bancos, empresas ou serviços online populares. Essas mensagens frequentemente contêm links ou anexos que, quando abertos, direcionam a vítima para sites falsos ou instalam *malware* no dispositivo.(CHHIKARA et al., 2013)

- **Websites Falsos:** As vítimas são frequentemente direcionadas a sites fraudulentos que imitam plataformas legítimas. Esses sites são projetados para capturar informações inseridas, como nomes de usuário e senhas, enganando as vítimas para que pensem que estão fornecendo esses dados a uma fonte confiável.(ALEROUD; ZHOU, 2017)

- **Spear Phishing:** Esta é uma variante mais direcionada do *phishing*, conhecida como *spear phishing*, na qual os atacantes personalizam suas mensagens para alvos específicos, como funcionários de uma empresa ou membros de uma organização. Isso aumenta a probabilidade de sucesso do ataque.(ALEROUD; ZHOU, 2017)

- **Clonagem de Sites:** Os sites legítimos são frequentemente clonados pelos atacantes para criar páginas falsas que se parecem exatamente com as originais. Isso confunde as vítimas e facilita a coleta de informações.(KIRDA; KRUEGEL, 2005)

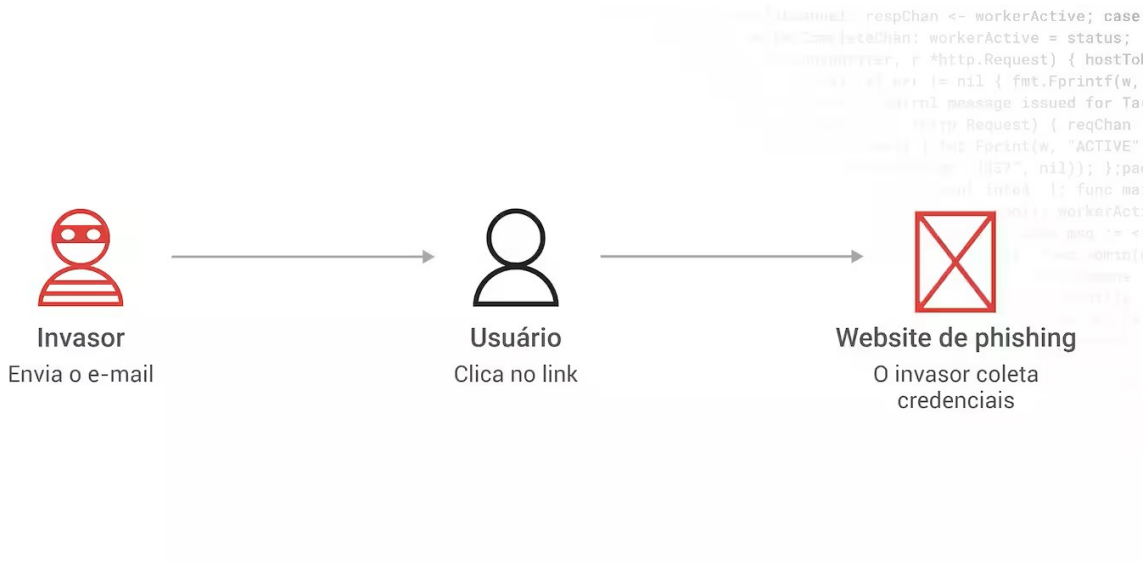
- **Malware:** Além da coleta de informações, o *phishing* também pode ser uma porta de entrada para a instalação de *ransomware* ou *malware* nos dispositivos das vítimas, permitindo que os atacantes acessem dados sensíveis ou até mesmo controlem os sistemas.(QBEITAH; ALDWAIRI, 2018)

- **Prevenção:** A educação e a conscientização são fundamentais para prevenir ataques de *phishing*. As pessoas devem ser instruídas a verificar cuidadosamente a autenticidade de e-mails e mensagens, evitando clicar em links ou baixar anexos de fontes suspeitas. Além disso, as organizações implementam medidas de segurança, como filtros de e-mail e soluções *antiphishing*, para detectar e bloquear tentativas de ataque.(CHHIKARA et al., 2013)

- **Evolução Constante:** Os métodos de *phishing* estão em constante evolução, com os cibercriminosos adaptando suas táticas para contornar as defesas tradicionais. Isso destaca a importância de manter-se atualizado sobre as ameaças cibernéticas e implementar práticas de segurança robustas.(CHHIKARA et al., 2013)

A Figura 2.2 representa como é feito um ataque *phishing*, nesse tipo de ataque, o invasor envia um e-mail para a vítima, contendo um link que levará esse usuário para um site falso, que ao acessá-lo o usuário está liberando o acesso das suas informações pessoais para o invasor, após isso pode ser pedido dinheiro para não divulgar informações sigilosas.

Figura 2.2: Phishing



Fonte: https://www.akamai.com/pt/glossary/what-is-phishing

2.2.4 Engenharia Social

Os ataques de engenharia social estão se espalhando de forma alarmante nas redes atuais, representando uma ameaça significativa à segurança cibernética. Esses ataques visam manipular tanto indivíduos quanto empresas, levando-os a divulgar informações valiosas em favor de criminosos cibernéticos. É interessante notar que a engenharia social desafia as defesas tradicionais, como *firewalls*, criptografia, sistemas de detecção de intrusões e antivírus, independentemente de quão avançadas sejam.(SALAHDINE; KAABOUCH, 2019)

O ponto crítico dessa vulnerabilidade está na tendência humana de confiar mais em outros humanos do que em máquinas ou tecnologias. Isso coloca as pessoas como o elo mais fraco na segurança, sendo exploradas por atividades maliciosas que buscam influenciar psicologicamente para revelarem informações confidenciais ou contornarem procedimentos de segurança.(KALNIŅŠ; PURIŅŠ; ALKSNIS, 2017)

O que torna os ataques de engenharia social únicos é sua capacidade de ameaçar todos os sistemas e redes, independentemente da sofisticação das defesas cibernéticas. Ao contrário de outros tipos de ataques, não podem ser evitados apenas com soluções de software ou hardware, a menos que as pessoas sejam devidamente treinadas para identificar e prevenir essas

táticas.(ALDAWOOD; SKINNER, 2018)

Os criminosos cibernéticos optam por esses métodos quando enfrentam sistemas que parecem ser à prova de falhas tecnicamente. Assim, a conscientização e a educação são cruciais na defesa contra ataques de engenharia social, destacando a importância de entender as nuances psicológicas envolvidas. Em resumo, a luta contra a engenharia social é tão humana quanto técnica, e apenas uma abordagem abrangente pode verdadeiramente fortalecer a resistência contra essas ameaças cada vez mais sofisticadas.(SALAHDINE; KAABOUCH, 2019)

Quando se trata de lidar com possíveis ataques por meio de chamadas telefônicas, é essencial adotar uma abordagem cuidadosa e proativa. Imagine verificar a origem das chamadas, como você faria ao consultar sua lista de contatos gravados, mantendo-se atento a chamadas que surgem de maneira inesperada ou não solicitada. Em situações assim, é sempre válido solicitar que a pessoa ligue de volta ou fazer algumas perguntas que apenas alguém legítimo seria capaz de responder.(OSUAGWU et al., 2015)

É interessante notar que, na maioria das vezes, a maneira mais eficaz de lidar com esses ataques é simplesmente não atender chamadas que parecem suspeitas. É como confiar em seu instinto para proteger sua segurança.(SYAFITRI et al., 2022)

Quando falar de ataques ao serviço de atendimento, considerar a atribuição de senhas a chamadores conhecidos é como adicionar uma camada extra de proteção. Isso cria uma espécie de código secreto entre você e os chamadores de confiança, afastando potenciais ameaças.(OSUAGWU et al., 2015)

Além disso, é importante educar as pessoas sobre essas práticas. Afinal, ao entender os riscos associados às chamadas telefônicas e como tomar medidas preventivas, todos se tornam mais resistentes contra possíveis ameaças de engenharia social. É como dar poder às pessoas para protegerem a si mesmas.(FOOZY et al., 2011)

2.2.5 Ataques DDoS

Os ataques distribuídos de negação de serviço (DDoS) são como tempestades digitais que representam uma ameaça real para nossas redes, ambientes digitais e estruturas cibernéticas. Eles têm o poder de causar interrupções massivas em qualquer lugar onde a tecnologia da informação e comunicação esteja presente.(BAWANY; SHAMSI; SALAH, 2017)

Os ataques DDoS têm a capacidade de paralisar redes e serviços ao sobrecarregar servidores, links de rede e dispositivos como roteadores e *switches* com um volume esmagador de tráfego ilegítimo. Isso pode resultar em desde uma simples degradação do serviço até uma negação total de serviço, causando enormes prejuízos. À medida que nos tornamos cada vez mais dependentes da internet e de data centers, essa ameaça se torna ainda mais séria.(OTTIS, 2008)

Destaca a urgência de encontrar soluções eficazes para se proteger contra esses ataques DDoS. Por exemplo, os data centers que sustentam serviços críticos, como as *smart grids*, precisam ser protegidos para garantir a continuidade na prestação de serviços confiáveis. Isso destaca a necessidade de abordagens inovadoras e proativas para enfrentar essa ameaça persistente em um mundo onde a tecnologia desempenha um papel central em nossa vida cotidiana.(BAWANY; SHAMSI; SALAH, 2017)

Detectar e mitigar ataques de negação de serviço distribuídos (DDoS) é uma preocupação crítica para garantir a segurança e a estabilidade dos sistemas online. Existem várias estratégias utilizadas para enfrentar esse desafio.(LI; LEE, 2005)

Ferramentas especializadas são empregadas para acompanhar padrões incomuns ou picos repentinos de atividade que podem indicar um ataque em curso. Além disso, análises regulares são conduzidas para identificar padrões de tráfego malicioso, como solicitações excessivas de um único endereço IP ou comportamentos de pacotes fora do comum. Sistemas de alerta automático também são implementados para notificar imediatamente a equipe de segurança sobre atividades suspeitas.(CHANG, 2002)

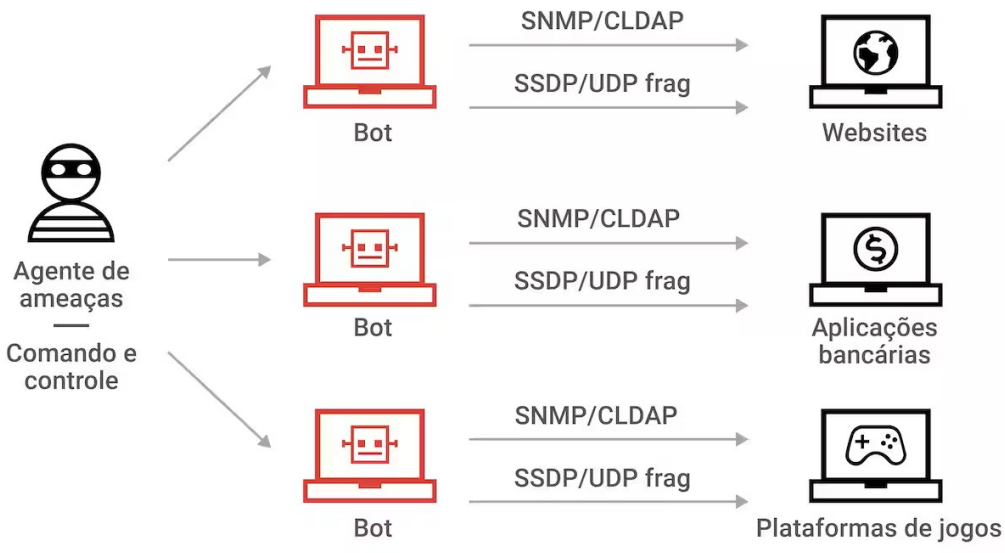
A mitigação de ataques DDoS envolve uma variedade de estratégias. O uso de *firewalls* e filtros de pacotes é comum para filtrar tráfego indesejado com base em endereços IP, protocolos ou tipos de tráfego. Além disso, redirecionar o tráfego por meio de serviços de mitigação especializados pode ajudar a distinguir entre tráfego legítimo e malicioso, bloqueando ou redirecionando solicitações suspeitas.(LI; LEE, 2005)

Projetar a rede para lidar com picos de tráfego, implementando redundâncias e escalabilidade, é fundamental para absorver volumes incomuns de solicitações. A limitação de taxa também é uma estratégia eficaz, impondo limites ao número de solicitações que um único endereço IP pode fazer em um determinado período.(BAWANY; SHAMSI; SALAH, 2017)

Outra abordagem é o uso de serviços especializados de proteção contra DDoS oferecidos por provedores que possuem a infraestrutura e a expertise necessárias. Além disso, a colaboração estreita com provedores de internet é essencial, permitindo uma resposta coordenada e eficaz diante de ataques em larga escala.(CHANG, 2002)

A Figura 2.3 representa como é feito um ataque DDoS, nesse ataque, um invasor consegue acesso a vários *bots* que serão responsáveis por tentar acessar diversos sites e sistemas assim causando a queda do servidor. Em grandes empresas essa queda de servidor por mais rápida que seja resolvida poderá causar prejuízos de milhares de reais.

Figura 2.3: Ataque DDoS



Fonte: https://www.akamai.com/pt/glossary/what-is-ddos

2.2.6 Smart Grids

A implementação das Redes Inteligentes (Smart Grids - SGs) marcou um avanço significativo na inteligência e na operação eficiente dos sistemas elétricos. Essas redes possibilitam um fluxo de informações bidirecional entre diversas unidades no sistema, promovendo uma verdadeira revolução na indústria de energia. Essa revolução se traduz em uma coleta abrangente de dados, desde a medição inicial até as subestações, distribuição, transmissão e geração de energia.(AMIN; WOLLENBERG, 2005)

O objetivo desse aprimoramento é na inserção de processadores em cada componente dos sistemas de energia. Cada componente é equipado com um sistema operacional robusto e agentes independentes conectados a sensores inteligentes específicos, formando assim uma plataforma de computação distribuída em larga escala. Essa abordagem permite que cada componente acesse suas próprias condições operacionais, compartilhando essas informações com agentes vizinhos por meio de caminhos de comunicação, circuitos de disjuntores e portas de comunicação nos processadores.(CAMARINHA-MATOS, 2016)

Essa arquitetura proporciona não apenas maior eficiência e controle, mas também aprimora a segurança, resiliência e monitoramento de ativos e serviços. A capacidade adaptativa e a comunicação efetiva entre os diversos componentes resultam em uma infraestrutura elétrica mais ágil, confiável e eficaz. A introdução de Redes Inteligentes é, portanto, um marco crucial na modernização e otimização do setor energético.(OTUOZE; MUSTAFA; LARIK, 2018)

Em todo o mundo, os sistemas de energia convencionais estão passando por uma atualização significativa para oferecer vantagens cruciais, tais como confiabilidade, segurança e flexibilidade na distribuição de energia, monitoramento do consumo de energia, gerenciamento da demanda, otimização aprimorada do tráfego na rede, períodos de inatividade reduzidos, falhas minimizadas, perdas na rede reduzidas, fornecimento e demanda regulamentados, e, de forma geral,

melhorias nas operações e serviços da rede elétrica.(MENDEL et al., 2017)

Com a crescente disponibilidade de tecnologias avançadas de computação, comunicação e medição, a resposta de emergência do sistema será grandemente aprimorada. As SGs também oferecem proteções que não são fornecidas pelos sistemas de controle central ou pelos esquemas de proteção convencionais para a infraestrutura de energia, tanto do ponto de vista das concessionárias quanto para residências inteligentes.(OTUOZE; MUSTAFA; LARIK, 2018)

Essas inovações não apenas elevam a eficiência e a confiabilidade do sistema elétrico, mas também abrem caminho para uma gestão mais efetiva da demanda de energia e para a integração harmoniosa de casas inteligentes. As SGs não são apenas uma modernização da infraestrutura elétrica; elas representam uma mudança fundamental em direção a um sistema mais inteligente, responsivo e adaptável, moldando o futuro da distribuição de energia de maneira mais eficiente e segura.(MENDEL et al., 2017)

2.3 Controle de Acesso

O controle de acesso desempenha um papel fundamental na segurança da informação, sendo essencial para proteger dados sensíveis e evitar acessos não autorizados a sistemas e informações confidenciais. Essa prática envolve uma série de medidas projetadas para assegurar que apenas usuários autorizados tenham permissão para acessar recursos específicos, ao mesmo tempo em que restringe ou nega o acesso a usuários não autorizados.(TOURANI et al., 2017)

O processo de controle de acesso inicia-se com a identificação do usuário, geralmente por meio de um nome de usuário único ou identificador. Em seguida, ocorre a autenticação, onde os usuários precisam comprovar sua identidade, podendo ser por senhas, *tokens*, biometria ou métodos multifatoriais.(BANERJEE; NAUMANN, 2005)

Após a autenticação bem-sucedida, o sistema verifica as permissões do usuário para determinar quais recursos e informações ele tem o direito de acessar. Este processo é conhecido como autorização. Um princípio fundamental nesse contexto é o do Menor Privilégio, que preconiza que os usuários devem ter apenas as permissões mínimas necessárias para realizar suas tarefas específicas, reduzindo assim o risco em caso de comprometimento de credenciais.(TOURANI et al., 2017)

A auditoria e o monitoramento contínuo desempenham um papel vital no controle de acesso, permitindo que as organizações rastreiem quem acessou o quê, quando e por quanto tempo. Isso é crucial para a detecção precoce de atividades suspeitas.(DANDURAND; SERRANO, 2013)

O gerenciamento de identidades é uma prática que envolve a administração eficiente de identidades de usuários ao longo de seu ciclo de vida, desde a criação até a desativação, garantindo que o acesso seja concedido e revogado conforme necessário. O *Single Sign-On* (SSO) simplifica o gerenciamento de acesso, permitindo que os usuários acessem várias aplicações com um único conjunto de credenciais de autenticação.(BANERJEE; NAUMANN, 2005)

Além disso, o controle de acesso baseado em funções envolve a atribuição de permissões com base nas funções dos usuários dentro da organização, facilitando o gerenciamento de autorizações em larga escala. A criptografia e a proteção de dados são práticas essenciais para além do

controle de acesso, visando garantir a segurança dos próprios dados.(TOURANI et al., 2017)

A definição e implementação de políticas de segurança, que estabelecem regras e diretrizes para o controle de acesso, são fundamentais para garantir a conformidade e consistência. Por fim, a educação e conscientização contínuas dos usuários sobre boas práticas de segurança, incluindo o manejo adequado de credenciais, são cruciais para fortalecer o controle de acesso e contribuir para um ambiente de tecnologia da informação seguro e confiável.(DANDURAND; SERRANO, 2013)

2.3.1 Exploração de padrões de segurança

A exploração de padrões de segurança é uma prática essencial no campo da segurança da informação, envolvendo uma análise profunda dos padrões presentes nos sistemas e redes de uma organização. O objetivo é identificar possíveis vulnerabilidades, pontos fracos e brechas de segurança que possam ser exploradas por indivíduos mal-intencionados. Essa atividade é crucial para fortalecer as defesas e mitigar riscos potenciais(KHANJI; IQBAL; HUNG, 2019). Assim como o ISO 27001, é uma abordagem reconhecidas e estabelecida para melhorar a postura de segurança cibernética de uma organização, pois oferece diretrizes, melhores práticas e estruturas que auxiliam na implementação de controles de segurança eficazes.(PRICHUA; BERZ, 2012)

ISO 27001 (International Organization for Standardization - Organização Internacional de Normalização):(ISO, 2022)

- **Objetivo:** Estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) em uma organização.
- **Enfoque:** Foco na proteção de informações, incluindo políticas, procedimentos e controles para gerenciar riscos de segurança.
- **Benefícios:** A ISO 27001 fornece uma estrutura sistemática para identificar, analisar e tratar riscos de segurança, estabelecendo um SGSI sólido e demonstrando compromisso com a segurança da informação.

Ao examinar os padrões de tráfego na rede, é possível detectar comportamentos atípicos que podem indicar atividades suspeitas, como variações no volume de dados, horários incomuns de acesso ou tipos de tráfego não usuais. A análise de *logs* de eventos do sistema revela tentativas de acesso não autorizado, atividades anômalas e outros indicadores de comprometimento, destacando possíveis incidentes de segurança.(KHANJI; IQBAL; HUNG, 2019)

Além disso, monitorar os padrões de comportamento dos usuários pode ajudar a identificar atividades incomuns, como múltiplas tentativas de login, acesso a recursos não habituais ou alterações abruptas nos padrões de trabalho. A exploração de padrões de vulnerabilidades conhecidas em sistemas e aplicativos permite que as organizações identifiquem e corrijam possíveis brechas antes que sejam exploradas por atacantes.(SIPONEN; WILLISON, 2009)

A exploração ativa, por meio de testes de penetração, envolve a análise ativa de padrões de vulnerabilidades em ambientes controlados, avaliando a resistência dos sistemas a possíveis ataques. A engenharia reversa, que consiste na análise de códigos e aplicativos, pode revelar padrões

que os atacantes poderiam explorar para contornar medidas de segurança.(SCHUMACHER, 2002)

Estratégias de mitigação incluem a manutenção regular de sistemas e softwares, garantindo que padrões de vulnerabilidades conhecidas sejam corrigidos. O monitoramento contínuo possibilita a identificação rápida de padrões suspeitos, permitindo uma resposta proativa a potenciais ameaças. A conscientização do usuário, por meio da educação sobre práticas de segurança, contribui para modificar padrões de comportamento que poderiam ser explorados por atacantes.(KHANJI; IQBAL; HUNG, 2019)

A implementação de políticas de segurança claras estabelece padrões de comportamento e utilização de recursos, reduzindo as oportunidades para exploração. Em resumo, a exploração de padrões de segurança é uma prática que visa não apenas reagir a ameaças, mas também antecipar e fortalecer as defesas, contribuindo para ambientes mais seguros e resilientes.(SCHUMACHER, 2002)

2.4 Gerenciamento de Riscos

O gerenciamento de risco na segurança da informação é uma prática estratégica fundamental para as organizações enfrentarem os desafios cada vez mais complexos e dinâmicos do ambiente digital. Esse processo abrangente visa proteger os ativos de informação, tais como dados, sistemas e infraestrutura, contra potenciais ameaças e vulnerabilidades, garantindo a integridade, confidencialidade e disponibilidade desses ativos.(BODIN; GORDON; LOEB, 2008)

O ponto de partida é a identificação e classificação dos ativos, seguida por uma avaliação minuciosa de vulnerabilidades existentes. Em paralelo, realiza-se uma análise profunda das ameaças potenciais e dos possíveis impactos que essas ameaças podem causar, considerando aspectos financeiros, operacionais e de reputação.(LÓPEZ et al., 2014)

A avaliação de riscos, resultante da combinação entre a probabilidade de ocorrência de ameaças e os impactos associados, fornece uma compreensão clara dos riscos específicos enfrentados pela organização. Com base nessa análise, estratégias de mitigação são desenvolvidas para reduzir a probabilidade de ocorrência de ameaças e minimizar os impactos em caso de incidentes.(FARAHMAND et al., 2005)

A implementação de controles de segurança é uma etapa crucial, envolvendo a aplicação de medidas técnicas, processuais e humanas para proteger os ativos de informação. Isso pode incluir a implementação de *firewalls*, criptografia, políticas e procedimentos de segurança, bem como treinamento de conscientização para os colaboradores.(BODIN; GORDON; LOEB, 2008)

Além disso, o gerenciamento de risco inclui a criação de sistemas de monitoramento contínuo para identificar atividades suspeitas e a definição de protocolos eficazes para a resposta a incidentes de segurança. A revisão e atualização regular dessas estratégias são essenciais para garantir que estejam alinhadas com as mudanças no ambiente de ameaças e nas operações da organização.(BODIN; GORDON; LOEB, 2008)

A conformidade com requisitos legais e normativos também é abordada, assegurando que a organização atenda a padrões específicos da indústria e regulamentações governamentais. O

envolvimento da alta direção é crucial para garantir o apoio necessário, alinhando as estratégias de segurança com os objetivos organizacionais e alocando os recursos adequados.(LÓPEZ et al., 2014)

2.4.1 Abordagens e metodologias

O gerenciamento de risco na segurança da informação segundo Blakley, McDermott e Geer (2001) envolve diversas abordagens e metodologias para identificar, avaliar e mitigar riscos potenciais. Essas estratégias ajudam as organizações a proteger seus ativos de informação e garantir a continuidade das operações em um ambiente cada vez mais complexo e dinâmico, oferecem estruturas valiosas para as organizações adaptarem e implementarem conforme suas necessidades específicas. A escolha de uma abordagem dependerá do contexto operacional, do setor, da cultura organizacional e dos objetivos específicos de segurança da informação. Integrar práticas contínuas de revisão e atualização é essencial para garantir a eficácia contínua do gerenciamento de riscos ao longo do tempo.(FARAHMAND et al., 2005)

Abaixo, estão algumas das abordagens e metodologias comuns nesse contexto:

- A ISO 27001 é uma norma internacional que define os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação . A ISO 27002 fornece diretrizes detalhadas para práticas de segurança da informação. Essas normas ajudam as organizações a estruturar seus programas de segurança e gerenciamento de risco de acordo com padrões reconhecidos globalmente.(ISO, 2022)

- A norma NIST SP 800-30, que fornece um guia para a realização de avaliações de risco de segurança da informação, considerando os aspectos de ameaças, vulnerabilidades, impactos e probabilidades. A norma também apresenta um processo para a seleção e implementação de controles de segurança da informação, baseado nos resultados da avaliação de risco.(FIKRI et al., 2019)

- A metodologia OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), que é um conjunto de ferramentas e técnicas para a identificação e análise dos riscos de segurança da informação, focando nos ativos críticos para a organização e nas necessidades dos seus usuários. A metodologia envolve a participação ativa dos gestores e funcionários da organização na definição dos objetivos, requisitos e estratégias de segurança da informação.(ALBERTS et al., 2003)

- A metodologia CRAMM (CCTA Risk Analysis and Management Method), que é uma abordagem estruturada para a análise e gerenciamento dos riscos de segurança da informação, baseada em uma classificação dos ativos, ameaças e vulnerabilidades em níveis de criticidade. A metodologia também utiliza um sistema automatizado para calcular os níveis de risco e sugerir os controles adequados para cada situação.(YAZAR, 2002)

2.5 Aspectos Humanos da Segurança da Informação

A segurança da informação é muito mais do que apenas proteger sistemas e dados. Ela também depende muito do comportamento e consciência das pessoas envolvidas. Os aspectos humanos desempenham um papel crucial nesse cenário, moldando a eficácia das medidas de segurança.(PARSONS et al., 2010)

Primeiramente, a conscientização e o treinamento são essenciais. Os colaboradores precisam entender as ameaças cibernéticas, como *phishing* e *malware*, através de programas educativos e treinamentos regulares. Comportamentos como o uso de senhas fortes, a verificação cuidadosa de links e a desconfiança de anexos suspeitos são fundamentais para a proteção.(PIPLAI et al., 2020)

A cultura organizacional também desempenha um papel importante. Uma cultura de segurança, onde todos na empresa valorizam e priorizam a proteção dos dados, é essencial. Cada indivíduo, independentemente do cargo, deve se sentir responsável pela segurança das informações.(PARSONS et al., 2010)

O gerenciamento de acesso é outra área crítica. A aplicação do princípio do menor privilégio, concedendo acesso mínimo necessário, e o monitoramento cuidadoso de quem acessa o quê e quando são práticas vitais.(SAFA; SOLMS; FUTCHER, 2016)

A compreensão das táticas de engenharia social e a conscientização sobre como identificar e evitar ser enganado por elas também são aspectos importantes.

Políticas claras de segurança, procedimentos para lidar com incidentes e até mesmo a compreensão de fatores psicológicos, como confiança e comportamento humano, desempenham um papel crucial.(SAFA; SOLMS; FUTCHER, 2016)

Em última análise, a segurança da informação depende da responsabilidade individual de cada membro da organização. Todos devem compreender sua importância na proteção dos dados e sistemas da empresa para que as medidas de segurança sejam eficazes e robustas.(KHANDO et al., 2021)

2.6 Inteligência Artificial em Segurança da Informação

Por meio de algoritmos avançados, a IA é capaz de analisar padrões de dados, identificar comportamentos anômalos e prevenir fraudes em tempo real. Além disso, contribui para a proteção de dados através de técnicas como criptografia, elevando o nível de segurança em diversos setores, como finanças, comércio eletrônico e empresas em geral(CHEN, 2006).

Entretanto, segundo Chen (2006) a utilização da IA na segurança da informação não está isenta de desafios. A vulnerabilidade dos próprios sistemas de IA é uma preocupação, pois podem ser alvo de ataques maliciosos. A possibilidade de viés nos modelos de IA, baseados nos dados utilizados no treinamento, levanta questões sobre a precisão e imparcialidade desses sistemas. Além disso, a complexidade dos modelos pode tornar difícil compreender como as decisões são tomadas, afetando a interpretabilidade e confiança.

Olhando para o futuro, de acordo Mughal (2018) IA na segurança da informação está destinada a se aprimorar, integrando-se a outras tecnologias para antecipar e conter ameaças de

forma mais eficiente. A transparência e a ética na utilização da IA serão elementos cruciais, juntamente com investimentos contínuos em pesquisas para mitigar vulnerabilidades e garantir que seu potencial seja maximizado para proteger nossos dados e sistemas.

2.7 BlockChain

De acordo com Tijan et al. (2019) a tecnologia blockchain, embora frequentemente associada a criptomoedas, oferece um amplo espectro de aplicações além das moedas digitais. Essencialmente, o blockchain funciona como um livro-razão descentralizado, e suas aplicações potenciais são diversas. Ele atua como um livro-razão distribuído que pode ser utilizado para várias formas de troca de dados, desde contratos até o rastreamento de remessas e transações financeiras, incluindo pagamentos.

No blockchain, cada transação ou ação é registrada em um bloco, e esses dados são distribuídos por inúmeros nós ou computadores. Segundo Braga, Marino e Santos (2017) essa natureza descentralizada contribui para a transparência do sistema, pois cada participante na rede tem acesso às mesmas informações. A interconexão dos blocos, onde cada um está vinculado aos blocos anteriores e subsequentes, aprimora a segurança do sistema.

Uma área notável em que a tecnologia blockchain pode trazer mudanças transformadoras é na cadeia de suprimentos. Ao aproveitar o blockchain, as organizações podem aprimorar significativamente a eficiência e a transparência de seus processos de cadeia de suprimentos. Esse impacto se estende por várias operações logísticas, abrangendo armazenamento, transporte, entrega e pagamento.(TIJAN et al., 2019)

O uso da tecnologia blockchain não apenas introduz maior transparência e segurança, mas também tem o potencial de otimizar o fluxo físico de mercadorias. Por meio de um livro-razão seguro e transparente, os participantes na cadeia de suprimentos podem acessar informações em tempo real, reduzir ineficiências e aprimorar a confiança entre as partes interessadas. Como resultado, o blockchain emerge como uma ferramenta poderosa com a capacidade de revolucionar a maneira como as indústrias gerenciam e otimizam suas operações.(TIJAN et al., 2019)

De acordo com (ULRICH, 1892), o blockchain nada mais é do que um banco de dados público, que contém o histórico de todas as transações entre criptomoedas realizadas, um exemplo de criptomoeda é o famoso Bitcoin. Blockchain e está ligado a criptomoedas e criptomoedas também estão ligadas a segurança, pois uma vez que você adquire partes de um Bitcoin por exemplo seu dinheiro fica mais seguro do que se estivesse em um banco.

Braga, Marino e Santos (2017) diz que as redes blockchain são divididas em dois grupos, as redes públicas que são aquelas que o acesso pode ser anônimo as aplicações têm característica aberta e a própria rede segue suas regras. Nestas redes, os nós são competidores na criação de blocos e, por isto, não confiam plenamente uns nos outros. Neste caso, a confiança advém da boa execução das regras de consenso e não dos pares e as redes privadas que geralmente oferecem acesso a usuários identificados, autenticados e autorizados. Nestas redes, os usuários não são anônimos, mas sim grupos selecionados de usuários conhecidos.

Blockchain usa criptografia de dois modos. Primeiro, as funções de resumo criptográfico

são usadas na geração dos endereços, que consistem de valores *hash* calculados a partir das chaves públicas. Segundo, as assinaturas digitais usadas na garantia de autenticidade e de irrefutabilidade das transações.(BRAGA; MARINO; SANTOS, 2017)

A criptografia assimétrica (de chave pública) para assinatura digital é usada para obter integridade, autenticidade e irrefutabilidade. A assinatura digital é o resultado uma operação criptográfica com a chave privada sobre o texto claro. O dono da chave privada pode gerar mensagens assinadas, que podem ser verificadas por qualquer um que conheça a chave pública correspondente. O assinante não pode negar a autoria, pois há uma assinatura digital feita com sua chave privada. Por isto, a assinatura é irrefutável. A assinatura pode ser verificada por qualquer um com a chave pública. (TIJAN et al., 2019)

2.8 Ferramentas e técnicas para segurança da informação

Silva (2017) diz a segurança da informação na realidade atual passa a ser um ponto de extrema importância para indivíduos e organizações, pois preserva o valor de dados sigilosos e viabiliza a execução de estratégias corporativas. Ainda segundo o autor as técnicas de segurança da informação mais usuais que ajudam no controle lógico são criptografia, assinatura digital e certificado digital.

- **Criptografia:** A criptografia tem utilizado diferentes cifras ao longo do tempo. Existem cifras de transposição e cifras de substituição. Enquanto na cifra de transposição cada letra conserva a sua identidade, mas muda de posição dentro da 5 mensagem. (FIARRESGA et al., 2010).

- **Assinatura digital:** Ao invés do signatário se dirigir até um cartório, ele deve utilizar um aplicativo voltado para este fim. E onde antes era utilizada uma caneta para assinar, nesse novo modelo é utilizado um certificado digital. (ZUNINO, 2017).

- **Certificado digital:** O certificado digital é um documento eletrônico que contém um nome e um número público exclusivo, chamado de chave pública. Foi criado pela medida provisória e visa garantir a identificação segura do trânsito de uma mensagem ou negócio eletrônico, além de permitir assinar, digitalmente, as mensagens e transações on-line com confidência, integridade e validade jurídica. (RESENDE, 2009).

Dentre as inúmeras ferramentas, as que mais se destacam são os Detectores de Intrusões: IDS / IPS, Antivírus, Filtros AntiSpam e Firewall. (SILVA, 2017).

- **Detectores de Intrusões:** IDS / IPS: Os detectores são responsáveis por tentar reconhecer um comportamento ou uma ação intrusiva para alertar o usuário ou automaticamente remover essa possível ameaça. (LAUREANO; MAZIERO; JAMHOUR, 2003).

- **Antivírus:** É um software desenvolvido para *scannear*, detectar e remover arquivos e programas instalados em um computador. (AIGBODI et al.,).

- **Filtros AntiSpam:** São programa que filtram e classificam e-mails de acordo com o conteúdo deles, são utilizadas técnicas de classificação Bayesiana e redes neurais. (SAHAMI et al., 1998).

- **Firewall:** Um *firewall* é um sistema de segurança colocado no ponto de entrada entre uma rede privada e a Internet por onde todos os pacotes de entrada e saída devem passar. (LIU; GOUDA, 2008)

2.9 Antivírus

De acordo com o que os anos vão passando as tecnologias e os meios de informação vão se tornando cada vez melhores, e devido a esse avanço tecnológico os meios de ataques também vão se modernizando e ficando cada vez mais comuns, porém para proteger o usuário contra esses ataques foram desenvolvidos softwares para garantir que eles possam utilizar a internet ou outros meios de comunicação de forma segura, esses softwares são conhecidos com antivírus. Um antivírus é um software desenvolvido com o objetivo de proteger os usuários e garantir que eles possam navegar pela internet de forma segura, também os protegem contra possíveis tentativas de infectar um computador, não permitindo que o usuário faça download de um arquivo que possa conter algum software malicioso por trás dele. (KORET; BACHAALANY, 2015).

A criação e disseminação de *malware* representam um desafio constante para a segurança cibernética, com implicações significativas para a proteção de dados e sistemas. A facilidade com que indivíduos podem desenvolver *malware*, utilizando ferramentas acessíveis online, destaca a necessidade premente de estratégias avançadas de defesa.(KALOGRANIS, 2018)

O *Metasploit*, mencionado anteriormente, é uma ferramenta poderosa que, embora tenha aplicações legítimas em testes de segurança, também pode ser explorado por atacantes para gerar *payloads* maliciosos. No entanto, o progresso na área de segurança cibernética não se limita apenas à detecção convencional de *malwares*. Os produtos antivírus modernos empregam técnicas avançadas, como análise heurística, *machine learning* e comportamental, para identificar e neutralizar ameaças em tempo real.(KALOGRANIS, 2018)

O desafio, porém, está em lidar com *malwares* que buscam evadir as defesas tradicionais. Ferramentas desenvolvidas para empregar técnicas de evasão complicam ainda mais a detecção, destacando a necessidade de constante inovação por parte dos desenvolvedores de software de segurança.(KALOGRANIS, 2018)

Essa corrida armamentista digital evidencia não apenas a importância de manter as defesas atualizadas, mas também a necessidade de uma abordagem proativa na identificação e neutralização de ameaças emergentes. A colaboração entre a comunidade de segurança cibernética, pesquisadores e organizações é vital para criar estratégias robustas e mitigar os riscos associados ao avanço constante das ameaças cibernéticas.(KALOGRANIS, 2018)

O antivírus é um software que o usuário pode fazer download de deixa-lo instalado em seu computador, após instalado o antivírus vai *scanner* todos os arquivos que estão armazenados no seu computador, além também de monitorar e impedir que o usuário faça download de

um arquivo ou software que possa conter algum tipo de vírus ou *malware*. (KORET; BACHAALANY, 2015) No mercado existe alguns antivírus que são mais conhecidos, o Avast, o Kaspersky, o McAfee e o Windows Defender o antivírus nativo do Windows. (WIDJAJARTO; ALMAARIF et al., 2023).

Avast Antivírus é desenvolvido pela Avast Software, ele foi desenvolvido para proteger os usuários que contratam o software contra todos os tipos de vírus e tentativas de ataque. Ele é um software desenvolvido para todos os tipos de dispositivos, sendo ele um dispositivo móvel, um computador com sistema operacional Windows ou MacOS, celulares android, Ipad e Iphone. (HAMLEN et al., 2009).

2.10 Firewall

Ao longo das décadas, a tecnologia de *firewall* passou por avanços substanciais desde sua introdução nos anos 1990. Os primeiros *firewalls* eram simples, baseados em filtragem de pacotes, mas ao longo do tempo evoluíram para soluções mais sofisticadas, capazes de analisar diversas camadas de atividade e conteúdo de rede.(WACK; CUTLER; POLE, 2002)

Com o desenvolvimento da Internet para a complexa e interconectada rede que conhecemos hoje, a segurança online tornou-se um desafio crescente. Invasões e ataques tornaram-se tão comuns que agora são considerados uma parte inerente das operações comerciais.(WACK; CUTLER; POLE, 2002)

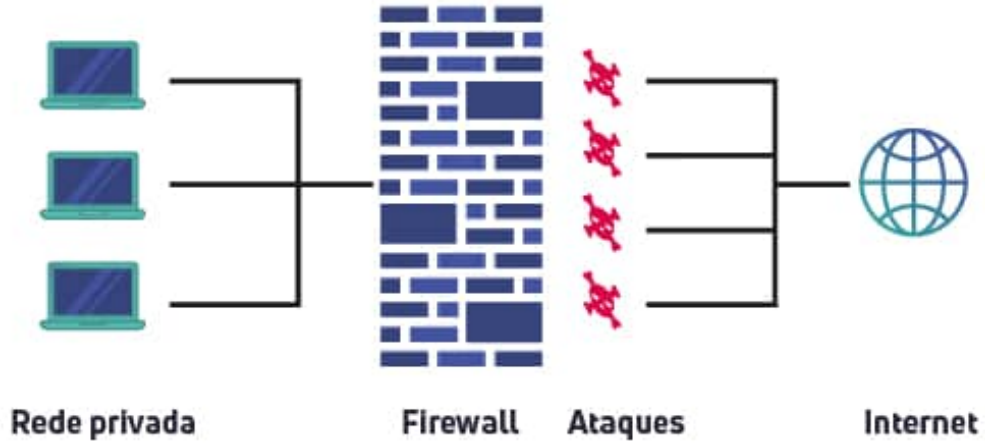
Atualmente, a tecnologia de *firewall* não é apenas uma opção, mas sim uma peça fundamental da arquitetura de segurança de redes em organizações. Além disso, os usuários domésticos, conectados através de linhas discadas comerciais e conexões de cabo, rotineiramente empregam *firewalls* pessoais e dispositivos de *firewall* para proteger suas conexões e dados. Essa adoção generalizada destaca a importância crescente da segurança cibernética em todos os níveis de uso da Internet.(WACK; CUTLER; POLE, 2002)

A implementação da tecnologia de *firewall* é um marco crucial para fortalecer a segurança de nossas redes. No entanto, a complexidade associada à administração das políticas de *firewall* pode impactar a eficácia da segurança proporcionada. Dentro de uma política de *firewall*, podem surgir anomalias, onde um pacote pode corresponder a duas ou mais regras de filtragem distintas. Ao estabelecer essas regras, é imperativo dedicar atenção especial às relações e interações entre elas, a fim de determinar a ordem adequada e garantir a semântica correta das políticas de segurança.(AL-SHAER; HAMED, 2003)

A Figura 2.4 representa como é feita um *firewall* realiza a proteção de seus arquivos. Um *firewall* é uma parede que como objetivo protege seus aparelhos contra possíveis ataques impedindo que os possíveis invasores não consigam acessar suas informações.

À medida que o número de regras de filtragem aumenta, a complexidade na redação de novas regras ou na modificação das existentes também cresce. Nesse contexto, há uma probabilidade considerável de introduzir regras conflitantes, como uma regra geral que obscurece uma específica, ou regras correlacionadas cuja ordem relativa determina ações distintas para um mesmo pacote.(AL-SHAER; HAMED, 2003)

Figura 2.4: Firewall



Fonte: https://vcx.solutions/o-que-e-firewall-e-seu-papel-na-seguranca-da-informacao/

Adicionalmente, em uma típica rede empresarial em larga escala, centenas de regras podem ser elaboradas por diferentes administradores ao longo do tempo. Essa diversidade aumenta significativamente o potencial de ocorrência de anomalias nas políticas de *firewall*, colocando em risco a segurança da rede protegida. Portanto, uma gestão cuidadosa, juntamente com revisões regulares das políticas de *firewall*, é essencial para assegurar a eficácia contínua da segurança da rede em face das complexidades crescentes.(AL-SHAER; HAMED, 2003)

Os experimentos são conduzidos em uma LAN dedicada a testes de segurança, na qual um *firewall* atua como o ponto de entrada para todo o tráfego que flui para dentro e para fora da rede local. Nesse cenário, são realizados testes abrangentes de segurança e desempenho no *firewall*. A configuração do *firewall* envolve a implementação de diferentes níveis de segurança, alcançados por meio de um roteador e vários servidores *proxy*.(LYU; LAU, 2000)

Essa abordagem estruturada permite a análise minuciosa do desempenho do *firewall* em diferentes cenários de segurança, oferecendo uma compreensão mais profunda de como ele lida com o tráfego variado. A diversidade nos níveis de segurança e a presença de servidores *proxy* adicionam complexidade aos testes, possibilitando uma avaliação mais abrangente do desempenho e da eficácia do *firewall* em condições diversas. Os detalhes específicos desse arranjo são delineados a seguir.(LYU; LAU, 2000)

2.11 Cloud Computing e Segurança na Nuvem

A computação em nuvem, ou *cloud computing*, representa uma mudança fundamental na maneira como as organizações acessam e utilizam recursos de TI. Em vez de depender de infraestrutura local, as empresas podem aproveitar serviços escaláveis fornecidos por provedores através da internet, resultando em uma transformação significativa nos modelos de gerenciamento de dados e operações.(WEI; BLAKE, 2010)

Este paradigma traz diversas características distintas. A acessibilidade via internet possibilita o uso remoto de recursos, enquanto o modelo de autoatendimento sob demanda permite

aos usuários provisionarem e gerenciarem recursos conforme necessário, sem intervenção direta do provedor. A escalabilidade é uma vantagem crucial, permitindo ajustes de capacidade em tempo real para atender às demandas variáveis, e o pagamento por uso oferece uma abordagem econômica, pagando apenas pelos recursos consumidos.(BASU et al., 2018)

Existem diferentes modelos de serviço na computação em nuvem. A Infraestrutura como Serviço (IaaS) fornece recursos fundamentais, como máquinas virtuais e armazenamento. Plataforma como Serviço (PaaS) oferece uma plataforma completa para desenvolvimento e execução de aplicativos, enquanto Software como Serviço (SaaS) entrega aplicativos prontos para uso pela internet.(RANI; RANJAN, 2014)

Os modelos de implantação variam entre nuvens públicas, privadas e híbridas. As nuvens públicas compartilham recursos entre várias organizações, proporcionando eficiência e economia de escala. Nuvens privadas dedicam recursos exclusivamente a uma única organização, oferecendo maior controle e personalização. Modelos híbridos combinam elementos de ambas, permitindo transferência de dados e aplicativos entre ambientes.(BASU et al., 2018)

Entre os benefícios notáveis da computação em nuvem estão a flexibilidade e escalabilidade, possibilitando adaptação rápida às demandas do negócio. A eficiência operacional é aprimorada com o compartilhamento de recursos e automação, reduzindo custos e aumentando a produtividade. O acesso remoto proporciona mobilidade, e a implementação rápida de novas ideias é facilitada, estimulando a inovação.(VELTE; ELSENPETER, 2010)

2.11.1 SaaS

O Software como Serviço (SaaS) representa um modelo inovador de distribuição de software, transformando a maneira como empresas e usuários finais interagem com aplicativos. Ao contrário dos métodos tradicionais que exigem instalações locais, o SaaS oferece acesso a aplicativos pela internet, proporcionando uma série de benefícios significativos.(SATYANARAYANA, 2012)

Uma característica central do SaaS é a acessibilidade remota. Usuários podem utilizar aplicativos a partir de qualquer local com conexão à internet, eliminando as restrições geográficas e promovendo a mobilidade. Além disso, o modelo de assinatura, comum no SaaS, implica em pagamento recorrente por meio de uma taxa de assinatura, tornando o acesso ao software mais flexível e previsível em termos financeiros.(MOHAMMED; ZEEBAREE, 2021)

Atualizações automáticas são uma marca registrada do SaaS. Provedores gerenciam e implementam melhorias de software sem exigir intervenção manual dos usuários. Essa abordagem garante que os usuários sempre tenham acesso às últimas funcionalidades e correções de segurança, sem a necessidade de lidar com processos de atualização complexos.(SATYANARAYANA, 2012)

As vantagens do modelo SaaS são diversas. Reduz os custos associados à infraestrutura local e à manutenção de software, ao mesmo tempo em que oferece implementação rápida e acesso universal às aplicações. A escalabilidade automática é outra vantagem, permitindo que organizações ajustem rapidamente seus recursos de acordo com as necessidades do momento.(ABDALLA; VAROL, 2019)

Entretanto, há desafios e considerações importantes a serem levados em conta. A segurança

de dados é uma preocupação crítica, visto que informações sensíveis são armazenadas externamente. A personalização pode ser limitada em algumas aplicações SaaS, o que pode ser uma consideração significativa para organizações com requisitos específicos. A dependência contínua de conectividade à internet também é uma consideração essencial, assim como garantir que o provedor SaaS esteja em conformidade com regulamentações específicas.(ABDALLA; VAROL, 2019)

2.11.2 PaaS

A Plataforma como Serviço, mais conhecida como PaaS, representa um modelo inovador dentro da computação em nuvem. Sua proposta central é oferecer uma plataforma completa para o desenvolvimento, execução e gerenciamento de aplicativos, sem que os desenvolvedores necessitem lidar com a complexidade da infraestrutura subjacente.(FREET et al., 2015)

Em seu cerne, o PaaS fornece um ambiente de desenvolvimento abrangente, equipado com ferramentas e serviços que facilitam todas as fases do ciclo de vida de um aplicativo. A abstração de infraestrutura é uma característica distintiva, liberando os desenvolvedores da necessidade de se preocupar com servidores, armazenamento e redes. Esse foco exclusivo na codificação e no design de aplicativos aumenta significativamente a eficiência do desenvolvimento.(FREET et al., 2015)

Uma característica notável do PaaS é a presença de serviços integrados, que abrangem desde bancos de dados até filas de mensagens. Essa inclusão simplifica diversas tarefas essenciais para o desenvolvimento de aplicativos, proporcionando uma experiência mais holística.(MOHAMMED; ZEEBAREE, 2021)

As vantagens do PaaS são diversas. A eficiência no desenvolvimento é aumentada, uma vez que os desenvolvedores podem focar exclusivamente na lógica de negócios, deixando a complexidade da infraestrutura para a plataforma. A escalabilidade automática oferece uma gestão mais eficaz da carga de trabalho, adaptando-se dinamicamente às demandas do tráfego.(RANI; RANJAN, 2014)

Entretanto, há desafios e considerações importantes a serem ponderados. Limitações de personalização podem ser uma preocupação para aplicativos altamente especializados, e o conceito de bloqueio de fornecedor deve ser considerado ao depender de uma plataforma específica. Questões de segurança e conformidade também são cruciais, demandando uma avaliação cuidadosa das capacidades da plataforma para atender a esses requisitos.(RANI; RANJAN, 2014)

2.11.3 IaaS

A Infraestrutura como Serviço, mais conhecida pela sigla IaaS, representa um modelo crucial dentro do cenário de computação em nuvem. Em seu cerne, o IaaS fornece recursos de infraestrutura virtualizados pela internet, permitindo que organizações e usuários adquiram e gerenciem elementos essenciais de TI, como servidores, armazenamento e redes, sem depender de investimentos em hardware físico.(FREET et al., 2015)

Uma característica distintiva do IaaS é a utilização da virtualização para criar instâncias virtuais de recursos. Isso possibilita que usuários acessem esses recursos de maneira flexível,

ajustando a capacidade para cima ou para baixo conforme necessário. Essa elasticidade e escalabilidade são fundamentais para atender às demandas variáveis e garantir eficiência operacional.(MOHAMMED; ZEEBAREE, 2021)

Ao optar pelo IaaS, os usuários podem acessar e gerenciar esses recursos remotamente pela internet. Esse modelo oferece não apenas acesso global, mas também a capacidade de gerenciar infraestruturas de forma remota, proporcionando uma abordagem mais ágil e adaptável.(FREET et al., 2015)

A capacidade de autoatendimento sob demanda é uma característica vital do IaaS. Os usuários podem provisionar e gerenciar recursos de maneira autônoma, eliminando a necessidade de intervenção manual por parte dos provedores de serviços. Isso não apenas agiliza o processo, mas também confere mais controle aos usuários sobre seus ambientes de infraestrutura.(MOHAMMED; ZEEBAREE, 2021)

As vantagens do modelo IaaS são diversas. Proporciona flexibilidade e controle total sobre a configuração da infraestrutura, permitindo que os usuários adaptem seus ambientes conforme as exigências específicas de suas cargas de trabalho. Além disso, há uma economia significativa de custos, uma vez que elimina a necessidade de investimentos iniciais em hardware físico, permitindo o pagamento apenas pelos recursos efetivamente utilizados. A elasticidade do IaaS é valiosa, garantindo que as organizações possam lidar eficientemente com picos de demanda sem comprometer o desempenho.(RANI; RANJAN, 2014)

Contudo, a adoção do IaaS também traz desafios e considerações importantes. A responsabilidade pela segurança recai sobre os usuários, exigindo a implementação de medidas robustas para proteger instâncias e dados. Além disso, gerenciar ativos virtuais requer novas habilidades e processos, especialmente no que diz respeito ao monitoramento e à otimização. A escolha de um provedor específico pode criar bloqueios, dificultando uma eventual mudança para outra plataforma.(RANI; RANJAN, 2014)

2.12 Métricas e Avaliação de Segurança

A avaliação da eficácia das estratégias de segurança da informação é uma parte essencial da gestão proativa de riscos cibernéticos. Utilizar métricas apropriadas e abordagens de avaliação contínua é fundamental para garantir que as práticas de segurança estejam alinhadas com os objetivos organizacionais.(KHAN et al., 2011)

Uma métrica crucial é a taxa de incidentes de segurança ao longo do tempo. A diminuição dessa taxa ao longo do tempo pode indicar que as estratégias de segurança estão sendo eficazes na prevenção de incidentes. O tempo médio de resposta (MTTR) também é fundamental, pois uma redução nesse indicador sugere uma resposta mais eficiente a incidentes, minimizando danos.(ABRAHAM; CHENGALUR-SMITH, 2019)

A conformidade com políticas internas e regulamentações externas é outra métrica significativa. Manter ou aumentar a taxa de conformidade indica que as estratégias estão alinhadas com os padrões regulatórios e internos estabelecidos. Testes de penetração, ao identificar e corrigir vulnerabilidades, oferecem uma métrica tangível da eficácia na proteção contra ameaças

externas.(CHEN; RAMAMURTHY; WEN, 2015)

O treinamento e conscientização dos funcionários também desempenham um papel crítico. A taxa de participação e avaliações pós-treinamento reflete a eficácia dessas iniciativas na construção de uma cultura de segurança. Além disso, avaliações regulares de riscos e a eficiência na mitigação de riscos críticos são métricas essenciais para garantir uma abordagem proativa na identificação e gestão de ameaças.(KHAN et al., 2011)

A monitorização contínua do ambiente, incluindo o tempo de detecção de atividades suspeitas, é uma métrica-chave para avaliar a capacidade de resposta rápida. Implementar atualizações e *patches* regularmente, refletidos na taxa de implementação, ajuda a manter a segurança dos sistemas, reduzindo a superfície de ataque.(CHEN; RAMAMURTHY; WEN, 2015)

Simulações de incidentes oferecem uma métrica valiosa para testar a eficácia das estratégias de resposta. Melhorias na gestão dessas simulações indicam uma preparação mais eficaz para incidentes reais. O *feedback* dos usuários sobre práticas de segurança, expresso em avaliações e comentários, fornece uma perspectiva valiosa sobre a experiência do usuário e a eficácia das medidas implementadas.(ABRAHAM; CHENGALUR-SMITH, 2019)

É essencial considerar que a avaliação da eficácia das estratégias de segurança é um processo contínuo. A adaptação constante é necessária para enfrentar um cenário de ameaças em constante evolução. Além disso, a participação de partes interessadas internas e externas e o *benchmarking* em relação aos padrões do setor são práticas recomendadas para obter uma visão abrangente da eficácia das estratégias de segurança.(CIOACĂ; BRATU; ȘTEFĂNESCU, 2017)

2.13 Colaboração entre organizações em relação à segurança da informação

A colaboração entre organizações em relação à segurança da informação apresenta uma série de benefícios, mas também implica desafios que precisam ser gerenciados com cuidado.

Um dos principais benefícios é o intercâmbio de inteligência de ameaças. Organizações podem compartilhar informações sobre ameaças cibernéticas, táticas de ataque e indicadores de comprometimento, permitindo uma defesa mais robusta contra ameaças conhecidas. Além disso, a colaboração facilita uma resposta rápida a incidentes de segurança, pois as organizações podem trabalhar em conjunto para identificar, conter e remediar ataques.(PRADITYA; JANSSEN, 2015)

A ampliação da visibilidade sobre o cenário de ameaças é outro benefício crucial. Ao colaborar, as organizações podem se beneficiar de perspectivas e *insights* que podem não estar disponíveis internamente. A troca de melhores práticas em segurança também é promovida, contribuindo para a padronização de abordagens eficazes e o aprimoramento geral das posturas de segurança. Além disso, a colaboração pode resultar em uma utilização mais eficiente dos recursos, especialmente para organizações menores que podem se beneficiar da experiência de parceiros mais experientes.(CHEN et al., 2021)

No entanto, enfrentar desafios é inevitável. A confidencialidade e privacidade das informações compartilhadas podem ser uma preocupação, especialmente quando não há confiança

mútua entre as organizações. Diferenças nas prioridades e cultura de segurança também podem dificultar a colaboração eficaz, assim como questões relacionadas à responsabilidade, responsividade e coordenação de esforços.(CHEN et al., 2021)

Além disso, questões jurídicas e regulatórias precisam ser cuidadosamente consideradas, exigindo conformidade com as leis e regulamentações pertinentes. Construir um nível adequado de confiança entre as organizações é crucial para o sucesso da colaboração, e a falta de confiança pode impedir a partilha completa e eficaz de informações. Coordenar esforços e manter uma comunicação eficaz também são desafios que precisam ser abordados, especialmente em ambientes complexos e dinâmicos.(PRADITYA; JANSSEN, 2015)

2.14 Educação e Conscientização em Segurança da Informação

A conscientização desempenha um papel fundamental na mitigação de ameaças internas em ambientes corporativos. Esta dimensão vai além de simplesmente informar; ela envolve capacitar os colaboradores a compreender e se comprometer ativamente com a proteção dos ativos e informações da organização.(KUUSISTO; ILVONEN, 2003)

Em primeiro lugar, a conscientização contribui para a identificação de comportamentos suspeitos por parte dos colaboradores. Isso inclui o reconhecimento de atividades anômalas, como acessos não autorizados a dados sensíveis, auxiliando na prevenção de ameaças internas. Além disso, ela desempenha um papel crucial na defesa contra táticas de engenharia social, capacitando os funcionários a reconhecerem e evitarem esquemas de *phishing* e manipulação psicológica.(STEFANIUK, 2020)

Ao reforçar as políticas de segurança da organização, a conscientização cria uma base sólida para práticas adequadas. Isso abrange desde a gestão de senhas até o uso responsável dos recursos tecnológicos, contribuindo para a construção de uma cultura organizacional que valoriza a segurança.(CURADO; TEIXEIRA, 2014)

A conscientização também promove a responsabilidade individual dos colaboradores em relação à segurança. Quando compreendem seu papel na proteção dos ativos da empresa, os funcionários tendem a adotar comportamentos mais alinhados com as melhores práticas de segurança.(STEPHANOU, 2008)

Um aspecto crítico é a mitigação de riscos associados à negligência não intencional. Muitas ameaças internas originam-se de erros inadvertidos, e a conscientização reduz esses riscos ao informar sobre práticas seguras, evitando, por exemplo, o envio acidental de informações confidenciais.(STEPHANOU, 2008)

Além disso, ela contribui para a criação de uma cultura organizacional que valoriza a segurança da informação. Quando incorporada nos valores da empresa, a segurança torna-se uma parte integral das atividades cotidianas.(WILSON; HASH et al., 2003)

Colaboradores conscientes também desempenham um papel crucial na resposta a incidentes. Ao relatarem prontamente atividades suspeitas, contribuem para uma resposta mais rápida, limitando danos e contendo ameaças em seus estágios iniciais.(CURADO; TEIXEIRA, 2014)

Em um cenário de ameaças em constante evolução, a conscientização prepara os colaboradores para se adaptarem a novas ameaças. Reconhecendo padrões e comportamentos que indicam riscos emergentes, os funcionários informados contribuem para a resiliência da organização.(WILSON; HASH et al., 2003)

Além disso, a conscientização é fundamental para o cumprimento de regulamentações em setores regulamentados. Colaboradores informados são mais propensos a aderir a práticas que garantem a conformidade com requisitos legais e normativos.(KUUSISTO; ILVONEN, 2003)

Um investimento contínuo em treinamento assegura que os colaboradores estejam atualizados sobre as últimas ameaças e melhores práticas de segurança. Dessa forma, a conscientização não é um evento único, mas um processo dinâmico que fortalece continuamente as defesas contra uma variedade de riscos internos.(STEFANIUK, 2020)

2.15 Direções e Desafios

Segundo (CHOOBINEH et al., 2007) segurança da informação é um tema muito importante e relevante nos dias de hoje, pois envolve a proteção de dados, sistemas e redes contra ataques cibernéticos, violações de privacidade, fraudes e outros riscos. A segurança da informação também está relacionada à conformidade com leis e regulamentações que visam garantir o uso ético e responsável dos dados.

Essas são algumas das tendências futuras em segurança da informação que podem impactar o cenário:

- O aumento do trabalho remoto, que pode dificultar o controle e a monitoração da segurança das empresas, exigindo soluções mais flexíveis e adaptáveis. (PAPADIMITRATOS et al., 2008).

- O uso de inteligência artificial e Machine Learning para detectar e prevenir ameaças específicas, mas também para criar novos tipos de ataques, como *deepfakes* e *bots* maliciosos. (ZHOU, 2021).

- A convergência entre as equipes de rede e segurança, que devem trabalhar de forma integrada para garantir a proteção dos dados, não apenas das redes, usando abordagens como *zero-trust* e *Secure Access Service Edge* (SASE). (CHOOBINEH et al., 2007).

- O crescimento das regulamentações de privacidade, como a LGPD no Brasil e a GDPR na Europa, que desafiam as empresas a se adequarem às normas e a respeitarem os direitos dos usuários. (PAPADIMITRATOS et al., 2008).

- A migração para a nuvem, que traz benefícios econômicos e de escalabilidade, mas também demanda controles de governança de dados e de segurança específicos para esse ambiente. (BOSS et al., 2007).

Essas tendências representam alguns dos desafios emergentes que as empresas e os profissionais de segurança da informação devem enfrentar nos próximos anos, buscando soluções

inovadoras e eficazes para garantir a confidencialidade, a integridade e a disponibilidade dos dados.

2.15.1 Como a tecnologia pode afetar a segurança da informação

Segundo OYAMA (2011) a proteção da informação se tornou um campo de batalha dinâmico no mundo tecnológico em constante evolução. À medida que a tecnologia avança, abre portas para um novo nível de complexidade na segurança da informação.

A crescente conectividade, impulsionada pela Internet das Coisas (IoT), transformou a maneira como interagimos com o mundo digital. Segundo (MIHOVSKA; SARKAR, 2018) no entanto, cada novo dispositivo conectado não apenas oferece conveniência, mas também amplia a superfície de ataque, criando mais pontos de vulnerabilidade para os cibercriminosos explorarem.

De acordo com OYAMA (2011) os avanços na área de segurança cibernética proporcionaram respostas a esse panorama desafiador. Soluções inovadoras, como sistemas de detecção de intrusões inteligentes e *firewalls* adaptáveis, oferecem camadas mais robustas de defesa contra ameaças sofisticadas. Além disso, o desenvolvimento contínuo de métodos avançados de criptografia fortalece a proteção dos dados, garantindo sua integridade e confidencialidade.

No entanto, o cenário não é apenas técnico. Cavelty e Wenger (2020) a coleta massiva de dados gera debates sobre privacidade e ética. Companhias e governos coletam grandes quantidades de informações, levantando questões sobre quem as controla e como são utilizadas. Esse aspecto demanda não só avanços tecnológicos em proteção de dados, mas também regulamentações sólidas e políticas que garantam a privacidade dos indivíduos.

Segundo (SAFA; SOLMS; FUTCHER, 2016) a educação também se torna uma peça-chave neste quebra-cabeça. A conscientização sobre práticas seguras na internet e a importância da ciber-higiene são cruciais para mitigar riscos. Treinar pessoas para reconhecerem e evitarem ameaças cibernéticas é tão crucial quanto investir em soluções tecnológicas.

Assim, a interseção entre tecnologia e segurança da informação é um campo vasto e em constante mutação. Enquanto a inovação impulsiona novos desafios, também oferece soluções avançadas. Encontrar um equilíbrio entre avanços tecnológicos, privacidade e proteção dos dados é essencial para um futuro digital seguro e confiável(CAVELTY; WENGER, 2020).

Capítulo

3

Análise e Discussão

Em um mundo cada vez mais conectado, a segurança da informação se torna uma necessidade premente. Este trabalho explorou os princípios, desafios e estratégias fundamentais para proteger dados em um cenário onde a tecnologia avança em ritmo acelerado e as ameaças cibernéticas se multiplicam.

Ao longo desta pesquisa, ficou evidente que a segurança da informação não é um destino final, mas sim uma jornada contínua. A constante evolução das ameaças exige estratégias adaptativas, políticas robustas e tecnologias avançadas para mitigar riscos e proteger informações sensíveis.

A compreensão das ameaças atuais, desde o *malware* até os sofisticados ataques de engenharia social, enfatiza a necessidade de preparo e educação contínua para enfrentar tais desafios. Estratégias como criptografia, *firewalls*, políticas de segurança bem definidas e conformidade regulatória são peças-chave nesse quebra-cabeça de proteção de dados.

A gestão de riscos emergiu como um aspecto crucial, permitindo uma abordagem proativa na identificação, avaliação e mitigação de possíveis vulnerabilidades. Além disso, a rápida evolução tecnológica, com tendências como inteligência artificial e internet das coisas, impõe desafios adicionais, exigindo uma constante adaptação e atualização das estratégias de segurança.

Na busca por informações para a realização do trabalho, me deparei com um desafio significativo. Encontrar artigos relacionados ao tema aspectos humanos na segurança da informação revelou ser uma tarefa difícil e de acesso limitado. A escassez de estudos que abordassem esse tema tão crucial da segurança digital foi surpreendente e, por sua vezes, frustrante.

Por outro lado, ao explorar o universo dos *malwares*, a situação foi completamente diferente. Uma vasta quantidade de artigos relacionados estava disponível, destacando a atenção significativa dada a essa área específica da cibersegurança. A abundância de recursos sobre *malwares* contrastou fortemente com a escassez notável de informações sobre os aspectos humanos na segurança da informação.

Essa diferença entre a quantidade de artigos disponíveis sobre *malwares* em comparação com os estudos relacionados aos aspectos humanos na segurança da informação ressalta a necessidade de um foco maior e aprofundado na compreensão do papel humano na proteção dos sistemas digitais.

Capítulo

4

Resultados

Um estudo abrangente de 106 artigos revelou uma distribuição interessante de publicações ao redor do mundo. Surpreendentemente, apenas 18 desses artigos foram publicados no Brasil, e destes, somente um foi disponibilizado em um site específico o site (https://www.iso.org/standard/27001).

Antes de realizar essa revisão foi colocado o tema no chat GPT para que ele listasse alguns tópicos em alta relacionados com o tema dessa revisão, dos 20 tópicos listados. após reunir com o professor foram escolhidos 13. Após isso foram utilizadas palavras chaves, relacionadas com cada tópico para fazer a pesquisa para encontrar artigos no Google Scholar.

A maior parte das publicações, totalizando 88 artigos, emergiu de locais distintos como Estados Unidos da América, Indonésia, África do Sul, Holanda, Grécia, Jordânia e Austrália. Isso demonstra uma ampla diversidade geográfica na origem desses estudos.

Outro aspecto curioso é a linha temporal das publicações. A grande maioria, precisamente 101 artigos, foram publicados após o ano 2000, evidenciando um foco considerável em pesquisas mais contemporâneas. Por outro lado, apenas 4 artigos datam de antes desse período.

Esses números ressaltam a amplitude geográfica e temporal das pesquisas analisadas, oferecendo um panorama diversificado e uma linha do tempo clara sobre o escopo e a distribuição geográfica das publicações estudadas.

4.1 Conclusão

À medida que se avança em direção a uma era cada vez mais digital, a segurança das informações torna-se uma tarefa difícil. Este estudo teve como objetivo conscientizar os usuários sobre os perigos presentes nos espaços virtuais, realçando os riscos provenientes dos ataques de *malware* e dos temidos DDoS.

Adicionalmente, com o surgimento da inteligência artificial como uma aliada na defesa contra essas ameaças, fornecendo uma camada extra de proteção para aqueles que buscam segurança.

No entanto, a segurança da informação ultrapassa os limites da tecnologia; ela está diretamente ligada com os aspectos humanos, exigindo uma vigilância constante e uma abordagem pró-ativa por parte de todos.

Este estudo destacou os desafios enfrentados para manter os dados seguros, evidenciando a crescente complexidade do cenário tecnológico. A proteção da informação não se restringe somente à parte técnica, mas sim a um equilíbrio entre inovação e precaução, entre o avanço da tecnologia e a consciência dos usuários.

Assim sendo, para assegurar a proteção dos dados em um mundo em constante evolução tecnológica, é crucial que os usuários se mantenham informados, adotem práticas de segurança eficazes e se envolvam ativamente na preservação de sua própria segurança digital. Somente assim estará apto a enfrentar os desafios futuros e construir um ambiente digital mais seguro e confiável para todos.

4.2 Trabalhos Futuros

Devido a problemas técnicos não foi possível realizar o projeto como inicialmente foi planejado, por isso a ideia foi colocada como trabalho futuro. O projeto se trata de desenvolver um sistema web com contenha conteúdos de artigos e informações para que posteriormente o usuário realize uma avaliação para colocar os conhecimentos adquiridos em prática, a medida que ele for adquirindo mais conhecimento o nível das avaliações também vão aumentando.

Referências Bibliográficas

ABDALLA, P. A.; VAROL, A. Advantages to disadvantages of cloud computing for small-sized business. In: IEEE. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. [S.l.], 2019. p. 1–6.

ABRAHAM, S.; CHENGALUR-SMITH, I. Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, Elsevier, v. 87, p. 101586, 2019.

AIGBODI, M. et al. Defence in-depth for cyber security with custom anti-virus signature definition.

AL-SHAER, E. S.; HAMED, H. H. Firewall policy advisor for anomaly discovery and rule editing. *Integrated network management VIII: Managing it all*, Springer, p. 17–30, 2003.

ALBERTS, C. et al. Introduction to the octave approach. *Pittsburgh, PA, Carnegie Mellon University*, p. 72–74, 2003.

ALDAAJEH, S. et al. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, Elsevier, v. 119, p. 102754, 2022.

ALDAWOOD, H.; SKINNER, G. Educating and raising awareness on cyber security social engineering: A literature review. In: IEEE. *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*. [S.l.], 2018. p. 62–68.

ALEROUD, A.; ZHOU, L. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, Elsevier, v. 68, p. 160–196, 2017.

AMIN, S. M.; WOLLENBERG, B. F. Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine*, IEEE, v. 3, n. 5, p. 34–41, 2005.

ANDRESS, J. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. [S.l.]: Syngress, 2014.

ASLAN, Ö. A.; SAMET, R. A comprehensive review on malware detection approaches. *IEEE access*, IEEE, v. 8, p. 6249–6271, 2020.

BANERJEE, A.; NAUMANN, D. A. Stack-based access control and secure information flow. *Journal of functional programming*, Cambridge University Press, v. 15, n. 2, p. 131–177, 2005.

BASU, S. et al. Cloud computing security challenges & solutions-a survey. In: IEEE. *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. [S.l.], 2018. p. 347–356.

BAWANY, N. Z.; SHAMSI, J. A.; SALAH, K. Ddos attack detection and mitigation using sdn: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, Springer, v. 42, p. 425–441, 2017.

BLAKLEY, B.; MCDERMOTT, E.; GEER, D. Information security is information risk management. In: *Proceedings of the 2001 workshop on New security paradigms*. [S.l.: s.n.], 2001. p. 97–104.

BODIN, L. D.; GORDON, L. A.; LOEB, M. P. Information security and risk management. *Communications of the ACM*, ACM New York, NY, USA, v. 51, n. 4, p. 64–68, 2008.

BOSS, G. et al. Cloud computing. *IBM white paper*, http:,/downl0ad. boulder. ibm. com/ibmdl/pub/software/dw/wes/hipods/Cloud ..., v. 321, p. 224–231, 2007.

BRAGA, A. M.; MARINO, F. C. H.; SANTOS, R. R. dos. Segurança de aplicaçoes blockchain além das criptomoedas. *Sociedade Brasileira de Computação*, 2017.

CAMARINHA-MATOS, L. M. Collaborative smart grids–a survey on trends. *Renewable and Sustainable Energy Reviews*, Elsevier, v. 65, p. 283–294, 2016.

CAMP, L. J. Web security and privacy: An american perspective. *The Information Society*, Taylor & Francis, v. 15, n. 4, p. 249–256, 1999.

CAVELTY, M. D.; WENGER, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, Taylor & Francis, v. 41, n. 1, p. 5–32, 2020.

CHANG, R. K. Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE communications magazine*, IEEE, v. 40, n. 10, p. 42–51, 2002.

CHEN, H. *Intelligence and security informatics for international security: Information sharing and data mining*. [S.l.]: Springer Science & Business Media, 2006. v. 10.

CHEN, S. et al. Processes, benefits, and challenges for adoption of blockchain technologies in food supply chains: a thematic analysis. *Information Systems and e-Business Management*, Springer, v. 19, p. 909–935, 2021.

CHEN, Y.; RAMAMURTHY, K.; WEN, K.-W. Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, Taylor & Francis, v. 55, n. 3, p. 11–19, 2015.

CHHIKARA, J. et al. Phishing & anti-phishing techniques: Case study. *International Journal of Advanced Research in computer science and software engineering*, v. 3, n. 5, 2013.

CHOOBINEH, J. et al. Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, v. 20, n. 1, p. 57, 2007.

CIOACĂ, C.; BRATU, A.; ȘTEFĂNESCU, D. The analysis of benchmarking application in cyber security. *Scientific Research and Education in the Air Force–Afases 2017*, 2017.

CONCEIÇÃO, B. T. L. Confidencialidade e segurança da informação. 2019.

CURADO, C.; TEIXEIRA, S. M. Training evaluation levels and roi: The case of a small logistics company. *European Journal of Training and Development*, Emerald Group Publishing Limited, v. 38, n. 9, p. 845–870, 2014.

DANDURAND, L.; SERRANO, O. S. Towards improved cyber security information sharing. In: IEEE. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. [S.l.], 2013. p. 1–16.

ELMRABIT, N.; YANG, S.-H.; YANG, L. Insider threats in information security categories and approaches. In: IEEE. *2015 21st International Conference on Automation and Computing (ICAC)*. [S.l.], 2015. p. 1–6.

EPSTEIN, K. J.; TANCER, B. Enforcement of use limitations by internet services providers: How to stop that hacker, cracker, spammer, spoofer, flamer, bomber. *Hastings Comm. & Ent. LJ*, HeinOnline, v. 19, p. 661, 1996.

FARAHMAND, F. et al. A management perspective on risk of security threats to information systems. *Information Technology and Management*, Springer, v. 6, p. 203–225, 2005.

FIARRESGA, V. M. C. et al. *Criptografia e matemática*. Tese (Doutorado), 2010.

FIKRI, M. A. et al. Risk assessment using nist sp 800-30 revision 1 and iso 27005 combination technique in profit-based organization: Case study of zzz information system application in abc agency. *Procedia Computer Science*, v. 161, p. 1206–1215, 2019. ISSN 1877-0509.

FOOZY, C. F. M. et al. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In: *Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor*. [S.l.: s.n.], 2011.

FREET, D. et al. Cloud forensics challenges from a service model standpoint: Iaas, paas and saas. In: *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*. [S.l.: s.n.], 2015. p. 148–155.

GAMA, J. P. S. P. da. Cibercriminalidade organizada: os modelos de organização em rede e o cibercriminoso. 2021.

HAMLEN, K. W. et al. Exploiting an antivirus interface. *Computer Standards & Interfaces*, Elsevier, v. 31, n. 6, p. 1182–1189, 2009.

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018.

HONG, J. The state of phishing attacks. *Communications of the ACM*, ACM New York, NY, USA, v. 55, n. 1, p. 74–81, 2012.

ISO, I. *ISO/IEC 27001:2022*. 2022. Disponível em: <`https://www.iso.org/standard/27001`>. Acesso em: 11 de novembro 2023.

KALNIŅŠ, R.; PURIŅŠ, J.; ALKSNIS, G. Security evaluation of wireless network access points. *Applied Computer Systems*, Walter de Gruyter GmbH, v. 21, n. 1, p. 38–45, 2017.

KALOGRANIS, C. *Antivirus software evasion: an evaluation of the av evasion tools*. Tese (Doutorado) — University of Piraeus (Greece), 2018.

KHAN, B. et al. Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, Academic Journals, v. 5, n. 26, p. 10862, 2011.

KHANDO, K. et al. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, Elsevier, v. 106, p. 102267, 2021.

KHANJI, S.; IQBAL, F.; HUNG, P. Zigbee security vulnerabilities: Exploration and evaluating. In: IEEE. *2019 10th international conference on information and communication systems (ICICS)*. [S.l.], 2019. p. 52–57.

KIRDA, E.; KRUEGEL, C. Protecting users against phishing attacks with antiphish. In: IEEE. *29th Annual International Computer Software and Applications Conference (COMPSAC'05)*. [S.l.], 2005. v. 1, p. 517–524.

KORET, J.; BACHAALANY, E. *The antivirus hacker's handbook*. [S.l.]: John Wiley & Sons, 2015.

KUUSISTO, T.; ILVONEN, I. Information security culture in small and medium size enterprises. *Frontiers of E-business Research*, p. 431–439, 2003.

LAUREANO, M. A. P.; MAZIERO, C. A.; JAMHOUR, E. Detecção de intrusão em máquinas virtuais. *5º Simpósio de Segurança em Informática–SSI. São José dos Campos*, p. 1–7, 2003.

LI, L.; LEE, G. Ddos attack detection and wavelets. *Telecommunication Systems*, Springer, v. 28, p. 435–451, 2005.

LIMA, P. R. S.; FERREIRA, L. M. M.; PEIXOTO, A. L. V. de A. Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. *P2P E INOVAÇÃO*, v. 9, n. 1, p. 206–221, 2022.

LIU, A. X.; GOUDA, M. G. Diverse firewall design. *IEEE Transactions on Parallel and Distributed Systems*, IEEE, v. 19, n. 9, p. 1237–1251, 2008.

LÓPEZ, V. L. O. et al. Análise/avaliação de riscos de segurança de informação: quantificação de confiança como um parâmetro de redução de desvios de resultados por causas humanas. Universidade Federal de Santa Maria, 2014.

LYU, M. R.; LAU, L. K. Firewall security: Policies, testing and performance evaluation. In: IEEE. *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000*. [S.l.], 2000. p. 116–121.

MENDEL, J. et al. Smart grid cyber security challenges: Overview and classification. *e-mentor*, Szkoła Główna Handlowa w Warszawie, Fundacja Promocji i Akredytacji ..., v. 68, n. 1, p. 55–66, 2017.

MIHOVSKA, A.; SARKAR, M. Smart connectivity for internet of things (iot) applications. *New advances in the internet of things*, Springer, p. 105–118, 2018.

MOHAMMED, C. M.; ZEEBAREE, S. R. Sufficient comparison among cloud computing services: Iaas, paas, and saas: A review. *International Journal of Science and Business*, IJSAB International, v. 5, n. 2, p. 17–30, 2021.

MUGHAL, A. A. Artificial intelligence in information security: Exploring the advantages, challenges, and future directions. *Journal of Artificial Intelligence and Machine Learning in Management*, v. 2, n. 1, p. 22–34, 2018.

OSUAGWU, E. et al. Mitigating social engineering for improved cybersecurity. In: IEEE. *2015 International Conference on Cyberspace (CYBER-Abuja)*. [S.l.], 2015. p. 91–100.

OTTIS, R. Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. In: ACADEMIC PUBLISHING LIMITED READING, MA. *Proceedings of the 7th European Conference on Information Warfare*. [S.l.], 2008. p. 163.

OTUOZE, A. O.; MUSTAFA, M. W.; LARIK, R. M. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, Elsevier, v. 5, n. 3, p. 468–483, 2018.

OYAMA, D. D. Educação e cibercultura: Pontos positivos e negativos. *São Paulo:[sn]*, 2011.

PAPADIMITRATOS, P. et al. Secure vehicular communication systems: design and architecture. *IEEE Communications magazine*, IEEE, v. 46, n. 11, p. 100–109, 2008.

PARSONS, K. et al. *Human factors and information security: individual, culture and security environment*. [S.l.], 2010.

PIPLAI, A. et al. Creating cybersecurity knowledge graphs from malware after action reports. *IEEE Access*, IEEE, v. 8, p. 211691–211703, 2020.

PRADITYA, D.; JANSSEN, M. Benefits and challenges in information sharing between the public and private sectors. In: *Academic Conferences Limited*. [S.l.: s.n.], 2015. p. 246.

PRICHUA, E.; BERZ, E. L. Software para aplicabilidade das normas nbr iso/iec 27001 e nbr iso/iec 27002 e apoio à tomada de decisões em segurança de ti. 2012.

QBEITAH, M. A.; ALDWAIRI, M. Dynamic malware analysis of phishing emails. In: IEEE. *2018 9th International Conference on Information and Communication Systems (ICICS)*. [S.l.], 2018. p. 18–24.

RAMZAN, Z. Phishing attacks and countermeasures. *Handbook of information and communication security*, Springer, p. 433–448, 2010.

RANI, D.; RANJAN, R. K. A comparative study of saas, paas and iaas in cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, v. 4, n. 6, 2014.

RESENDE, D. A. Certificação digital. *Revista jurídica UNIGRAN*, v. 11, n. 22, p. 111, 2009.

RICHET, J.-L. From young hackers to crackers. *International Journal of Technology and Human Interaction (IJTHI)*, IGI Global, v. 9, n. 3, p. 53–62, 2013.

ROSA, K. M. Estudo de caso: caso do vazamento de dados do facebook. 284, 2021.

SAFA, N. S.; SOLMS, R. V.; FUTCHER, L. Human aspects of information security in organisations. *Computer Fraud & Security*, Elsevier, v. 2016, n. 2, p. 15–18, 2016.

SAHAMI, M. et al. A bayesian approach to filtering junk e-mail. In: CITESEER. *Learning for Text Categorization: Papers from the 1998 workshop*. [S.l.], 1998. v. 62, p. 98–105.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. *Future internet*, MDPI, v. 11, n. 4, p. 89, 2019.

SAMONAS, S.; COSS, D. The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, v. 10, n. 3, 2014.

SANTOS, G. P. Proteção geral de dados: invasão e vazamentos de dados. 2022.

SATYANARAYANA, S. Cloud computing: Saas. *Computer Sciences and Telecommunications*, - , n. 4, p. 76–79, 2012.

SCHUMACHER, M. Security patterns and security standards. In: CITESEER. *EuroPLoP*. [S.l.], 2002. p. 289–300.

SEN, M. et al. Issues of privacy and security in the role of software in smart cities. In: IEEE. *2013 International Conference on Communication Systems and Network Technologies*. [S.l.], 2013. p. 518–523.

SILVA, B. P. R. A. d. et al. Planeamento e implementação de um sistema de gestão da segurança da informação. 2011.

SILVA, F. M. F. Segurança da informação em instituições com dispositivos móveis pessoais conectados à rede: um levantamento sobre ferramentas e técnicas utilizadas. *Gestão da Segurança da Informação-Unisul Virtual*, 2017.

SIPONEN, M.; WILLISON, R. Information security management standards: Problems and solutions. *Information & management*, Elsevier, v. 46, n. 5, p. 267–270, 2009.

SKOPIK, F.; SETTANNI, G.; FIEDLER, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, Elsevier, v. 60, p. 154–176, 2016.

STEFANIUK, T. Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, v. 7, n. 3, p. 1832, 2020.

STEPHANOU, A. The impact of information security awareness training on information security behaviour. University of the Witwatersrand Johannesburg, South Africa, 2008.

SYAFITRI, W. et al. Social engineering attacks prevention: A systematic literature review. *IEEE Access*, IEEE, v. 10, p. 39325–39343, 2022.

TAEWEE, T. Cracker "keropok": A review on factors influencing expansion. *International Food Research Journal*, v. 18, n. 3, p. 855–866, 2011.

TAHIR, R. A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, Modern Education and Computer Science Press, v. 8, n. 2, p. 20, 2018.

TIJAN, E. et al. Blockchain technology implementation in logistics. *Sustainability*, MDPI, v. 11, n. 4, p. 1185, 2019.

TOURANI, R. et al. Security, privacy, and access control in information-centric networking: A survey. *IEEE communications surveys & tutorials*, IEEE, v. 20, n. 1, p. 566–600, 2017.

ULRICH, F. Bitcoin-a moeda na era digital. *Journal, volume*, v. 2, p. 239, 1892.

VELTE, A. T. V. T. J.; ELSENPETER, P. D. R. *Cloud computing*. [S.l.: s.n.], 2010.

WACK, J.; CUTLER, K.; POLE, J. Guidelines on firewalls and firewall policy. *NIST special publication*, v. 800, p. 41, 2002.

WEI, Y.; BLAKE, M. B. Service-oriented computing and cloud computing: Challenges and opportunities. *IEEE Internet Computing*, IEEE, v. 14, n. 6, p. 72–75, 2010.

WIDJAJARTO, A.; ALMAARIF, A. et al. Analisis karakteristik antivirus berdasarkan aktivitas malware menggunakan analisis dinamis. *Journal of Information System Research (JOSH)*, v. 4, n. 2, p. 693–700, 2023.

WILSON, M.; HASH, J. et al. Building an information technology security awareness and training program. *NIST Special publication*, v. 800, n. 50, p. 1–39, 2003.

YAZAR, Z. A qualitative risk analysis and management tool–cramm. *SANS InfoSec Reading Room White Paper*, Citeseer, v. 11, n. 1, p. 12–32, 2002.

YE, Y. et al. A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 50, n. 3, p. 1–40, 2017.

YEE, C. K.; ZOLKIPLI, M. F. Review on confidentiality, integrity and availability in information security. *Journal of Information and Communication Technology in Education*, v. 8, n. 2, p. 34–42, 2021.

ZHOU, Z.-H. *Machine learning*. [S.l.]: Springer Nature, 2021.

ZUNINO, J. D. Certificação digital: assinatura digital, certificados digitais e sua utilização no mercado nacional. *Maiêutica-Tecnologias da Informação*, v. 2, n. 1, 2017.