UNIVERSIDADE SANTO AMARO

CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

SEGURANÇA DA INFORMAÇÃO: PANORAMA E DESAFIOS

MARCIO APARECIDO FERREIRA – RA 4699670

PAULINO PARPINELI BUENO – RA 4659465

SÃO PAULO

2024

MARCIO APARECIDO FERREIRA – RA 4699670

PAULINO PARPINELI BUENO – RA 4659465

SEGURANÇA DA INFORMAÇÃO: PANORAMA E DESAFIOS

Monografia apresentada como Trabalho de Conclusão de Curso para a graduação em Engenharia de Software.

Orientador: Prof. Dr. Alexandre Las Casas.

SÃO PAULO

2024

RESUMO

A segurança da informação tornou-se uma preocupação central na era digital, devido ao crescente fluxo de dados e à digitalização de informações sensíveis, como dados pessoais e comerciais. O aumento da conectividade trouxe novas vulnerabilidades, como invasões, malware e phishing, que exigem uma abordagem robusta para garantir a confidencialidade, integridade e disponibilidade dos dados. Embora as soluções tecnológicas estejam evoluindo, muitos usuários negligenciam práticas básicas de proteção, como senhas fortes, autenticação multifatorial e atualizações regulares, o que os expõe a riscos desnecessários. A pesquisa destaca que a falta de conscientização e o comportamento inadequado dos usuários são responsáveis por muitas falhas de segurança. Assim, a educação contínua em segurança da informação, tanto em ambientes corporativos quanto educacionais, é essencial. Programas de conscientização, treinamentos e simulações de ataques são estratégias eficazes para preparar as pessoas para incidentes cibernéticos. A colaboração entre os setores público e privado é vital para criar políticas e desenvolver ferramentas que fortaleçam a proteção digital. Além disso, regulamentações como a LGPD desempenham um papel importante, incentivando empresas a adotarem práticas robustas. A responsabilidade pela segurança digital é compartilhada, e promover uma cultura de segurança é crucial para um ambiente digital seguro e resiliente.

Palavra-chave: Segurança da informação. Segurança cibernética. Melhores Práticas.

ABSTRACT

Information security has become a central concern in the digital age, due to the increasing flow of data and the digitization of sensitive information, such as personal and business data. Increased connectivity has brought new vulnerabilities, such as hacking, malware and phishing, which require a robust approach to ensure the confidentiality, integrity and availability of data. Although technological solutions are evolving, many users neglect basic protection practices, such as strong passwords, multi-factor authentication and regular updates, which exposes them to unnecessary risks. The research highlights that lack of awareness and inappropriate user behavior are responsible for many security breaches. Therefore, ongoing education in information security, both in corporate and educational environments, is essential. Awareness programs, training and attack simulations are effective strategies to prepare people for cyber incidents. Collaboration between the public and private sectors is vital to create policies and develop tools that strengthen digital protection. In addition, regulations such as the LGPD play an important role in encouraging companies to adopt robust practices. Responsibility for digital security is shared, and fostering a culture of security is crucial to a safe and resilient digital environment.

Keywords: Information Security. Cyber Security. Best Practices.

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

ARP spoofing - Protocolo de resolução de endereço

CSP - Content Security Policy

DDoS - Negação de Serviço Distribuída

DNS spoofing - Domain Name System

GDPR - General Data Protection Regulation

HTTPS - Protocolo de transferência de hipertexto seguro

IBRASPD - Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados

IOT - Internet das coisas

LGPD - Lei Geral de Proteção de Dados

MFA - Autenticação multifatorial

MitM - Man in the Middle

SI - Segurança da Informação

SQL - Structured Query Language

VPN - Rede Privada Virtual

XSS - Cross-Site Scripting

SUMÁRIO

1. INTRODUÇÃO

A segurança da informação tornou-se um dos temas mais relevantes da era digital, em que o fluxo de dados entre pessoas, empresas e governos é constante e crescente. A transformação digital trouxe inúmeras oportunidades e avanços para a sociedade, mas também abriu caminho para uma vasta gama de ameaças cibernéticas que podem comprometer a privacidade, a integridade e a disponibilidade de informações. Nesse contexto, a proteção dos dados se tornou uma prioridade tanto para organizações quanto para usuários individuais, que precisam estar cada vez mais atentos aos riscos associados ao uso de tecnologias. Em concordância com este contexto, SILVA (2023, p.38) destaca que “o tema é tão importante que existe a comemoração anual no dia 08 de fevereiro do Dia da Internet Segura (Safer Internet Day)”.

A necessidade de proteger informações sensíveis é um dos principais motores para a evolução da segurança da informação. Empresas, instituições financeiras, governos e até mesmo indivíduos armazenam quantidades enormes de dados, muitos dos quais são extremamente valiosos e, se acessados indevidamente, podem causar danos significativos. Dados bancários, registros médicos, informações pessoais e segredos comerciais são apenas alguns exemplos de informações que precisam ser protegidas contra roubo, manipulação ou destruição. Com o avanço das tecnologias de armazenamento e compartilhamento de informações, novas ameaças emergem constantemente, exigindo que as práticas de segurança se adaptem. Antigamente, as preocupações com a segurança da informação eram restritas a questões como o controle físico de acesso a documentos. Hoje, no entanto, a maior parte dos dados está digitalizada e pode ser acessada remotamente, o que amplia significativamente a superfície de ataque. Isso requer uma abordagem mais robusta e dinâmica de segurança, que combine processos, tecnologias e conscientização dos usuários. Como um ponto de atenção, MATHIAS (2024), informa que a OpenAI, criadora do ChatGPT, confirmou que seus engenheiros identificaram mais de 20 ataques cibernéticos utilizando a ferramenta.

Os ataques cibernéticos, como invasões de sistemas, malware, phishing e ransomware, são algumas das ameaças mais frequentes enfrentadas atualmente. A motivação por trás desses ataques pode variar de ganhos financeiros e sabotagem a

espionagem industrial e política. Além disso, a facilidade de disseminação e a rápida evolução das técnicas de ataque tornam a segurança cibernética um campo desafiador e em constante mudança. Para mitigar esses riscos, a segurança da informação baseia-se em três pilares fundamentais: confidencialidade, integridade e disponibilidade, que devem ser mantidos em equilíbrio para garantir a proteção eficaz dos dados. THOMAZ (2023) afirma que o tratamento de dados na atualidade requer cuidado extremo, tendo em vista o aumento no volume de informações geradas em face da evolução dos sistemas produtivos; portanto a preocupação com segurança é indispensável.

A disseminação das ameaças cibernéticas se dá, em grande parte, por conta da conectividade global proporcionada pela internet e pela interconectividade entre sistemas. O desenvolvimento da Internet das Coisas (IoT) e a expansão das redes 5G são exemplos de avanços tecnológicos que ampliam as oportunidades de inovação, mas também criam novas vulnerabilidades. Dispositivos como câmeras de segurança, eletrodomésticos inteligentes e sensores industriais, quando conectados à internet, podem se tornar portas de entrada para ataques se não forem devidamente protegidos. O cenário de segurança da informação também é afetado por fatores humanos, como o comportamento dos usuários. Muitas vezes, os erros humanos são a principal causa de falhas de segurança. A falta de conscientização sobre os riscos cibernéticos, como clicar em links suspeitos ou compartilhar informações sensíveis em plataformas inseguras, pode abrir brechas significativas para ataques. Portanto, a educação em segurança cibernética é tão importante quanto a implementação de tecnologias de proteção. Mesmo empresas consolidadas no cenário de desenvolvimento de softwares estão passíveis de problemas associados ao assunto, como a Totvs, que sofreu um ataque com ransonware e confirmou tal situação em setembro de 2024 (SANTINO, 2024).

O estudo de ameaças e de técnicas de mitigação deve ser um processo contínuo. As ameaças cibernéticas evoluem rapidamente e, por isso, a segurança da informação não pode ser tratada como um processo estático. Novos tipos de ataques surgem constantemente, exigindo que as organizações estejam sempre atualizadas e que as práticas de segurança sejam revisadas regularmente. A evolução de técnicas como a inteligência artificial e o aprendizado de máquina também apresenta novas oportunidades e desafios para o campo da segurança. Outro ponto relevante é a

crescente regulamentação sobre a proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia. Segundo o Tribunal de Justiça do Distrito Federal e dos Territórios (2024), “a norma tem por escopo garantir a movimentação e o uso adequados de informações reservadas, com a anuência do usuário”. Essas legislações visam garantir a privacidade e a segurança dos dados pessoais, impondo sanções a empresas que não implementem medidas adequadas de proteção. Além de trazer benefícios para os consumidores, essas regulamentações incentivam as organizações a investir mais na segurança de suas informações, promovendo um ambiente digital mais seguro e confiável.

O papel das empresas de tecnologia também é fundamental para o avanço da segurança da informação. Muitas dessas empresas investem pesadamente em pesquisa e desenvolvimento de novas soluções de segurança, além de colaborarem com governos e outras instituições para enfrentar as ameaças cibernéticas de maneira coordenada. A cooperação entre o setor público e o privado tem se mostrado essencial para combater cibercriminosos e aumentar a resiliência digital em nível global. Compreender o panorama atual da segurança da informação envolve não apenas a análise das ameaças tecnológicas, mas também as motivações e os perfis dos cibercriminosos. Existem grupos organizados, como hacktivistas e ciberterroristas, que atuam com propósitos ideológicos ou políticos, além de criminosos que têm como objetivo o ganho financeiro. Esses diferentes perfis de ameaças exigem estratégias de defesa variadas e que considerem tanto os aspectos técnicos quanto os comportamentais, incluindo técnica de programação, visto que “cada desenvolvedor é único, com seus pontos e fracos, preferências e aversões” (HUNT E THOMAS, 2010).

Neste contexto, a importância de investir em segurança da informação não pode ser subestimada. A implementação de políticas de segurança, o uso de ferramentas adequadas e a capacitação constante dos usuários são ações essenciais para a mitigação dos riscos, abrangendo tanto questões de hardware quando de software (FERREIRA, 2022). No entanto, é necessário que esse investimento seja visto como um processo contínuo e evolutivo, já que as ameaças cibernéticas estão em constante transformação. Por fim, a segurança da informação é uma área de estudo multidisciplinar que abrange desde aspectos técnicos, como criptografia e

controle de acesso, até questões legais e comportamentais. A proteção de dados é uma responsabilidade compartilhada entre governos, empresas e indivíduos, e sua efetividade depende de uma abordagem holística e coordenada. Diante de um futuro cada vez mais digital, garantir a segurança das informações é fundamental para preservar a privacidade, a confiança e a funcionalidade da sociedade moderna.

2. OBJETIVO

2.1. Objetivo geral

O objetivo geral deste trabalho é centrado em identificar os principais perigos que ameaçam a segurança de usuários e sistemas no campo da Engenharia de Software, bem como na proposição de ações que possam mitigar esses riscos.

2.2. Objetivo específico

Os objetivos específicos aqui propostos são:

- Analisar os tipos de ataques mais comuns direcionados a usuários de software e suas causas;
- Apresentar estratégias práticas para reduzir a vulnerabilidade de sistemas a essas ameaças;
- Identificar e categorizar os principais tipos de ataque cibernético que afetam usuários, tanto em nível individual quanto organizacional;
- Investigar, quando apoiado por acontecimentos reais e recentes, as falhas no processo de desenvolvimento de software que contribuem para essas vulnerabilidades;
- Propor ações para mitigar os perigos identificados, tanto do ponto de vista técnico quanto comportamental.

Com essas ações, espera-se contribuir para o fortalecimento da segurança de software e para a proteção dos dados dos usuários diante de ataques, propondo uma discussão aprofundada sobre o tema, além de criar bases para estudos futuros neste tema.

3. METODOLOGIA DA PESQUISA

A metodologia deste estudo é baseada em uma pesquisa bibliográfica, sendo esta conduzida utilizando material disponível em diversas fontes, incluindo artigos acadêmicos, livros, teses e publicações de especialistas no campo. CAVALCANTE E OLIVEIRA (2020) afirmam que o aumento da produção científica nas diversas áreas do conhecimento e a velocidade com que essa produção, em seus variados formatos (teses de doutorado, dissertações de mestrado e artigos científicos), tem sido divulgada reivindicam estudos de reconhecimento dos avanços científicos. Este contexto nos fornece apoio para afirmar que os diferentes métodos de revisão bibliográfica surgem como alternativas de compreensão ampla do conhecimento de um campo, área ou objeto de pesquisa. O foco deste estudo foi baseado em estudos que abordem os tipos de ataques cibernéticos que afetam diretamente os usuários de software, bem como os desafios enfrentados no processo de desenvolvimento e manutenção de sistemas seguros.

O levantamento bibliográfico foi realizado de maneira sistemática, buscando compreender tanto os aspectos técnicos envolvidos nas vulnerabilidades de softwares, quanto os fatores humanos que contribuem para a ocorrência de falhas de segurança, fator bastante impactante conforme NAKAMURA (2016). Além disso, foram analisadas práticas recomendadas de desenvolvimento seguro, com ênfase nas metodologias que integram a segurança desde as fases iniciais do ciclo de vida do software, como o gerenciamento de requisitos e o controle de qualidade. A análise inclui também a identificação de tendências emergentes em segurança da informação, focando em soluções que estão sendo adotadas de maneira eficaz por empresas e desenvolvedores. Após o levantamento e a análise dos materiais coletados, foi realizada uma síntese dos principais perigos e das melhores práticas para mitigação de riscos. O objetivo é criar um panorama atualizado sobre os desafios de segurança enfrentados atualmente e propor ações que possam ser aplicadas tanto por desenvolvedores quanto por usuários. A análise crítica permitirá comparar as soluções existentes e sugerir adaptações ou melhorias que contribuam para um ambiente mais seguro e confiável no desenvolvimento de software.

4. DESENVOLVIMENTO

A segurança da informação é uma preocupação fundamental na sociedade contemporânea, onde grande parte das interações, transações e dados pessoais são mediadas por sistemas digitais. Em um mundo cada vez mais conectado, o volume de informações sensíveis, como dados financeiros, informações pessoais e segredos empresariais, cresce exponencialmente. FERREIRA (2022) afirma que, “de alguns anos para cá, houve um aumento de dados de milhões de pessoas disponíveis na internet”. Com isso, o risco de que essas informações sejam comprometidas por ataques cibernéticos ou por falhas de segurança aumenta proporcionalmente. A preocupação com a segurança da informação é essencial para garantir a privacidade dos indivíduos, proteger a integridade de organizações e assegurar a continuidade de operações críticas, tanto no âmbito público quanto privado.

Uma das principais razões para se preocupar com a segurança da informação é a ameaça constante de ataques cibernéticos. Essa preocupação faz parte da estratégia nacional de segurança cibernética (BRASIL, 2020), no qual é definido o objetivo de tornar o Brasil uma país de excelência em segurança cibernética. Criminosos virtuais, conhecidos como hackers, exploram vulnerabilidades em sistemas para roubar dados, causar prejuízos financeiros ou até mesmo interromper serviços essenciais. Ataques como ransomware, que sequestram dados e exigem resgates para sua liberação, e phishing, que induz usuários a fornecerem informações confidenciais, são exemplos de como a falta de segurança pode impactar diretamente indivíduos e organizações. Além disso, ataques direcionados a infraestrutura crítica, como redes elétricas e sistemas de saúde, podem ter consequências catastróficas para a sociedade como um todo.

Outro fator que reforça a necessidade de preocupação com a segurança da informação é a crescente regulação de proteção de dados ao redor do mundo. Leis como a GDPR na Europa e a LGPD no Brasil impõem exigências rigorosas sobre como empresas e organizações devem lidar com os dados pessoais de seus usuários. O não cumprimento dessas regulamentações pode resultar em multas severas e danos à reputação das empresas, o que torna a segurança da informação uma prioridade estratégica para qualquer organização. Em 2023, a ANPD aplicou no Brasil a primeira multa por descumprimento à LGPD, no valor de R$ 14.400,00 (BRASIL,

2023). A implementação de medidas de proteção adequadas não só garante conformidade legal, mas também fortalece a confiança dos clientes e parceiros comerciais. É importante reforçar que a segurança da informação é um pilar essencial para a inovação tecnológica. À medida que novas tecnologias emergem, como a Internet das Coisas (IoT), inteligência artificial e computação em nuvem, a superfície de ataque se expande, introduzindo novos desafios de segurança. Sem a implementação de práticas de segurança robustas, o desenvolvimento dessas tecnologias pode ser comprometido, limitando seu potencial de transformação e progresso. Portanto, garantir a segurança da informação é essencial para o avanço tecnológico de maneira segura, sustentável e confiável, assegurando que tanto indivíduos quanto empresas possam usufruir dos benefícios das inovações sem correr riscos desnecessários.

A Figura 1 nos fornece um compilado de notícias de diversos veículos de comunicação com uma visão da amplitude dos ataques recentes que ocorreram em âmbito mundial, trazendo a necessidade de discussão e estudos sobre o tema, sob uma ótica científica, fins identificarmos as melhores práticas hoje utilizadas.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas.

Fonte: Página VEJA, CNN BRASIL, Rio de Janeiro, 2023.

4.1. Cenário mundial

A segurança da informação diz respeito a um conjunto de ações tomadas com o objetivo de proteger um grupo de dados, mantendo em segurança o valor que ele possui. Em síntese, a segurança da informação impede que determinados dados que precisam ser mantidos seguros caiam nas mãos de pessoas não autorizadas (BATISTELLA, 2020). Além disso, os processos de segurança da informação também são responsáveis por impedir que tais dados sejam destruídos acidentalmente, perdidos, roubados ou danificados.

Quando nos referimos a dados, estamos falando de qualquer informação, documento ou testemunho que permita chegar ao conhecimento ou dedução de algo (CONCEITO, 2019). Os dados pessoais, por exemplo, são o conjunto de informações distintas que permitem a identificação de determinada pessoa.

A IBRASPD (2023) compilou em um dos painéis de seu segundo congresso anual, realizado em 2023, incidentes de segurança da informação com repercussão na mídia, entre Janeiro de 2022 e Junho de 2023. A Figura 2 apresenta uma visão mundial dos incidentes com repercussão na mídia em 2022.

Figura 2: Incidentes de segurança com repercussão na mídia em 2022

Fonte: Página IBRASPD, 2023.

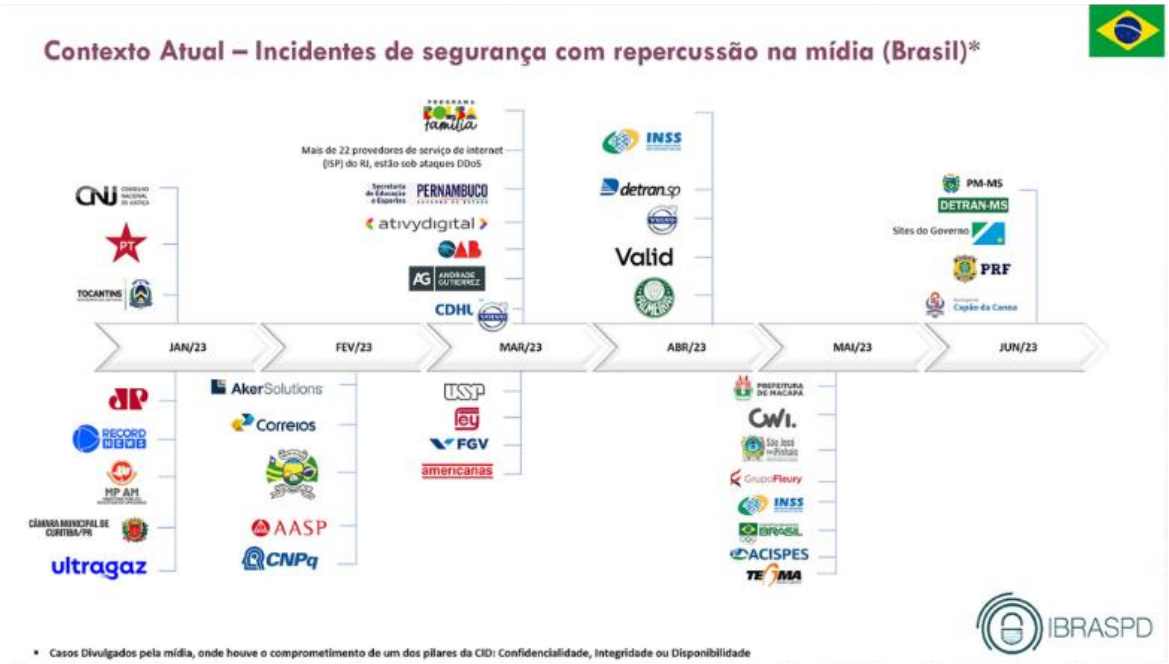
Já a Figura 3 apresenta uma visão dos incidentes de segurança da informação com repercussão na mídia com referência ao ano de 2023 (IBRASPD, 2023).

Figura 3: Incidentes de segurança com repercussão na mídia em 2023

Fonte: Página cenário mundial, IBRASPD, 2023.

Por fim, a Figura 4 apresenta um recorte dos incidentes mais significativos no ano de 2023 ocorridos no Brasil (IBRASPD, 2023).

Figura 4: Incidentes de segurança com repercussão na mídia em 2023 ocorridos no Brasil



Fonte: Página cenário Brasil, IBRASPD, 2023.

O aumento de casos de ataques hackers com o objetivo de roubar informações tem se tornado uma preocupação global nos últimos anos. Segundo COLAÇO (2024), esse aumento é impulsionado pela crescente sofisticação dos cibercriminosos. Esses ataques, que antes eram mais focados em alvos específicos, como grandes empresas e instituições financeiras, hoje afetam todos os setores, incluindo pequenas empresas, governos e até indivíduos comuns. Com a digitalização crescente e o aumento do número de dispositivos conectados à internet, os cibercriminosos encontram novas oportunidades para explorar vulnerabilidades em sistemas mal protegidos. Ataques como ransomware, phishing e violação de dados estão cada vez mais sofisticados, resultando em perdas financeiras significativas, vazamento de informações sensíveis e graves impactos na privacidade de milhões de pessoas ao redor do mundo.

Essa crescente onda de ataques hackers ressalta a importância crítica da segurança da informação no cenário atual. Governos e empresas têm investido mais em estratégias de cibersegurança para proteger suas redes e dados, mas a velocidade com que os criminosos desenvolvem novos métodos torna o desafio constante. BRASIL (2020), trabalha esta questão em dois eixos distintos, sendo um eixo focado em proteção e segurança, com a governança nacional, políticas de prevenção e mitigação além da proteção estratégica e, no outro eixo, os itens transformadores, sendo a dimensão normativa, a pesquisa, desenvolvimento e

inovação, a dimensão internacional e parcerias estratégicas e a o item focado em educação. Além das implicações econômicas, esses ataques afetam a confiança dos usuários em plataformas digitais e na capacidade das instituições de proteger suas informações. Em um mundo cada vez mais conectado, garantir a segurança dos dados tornou-se um pilar essencial para a estabilidade econômica, social e política, reforçando a importância de medidas eficazes e contínuas de proteção digital.

4.2. Segurança da informação e seus pilares

A segurança da informação é estruturada em três pilares fundamentais que formam a base de qualquer sistema de proteção digital: confidencialidade, integridade e disponibilidade. SILVA (2023) denomina estes princípios como Tríade CIA. Esses pilares são essenciais para garantir que os dados e informações sejam acessados, processados e armazenados de maneira segura, protegendo tanto os indivíduos quanto as organizações de ameaças internas e externas. A compreensão e a aplicação adequada desses conceitos são cruciais para o desenvolvimento de sistemas seguros e resilientes, capazes de mitigar riscos e prevenir ataques.

Cada um desses pilares desempenha um papel único e interdependente na segurança da informação, sendo estes seus princípios básicos (NAKAMURA, 2016). A confidencialidade garante que informações sensíveis sejam acessíveis apenas a indivíduos ou sistemas autorizados. A integridade assegura que os dados permaneçam precisos e não sejam alterados sem permissão. A disponibilidade, por sua vez, visa garantir que as informações e sistemas estejam sempre acessíveis e operacionais para os usuários autorizados quando necessário. Juntos, esses pilares formam a base para a implementação de políticas e práticas de segurança que protegem os dados em todas as suas fases.

Confidencialidade é o pilar que assegura que informações sensíveis sejam acessadas apenas por indivíduos ou sistemas devidamente autorizados (ISO 27001, 2013). Ela envolve a proteção de dados contra acessos não autorizados e garante que informações privadas, como senhas, dados financeiros ou documentos sigilosos, permaneçam restritas a quem tem permissão para visualizá-las ou manipulá-las. Para garantir a confidencialidade, são usadas técnicas como criptografia, controles de acesso e autenticação robusta, como sistemas de senhas e autenticação multifator. A

violação deste princípio pode resultar no comprometimento de informações críticas, expondo pessoas e organizações a riscos como fraudes, espionagem e roubo de identidade.

Integridade refere-se à garantia de que as informações mantidas em um sistema não sejam alteradas de maneira não autorizada, acidental ou maliciosa. Segundo a ABNT NBR ISO/IEC 27001:2013, integridade é a propriedade de salvaguarda da exatidão e completeza de ativos. Este pilar é crucial para assegurar que os dados permaneçam corretos, completos e confiáveis ao longo de todo o seu ciclo de vida. A integridade dos dados pode ser ameaçada por ataques, falhas de sistema ou erros humanos, e uma falha nesse aspecto pode comprometer a tomada de decisões com base em informações erradas. Para proteger a integridade, são aplicadas medidas como a verificação de hashes, backups regulares e o uso de logs de auditoria, que monitoram e registram todas as mudanças realizadas em um sistema ou banco de dados.

A disponibilidade garante que as informações e os sistemas estejam acessíveis e utilizáveis por usuários autorizados sempre que necessário (NAKAMURA, 2016). Esse pilar é especialmente importante em cenários onde a continuidade das operações é crítica, como em sistemas de saúde, bancos e infraestruturas essenciais. Ataques que comprometem a disponibilidade, como ataques de negação de serviço (DDoS), podem impedir que usuários legítimos acessem sistemas e dados, causando prejuízos financeiros e operacionais. Para assegurar a disponibilidade, são implementadas redundâncias, sistemas de backup, balanceamento de carga e planos de recuperação de desastres, que permitem a continuidade das operações mesmo diante de falhas ou ataques.

Esses três pilares trabalham em conjunto para proporcionar um ambiente seguro, no qual as informações são tratadas de maneira adequada, protegendo tanto a privacidade quanto a integridade dos sistemas e dados, conforme proposto pela Figura 5.

Figura 5: Pilares da Segurança da Informação

Fonte: Página UFRJ, 2020.

Vale destacar também que, segundo SILVA (2023), outros aspectos importantes podem ser considerados, como a “legalidade”, representada como a garantia de que a informação foi produzida em conformidade com a lei e a “autenticidade”, que é a garantia de que em um processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação, uma característica muito relevante para e-commerce e internet banking.

4.3. Tipos de ataque

Um ataque cibernético “compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (PAZ, 2019). Esses ataques são realizados por agentes maliciosos que exploram vulnerabilidades em sistemas, redes e dispositivos para obter acesso não autorizado, causar danos ou manipular informações. Eles podem se manifestar de diversas formas, e trazem grandes riscos à segurança da informação.

A gravidade de um ataque cibernético pode variar, desde simples invasões que causam pequenos transtornos até ações altamente sofisticadas que resultam em perdas financeiras, vazamento de informações sensíveis ou comprometimento de

infraestruturas críticas. FRUHLINGER (2018) classifica os ataques cibernéticos em duas modalidades: 1. Ataques em que o objetivo é desativar o computador de destino. 2. Ataques que objetivam acesso aos dados do computador atacado para talvez, obter privilégios de administrador. Com a crescente dependência da tecnologia na sociedade atual, a frequência e o impacto desses ataques têm aumentado, tornando a segurança da informação um tema cada vez mais relevante. A prevenção e a resposta a ataques cibernéticos exigem uma combinação de práticas de segurança, conscientização dos usuários e tecnologias avançadas para proteger sistemas contra ameaças em constante evolução.

4.3.1. Engenharia social: Phishing

Ataques cibernéticos do tipo engenharia social: phishing são métodos utilizados por criminosos para enganar usuários e fazê-los revelar informações confidenciais, como senhas, números de cartão de crédito ou outros dados sensíveis (INSTITUTO PROPAGUE, 2024). Esses ataques exploram a confiança dos usuários, simulando comunicações legítimas de empresas, instituições financeiras ou até mesmo contatos pessoais. O atacante cria mensagens, geralmente por e-mail, SMS ou redes sociais, que parecem ser de fontes confiáveis, induzindo o usuário a clicar em links maliciosos, baixar arquivos infectados ou inserir dados em páginas falsas.

O funcionamento do phishing é baseado na manipulação psicológica. Os cibercriminosos elaboram mensagens que provocam urgência, medo ou curiosidade, incentivando a vítima a agir rapidamente sem questionar a autenticidade da solicitação. Um exemplo comum é um e-mail que parece ser do banco, informando que há um problema com a conta e solicitando que o usuário faça login através de um link, que, na verdade, redireciona para uma página fraudulenta (FRUHLINGER, 2018). Uma vez que o usuário insere seus dados, eles são capturados pelos atacantes, que podem utilizá-los para fins maliciosos, como roubo de identidade ou fraude financeira.

Esses ataques podem ser sofisticados e difíceis de detectar, especialmente quando as comunicações são bem elaboradas e imitam com precisão as mensagens originais de uma organização. Por isso, a conscientização dos usuários e a aplicação de boas práticas, como verificar a autenticidade das mensagens e nunca clicar em links desconhecidos, são essenciais para prevenir ataques de phishing.

CHIN (2024), destaca alguns tipos específicos de phishing, que podem ser divididos nos seguintes agrupamentos:

- Spear phishing é uma variação mais direcionada do phishing tradicional, onde o atacante foca em uma pessoa ou grupo específico, personalizando a mensagem com informações sobre a vítima para torná-la mais convincente. Esse tipo de ataque frequentemente envolve pesquisas sobre a vítima para garantir que o conteúdo do e-mail ou mensagem pareça legítimo e pessoal, o que aumenta as chances de sucesso do ataque;

- Whaling phishing é uma forma de spear phishing que tem como alvo indivíduos de alto perfil, como executivos de empresas ou líderes organizacionais. O objetivo é obter informações sensíveis de alto valor, como segredos corporativos ou acessos privilegiados. Como esses alvos geralmente têm um maior nível de conscientização sobre segurança, os ataques de whaling são cuidadosamente planejados e altamente personalizados;

- Clone phishing ocorre quando os atacantes copiam uma mensagem legítima enviada anteriormente, recriam seu conteúdo e anexam links maliciosos. O ataque é bem-sucedido porque a vítima já confia na fonte da mensagem original, sendo mais propensa a clicar nos novos links ou abrir anexos sem suspeitar de qualquer ameaça;

- Angler phishing é uma forma de ataque que ocorre principalmente em plataformas de redes sociais. Os criminosos criam perfis falsos ou respondem a postagens de usuários que buscam ajuda de marcas ou serviços. Fingindo ser representantes legítimos da empresa, os atacantes enviam links maliciosos ou solicitam informações pessoais, aproveitando a confiança que os usuários têm em interações rápidas e públicas nas redes sociais.

4.3.2. Malware

Malware, uma contração de “malicious software” (software malicioso), refere-se a qualquer programa ou código projetado para infiltrar, danificar ou obter acesso não autorizado a um sistema computacional sem o conhecimento do usuário. Varia de vírus, worms, spyware a trojans, cada um com métodos únicos de ataque e

propagação. Identificar rapidamente tais ameaças é essencial para mitigar seus efeitos prejudiciais (SOUSA, 2024). O objetivo principal dos ataques cibernéticos que utilizam malware é comprometer a integridade, a confidencialidade ou a disponibilidade dos dados e sistemas de uma vítima. Esses programas maliciosos podem ser distribuídos por e-mails, sites infectados, downloads de software aparentemente legítimo ou até mesmo através de mídias removíveis, como pen drives. Uma vez que o malware é instalado, ele pode executar diversas ações prejudiciais, como roubo de dados, monitoramento de atividades, bloqueio de sistemas ou uso do dispositivo infectado para ataques em cadeia.

O funcionamento de um ataque de malware geralmente começa com a infiltração do código malicioso no sistema da vítima. SOUSA (2024) explica que isso pode ocorrer de várias maneiras, como ao clicar em links maliciosos, abrir anexos infectados ou visitar sites comprometidos. Após a instalação, o malware pode permanecer oculto no sistema, operando de maneira invisível para o usuário. Existem diferentes tipos de malware, cada um com um propósito específico, como vírus, worms, trojans (ou cavalos de Troia), ransomware e spyware. Por exemplo, um ransomware sequestra o sistema ou dados da vítima, exigindo um pagamento para restaurar o acesso, enquanto o spyware coleta dados sigilosos sem o conhecimento do usuário. O impacto de um ataque de malware pode ser alto para indivíduos, empresas e até infraestruturas críticas. Além de prejuízos financeiros, como roubo de informações bancárias ou pagamentos de resgate em ataques de ransomware, o malware pode comprometer a privacidade dos dados, causar a perda irreparável de informações e interromper serviços essenciais. Para proteger-se contra ataques de malware, é fundamental que os usuários adotem boas práticas de segurança, como manter softwares atualizados, evitar clicar em links desconhecidos, utilizar antivírus confiáveis e realizar backups regulares de dados.

4.3.3. Ransonware

Ransomware é um tipo de ataque cibernético no qual os criminosos utilizam software malicioso para sequestrar sistemas ou dados, bloqueando o acesso a eles até que um resgate (geralmente em criptomoedas) seja pago (TECHTUDO, 2023). Esse tipo de malware criptografa arquivos importantes no computador ou em uma rede, impedindo que o usuário ou empresa afetada utilize seus sistemas ou acesse

seus dados. Os criminosos exigem um pagamento em troca da chave de descriptografia, prometendo restaurar o acesso após o recebimento do valor. Esses ataques são geralmente executados através de e-mails fraudulentos, downloads maliciosos ou vulnerabilidades exploradas em sistemas desatualizados.

O funcionamento de um ataque de ransomware é relativamente simples, conforme descrição disponível no site TECHTUDO (2023): após infectar o dispositivo, o malware começa a criptografar os arquivos, tornando-os inacessíveis. Uma vez que a criptografia é concluída, a vítima recebe uma mensagem de extorsão, instruindo-a sobre como pagar o resgate para liberar os arquivos. Além da ameaça de perda de dados, alguns cibercriminosos também ameaçam expor informações confidenciais da vítima caso o pagamento não seja feito. Mesmo que o pagamento seja realizado, não há garantia de que os criminosos realmente irão fornecer a chave de descriptografia, o que torna o ataque ainda mais perigoso.

Nos últimos anos, os ataques de ransomware têm crescido exponencialmente, tanto em volume quanto em sofisticação. A América Latina tem sido uma das regiões mais afetadas, com o Brasil liderando o ranking de países mais atingidos, seguido por Colômbia e Argentina (NALIN, 2023). O aumento desses casos se deve à facilidade de distribuição do malware e à lucratividade para os criminosos, que aproveitam as vulnerabilidades em sistemas mal protegidos. Com empresas e governos cada vez mais dependentes de sistemas digitais, a proteção contra ransomware se tornou uma prioridade crítica para evitar danos financeiros, interrupção de serviços e comprometimento da privacidade.

A Tabela 1 auxilia a avaliação deste cenário e como o Brasil tem sido visado sob este tipo de ataque. NALIN (2023) identifica que “houve um crescimento exponencial em infraestrutura e serviços desde a privatização do mercado das telecomunicações até agora, elevando a posição de destaque do país”. Este não é o único motivo e outros fatores influenciam essa situação, como condições econômicas, nível educacional entre outros.

Tabela 1: Países que mais sofrem ataques cibernéticos na América Latina em 2022.

País	**Número de ataques**

Brasil	285.529
Colômbia	90.063
Argentina	25.800
Equador	24.540
Chile	24.184
México	15.328
Peru	14.197
Venezuela	2.537
Total da região (21 países)	727.686

Fonte: Página Veja, 2023

4.3.4. Man in the middle

Man in the Middle (MitM) é um tipo de ataque cibernético em que um invasor intercepta e manipula a comunicação entre duas partes sem que elas percebam (FRUHLINGER, 2018). O objetivo do ataque é roubar informações confidenciais, como credenciais de login, dados financeiros ou qualquer outra informação sensível que esteja sendo transmitida. O invasor posiciona-se entre a vítima e o serviço com o qual ela está se comunicando, agindo como um intermediário. Isso permite ao criminoso capturar, alterar ou até injetar dados na comunicação, fazendo com que ambas as partes acreditem que estão se comunicando diretamente uma com a outra.

Segundo FRUHLINGER (2018), o funcionamento de um ataque MitM geralmente começa com a interceptação da conexão, seja por meio de redes Wi-Fi desprotegidas, compromissos com roteadores ou o uso de técnicas como ARP spoofing e DNS spoofing, que redirecionam o tráfego da rede para o invasor. Uma vez que a comunicação é interceptada, o atacante pode observar ou modificar as mensagens sem que as partes envolvidas suspeitem. Por exemplo, em uma conexão bancária comprometida por um MitM, o invasor pode alterar os detalhes da transação,

transferindo dinheiro para sua própria conta em vez da conta pretendida pelo usuário, enquanto a vítima acredita estar realizando uma transação segura.

4.3.5. Cross site scripting

Cross-Site Scripting (XSS) é um tipo de ataque cibernético em que um invasor injeta scripts maliciosos em sites ou aplicações web, que são executados diretamente no navegador da vítima, conforme definição da CLOUDFLARE (2024). O objetivo desse ataque é comprometer a segurança de usuários ao explorar vulnerabilidades em sites que não validam corretamente as entradas fornecidas pelos usuários. O script injetado pode ser utilizado para roubar informações confidenciais, como cookies de sessão, credenciais de login ou outros dados sensíveis, além de realizar ações indesejadas em nome da vítima sem o seu conhecimento.

Baseado nas informações do canal Código Fonte TV (2022), o funcionamento de um ataque XSS começa quando o invasor insere um código malicioso em uma parte de uma página da web que será exibida para outros usuários, como campos de formulários, seções de comentários ou URLs. Quando a vítima acessa a página comprometida, o navegador executa o script injetado, acreditando ser um conteúdo legítimo. Existem diferentes tipos de XSS, como o armazenado, que permanece no servidor e afeta todos que acessam a página, e o refletido, onde o código malicioso é temporariamente retornado ao usuário por meio de uma solicitação manipulada. Uma vez que o script é executado, o invasor pode capturar dados ou realizar ações não autorizadas, comprometendo a segurança do usuário e do site.

4.3.6. DDoS

Um ataque de negação de serviço distribuído (DDoS) é um tipo de ataque cibernético em que o objetivo é sobrecarregar um servidor, serviço ou rede, tornando-os indisponíveis para os usuários legítimos. OLIVEIRA (2024), informa ainda que ataques do tido DDoS, pode paralisar websites, derrubar serviços online e causar estragos significativos na infraestrutura digital. O ataque é realizado através da inundação do alvo com um grande volume de tráfego malicioso proveniente de múltiplas fontes, geralmente uma rede de dispositivos comprometidos chamada botnet. Como o tráfego gerado é imenso e simultâneo, o servidor ou rede do alvo não

consegue processar todas as solicitações, levando à lentidão extrema ou à total interrupção dos serviços.

Segundo SOLHA, TEIXEIRA e PICCOLINI (2000), o funcionamento de um ataque DDoS envolve três etapas principais. Primeiro, o invasor compromete um grande número de dispositivos, como computadores, roteadores ou dispositivos IoT (Internet das Coisas), por meio de malwares. Esses dispositivos infectados formam a botnet, que é controlada remotamente pelo atacante. Em seguida, o invasor coordena a botnet para enviar um volume massivo de solicitações simultâneas ao alvo. Essas requisições sobrecarregam os recursos do servidor, como capacidade de processamento e largura de banda da rede, resultando em falhas ou interrupções temporárias do serviço.

Existem diferentes tipos de ataques DDoS, que podem variar dependendo da camada do sistema que está sendo atacada. Um ataque volumétrico, por exemplo, tenta esgotar a largura de banda da rede, enquanto um ataque ao protocolo pode explorar falhas específicas em como um servidor lida com solicitações. Já os ataques à camada de aplicação miram diretamente serviços como sites, enviando múltiplas requisições para esgotar os recursos do servidor. Independentemente do método utilizado, o objetivo é o mesmo: fazer com que o alvo não consiga responder adequadamente às requisições legítimas. SOLHA, TEIXEIRA e PICCOLINI (2000) descrevem, também, que o impacto de um ataque DDoS pode ter grandes consequências, especialmente para empresas que dependem de seus serviços online para operar. Durante o ataque, o site ou serviço se torna inacessível para clientes e usuários, resultando em perda de receita, danos à reputação e aumento de custos para mitigar o ataque e restaurar o funcionamento normal. Para combater esses ataques, são implementadas medidas de segurança como o uso de firewalls, balanceamento de carga e serviços de mitigação especializados, que ajudam a filtrar o tráfego malicioso e manter o serviço disponível, mesmo diante de um ataque.

4.3.7. Password attack (brute force)

Um Password Attack do tipo Brute Force é uma técnica de ataque cibernético em que o invasor tenta adivinhar ou "forçar" uma senha por meio de tentativas sucessivas, utilizando todas as combinações possíveis até encontrar a correta.

FERNANDES (2022), afirma que este tipo de ataque pode ser realizado de forma manual ou automática. O processo envolve a utilização de programas automatizados que testam grandes volumes de combinações de caracteres, incluindo letras, números e símbolos, para descobrir a senha de um usuário. Esses ataques podem ser direcionados a contas de e-mail, redes sociais, sistemas corporativos ou qualquer plataforma que utilize autenticação por senha. O funcionamento de um ataque de força bruta é simples, mas extremamente eficiente contra senhas fracas ou mal protegidas. O software utilizado pelo atacante executa milhões de tentativas por segundo, testando todas as combinações possíveis até que a senha correta seja descoberta. A eficácia do ataque depende do poder computacional disponível e da complexidade da senha; quanto mais curta e simples for a senha, mais rápido será o processo de quebra.

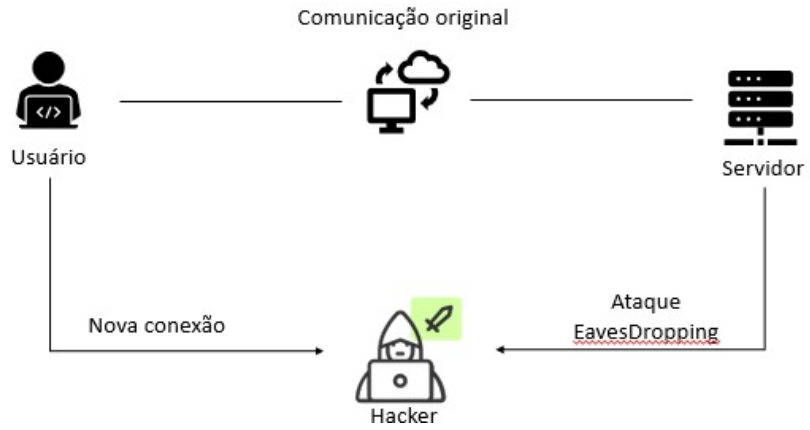
4.3.8. Drive-by-attack

Um Drive-by Attack é um tipo de ataque cibernético no qual o invasor infecta o sistema da vítima quando ela simplesmente visita um site comprometido. Antes, segundo o portal PSAFE (2013), este tipo de ataque era mais comum via download de arquivos infectados com códigos maliciosos. Ao contrário de outros métodos de ataque que exigem a interação do usuário, como clicar em um link ou baixar um arquivo, o drive-by attack explora vulnerabilidades no navegador, plugins ou software desatualizados. O código malicioso é automaticamente executado enquanto a página é carregada, permitindo ao atacante instalar malware no dispositivo da vítima sem que ela perceba. O funcionamento desse ataque depende da exploração de falhas de segurança em sites legítimos ou em servidores mal configurados. Os criminosos injetam scripts maliciosos nas páginas da web, e, quando o usuário acessa a página, o código é executado silenciosamente. Esses ataques podem resultar na instalação de malware como trojans, ransomware ou spyware, que podem roubar dados, monitorar atividades ou comprometer a integridade do sistema. Para se proteger contra drive-by attacks, é essencial manter o navegador e os plugins atualizados, além de utilizar ferramentas de segurança, como antivírus e bloqueadores de scripts maliciosos.

4.3.9. EavesDropping

Eavesdropping é um tipo de ataque cibernético em que um invasor intercepta comunicações entre duas partes sem o consentimento delas, com o objetivo de obter informações confidenciais ou sensíveis. PRADA (2024), define este tipo de ataque como “a prática de interceptar e escutar conversas ou comunicações eletrônicas sem o consentimento dos envolvidos. Isso pode ser feito através de técnicas de interceptação de rede, como sniffing de pacotes”. Esse tipo de ataque pode ocorrer em diferentes formas de comunicação, como e-mails, chamadas telefônicas, mensagens instantâneas ou tráfego de rede. Os atacantes utilizam técnicas como sniffing, que envolve a captura de pacotes de dados em uma rede, ou exploits que aproveitam falhas de segurança em protocolos de comunicação para acessar informações transmitidas. O funcionamento do eavesdropping é frequentemente facilitado por redes não seguras, como redes Wi-Fi públicas, onde a falta de criptografia torna as comunicações vulneráveis à interceptação. Uma vez que o invasor consegue acessar a comunicação, ele pode coletar dados como senhas, números de cartão de crédito ou informações pessoais. Para se proteger contra esse tipo de ataque, é fundamental utilizar conexões seguras, como HTTPS para navegação na web, VPNs para proteger o tráfego em redes públicas e criptografia de ponta a ponta em mensagens, que garantem que apenas as partes envolvidas possam acessar as informações transmitidas.

Figura 6: Esquemático de um ataque EavesDropping.



Fonte: Autor próprio, 2024.

4.3.10. SQL Injection

SQL Injection é uma técnica de ataque cibernético que explora vulnerabilidades em aplicações web que utilizam bancos de dados (FRUHLINGER, 2018). O atacante insere ou "injeta" comandos SQL maliciosos em campos de entrada, como formulários de login ou pesquisa, que não são devidamente filtrados ou validados. Esse tipo de ataque permite que o invasor execute comandos SQL arbitrários no banco de dados da aplicação, possibilitando acesso não autorizado a dados sensíveis, como informações pessoais de usuários, credenciais de login ou até mesmo a manipulação completa do banco de dados.

Segundo FRUHLINGER (2018), o funcionamento de um ataque SQL Injection geralmente começa com a identificação de um ponto vulnerável na aplicação, onde o atacante pode inserir comandos SQL. Por exemplo, ao tentar acessar uma conta de usuário, um invasor pode inserir uma string manipulada no campo de senha que altera a consulta SQL original, permitindo que ele contorne a autenticação e acesse a conta sem conhecer a senha real. Esse método pode ser utilizado para extrair informações, modificar dados existentes ou até mesmo excluir tabelas inteiras do banco de dados. Além de simples tentativas de login, as injeções SQL podem ser utilizadas para realizar ataques mais complexos, como a extração de dados confidenciais, o que pode levar a vazamentos de informações e compromissos de segurança. Os atacantes podem, por exemplo, utilizar SQL Injection para criar novas contas de usuário com privilégios elevados, permitindo acesso administrativo à aplicação. A gravidade desse tipo de ataque está na sua capacidade de causar danos significativos a sistemas, afetando a integridade dos dados e a confiança dos usuários nas aplicações.

4.4. Formas de proteção

A prevenção de ataques cibernéticos começa com a conscientização e a educação dos usuários sobre as ameaças existentes. NAKAMURA (2016) afirma treinamentos regulares sobre segurança da informação, que abordem como identificar e responder a ataques, são fundamentais para criar uma cultura de segurança dentro das organizações e vida privada. Hoje este é um papel de empresas privadas, mas é importante este tópico estar presente na educação, desde os primeiros níveis, devido a cada vez mais crescente utilização de dispositivos eletrônicos por crianças. A

população deve ser instruída a reconhecer sinais de phishing e outras tentativas de engenharia social, além de entender a importância de manter senhas seguras e não compartilhar informações confidenciais.

Outra prática essencial, conforme descrito por MARCHI (2024) é a implementação de medidas de segurança robustas, como autenticação multifatorial (MFA), que adiciona uma camada extra de proteção ao processo de login. O uso de softwares de segurança, como antivírus e firewalls, também é crucial para proteger dispositivos contra malware e outras ameaças. Manter sistemas e aplicativos atualizados, com patches de segurança aplicados prontamente, ajuda a fechar brechas que podem ser exploradas por atacantes.

É importante, também, segundo NAKAMURA (2016), a realização de backups regulares dos dados é uma prática recomendada para garantir que informações críticas não sejam perdidas em caso de um ataque, como ransomware. Os backups devem ser armazenados em locais seguros, preferencialmente offline ou em nuvem, para evitar que também sejam comprometidos. Avaliações de risco e testes de segurança periódicos ajudam a identificar vulnerabilidades e a garantir que as medidas de proteção sejam eficazes.

O contexto corporativo incorpora desafios adicionais e MANOEL (2014), afirma que a gestão é o básico numa organização, ou seja, atuar no nível da gestão é buscar meios para implementar a estratégia definida pela governança de segurança da informação. Enquanto no nível estratégico se planeja, no nível tático tomam-se decisões reais a respeito de mecanismos, abordagens e ações de SI que permitem a organização atingir objetivos estratégicos.

Além destas recomendações, no caso de ataques do tipo phishing, outra estratégia eficaz é a adoção de políticas de comunicação que orientem as pessoas sobre como compartilhar informações sensíveis. FRUHLINGER (2018) ressalta que é importante estabelecer regras claras sobre a não solicitação de informações confidenciais por e-mail ou mensagens, especialmente sem verificação. O uso de tecnologias de filtragem de e-mail pode ajudar a detectar e bloquear mensagens de phishing antes que cheguem aos usuários. Ferramentas que analisam o conteúdo e

os remetentes dos e-mails podem reduzir significativamente a probabilidade de um ataque bem-sucedido.

Para prevenir infecções por malware, SOUSA (2024) recomenda a instalação de softwares antivírus e antimalware em todos os dispositivos é muito importante. Essas ferramentas devem ser mantidas atualizadas para que possam detectar e neutralizar novas ameaças. Além disso, é importante configurar o sistema para realizar verificações regulares e automáticas em busca de malware. A conscientização dos usuários também desempenha um papel vital na prevenção. A população deve ser instruída a não clicar em links ou baixar anexos de fontes desconhecidas, além de evitar a instalação de softwares de fontes não confiáveis. Manter o sistema operacional e todos os aplicativos atualizados ajuda a fechar vulnerabilidades que poderiam ser exploradas por malware.

A prevenção contra ransomware envolve uma abordagem em múltiplas camadas (NALIN, 2023). Primeiro, as pessoas devem realizar backups regulares e armazená-los em locais seguros, como em nuvem ou offline. Isso garante que, caso um ataque ocorra, os dados possam ser recuperados sem a necessidade de pagamento de resgates. Outra prática essencial é a implementação de políticas de segurança rigorosas pelas empresas, que incluem a limitação de privilégios de acesso dos usuários.

Para se proteger contra ataques Man in the Middle, FRUHLINGER (2018) recomenda usar conexões seguras, como HTTPS, sempre que possível. O uso de redes privadas virtuais (VPNs) também é recomendado, especialmente ao acessar redes públicas ou desconhecidas. Além disso, é importante evitar a transmissão de informações sensíveis em redes não seguras.

A prevenção de ataques XSS pode ser alcançada através da validação e sanitização rigorosa das entradas de usuários em aplicações web, conforme orientações da CLOUDFLARE (2024). É essencial que os desenvolvedores utilizem técnicas de codificação segura, como a utilização de bibliotecas que protejam contra injeções de scripts. Além disso, cabeçalho de segurança como o Content Security Policy (CSP) pode ser implementado para reduzir o risco de execução de scripts maliciosos.

Para mitigar ataques DDoS, DANTAS (2015) recomenda algumas estratégias, as quais destaca-se a implementação soluções de proteção que possam detectar e filtrar tráfego anômalo antes que ele atinja os servidores. O uso de serviços de mitigação DDoS, que distribuem o tráfego entre vários servidores, pode ajudar a absorver ataques massivos e manter os serviços online. Outra prática eficaz é a configuração de sistemas de alerta e monitoramento que identifiquem picos de tráfego incomuns. Com uma resposta rápida a esses alertas, as organizações podem implementar medidas de contenção antes que o ataque cause interrupções significativas.

A melhor forma de prevenir ataques de força bruta é utilizar senhas longas e complexas, CUPRIK (2023) sugere a combinação de letras maiúsculas, minúsculas, números e símbolos. Além disso, a implementação de autenticação multifatorial (MFA) adiciona uma camada extra de segurança, tornando muito mais difícil para um invasor acessar uma conta, mesmo que consiga descobrir a senha. Outra opção é a utilização de aplicativos de gerenciamento de senhas.

Para se proteger contra drive-by attacks, é fundamental manter todos os navegadores e plugins atualizados, garantindo que as últimas correções de segurança estejam aplicadas, conforme descrito por SILVESTRE (2022). Além disso, o uso de bloqueadores de scripts e extensões de segurança que detectem sites maliciosos pode reduzir significativamente o risco de infecção por malware ao visitar sites comprometidos.

A prevenção de ataques de SQL Injection envolve os programadores e começa com a implementação de práticas de codificação segura, como o uso de consultas preparadas e procedimentos armazenados. HOGLUND E MCGRAW (2006) propõem que três fatores atuam em conjunto para tornar desafiador o gerenciamento de risco de software: complexidade, extensibilidade e conectividade. Validar e sanitizar todas as entradas de usuários é essencial para garantir que dados maliciosos não sejam processados pela aplicação. Além disso, a realização de testes de segurança e auditorias regulares pode ajudar a identificar e corrigir vulnerabilidades antes que sejam exploradas.

4.5. Logins e senhas

Criar senhas fortes é uma das medidas mais importantes que os usuários podem adotar para proteger suas contas online e dados pessoais. Em um mundo cada vez mais digital, onde transações financeiras, comunicações e armazenamento de informações sensíveis ocorrem online, a segurança das senhas é fundamental para evitar acessos não autorizados. Senhas fracas ou reutilizadas em múltiplas contas tornam-se um convite aberto para os atacantes, que podem facilmente comprometer informações valiosas se conseguirem descobrir ou adivinhar as senhas. Neste contexto, CUPRIK (2023) fornece algumas percepções de como criar senhas robustas para mitigar os problemas de ataques cibernéticos.

Segundo CUPRIK (2023), uma senha forte deve ser longa, contendo no mínimo 12 a 16 caracteres. A complexidade é igualmente importante; uma boa senha deve incluir uma combinação de letras maiúsculas, minúsculas, números e símbolos. Essa variedade dificulta que os atacantes que utilizam técnicas como força bruta ou dicionário consigam adivinhar a senha. Além disso, evitar palavras comuns ou combinações facilmente associáveis, como datas de nascimento ou nomes de familiares, pode aumentar ainda mais a segurança da senha. Ao criar uma senha, também é importante não a reutilizar em diferentes sites ou serviços. Se um site for comprometido e a senha for exposta, todas as outras contas que utilizam a mesma senha ficam em risco. Uma solução eficaz para gerenciar múltiplas senhas é o uso de gerenciadores de senhas, que podem gerar e armazenar senhas complexas de forma segura. Isso permite que os usuários utilizem senhas únicas e robustas para cada conta, sem precisar memorizá-las.

Outro ponto de atenção indicado por CUPRIK (2023) é a atualização regular das senhas. Mesmo que uma senha tenha sido criada seguindo as melhores práticas, é aconselhável alterá-la periodicamente, especialmente se houver indícios de que uma conta possa ter sido comprometida. Além disso, os usuários devem ficar atentos a qualquer comunicação suspeita que solicite informações de login e evitar clicar em links ou baixar arquivos de fontes não confiáveis, pois isso pode resultar em phishing e comprometimento de contas.

A autenticação multifatorial (MFA) é uma excelente forma de adicionar uma camada extra de segurança às contas, conforme indicado por MARCHI (2024). Mesmo que um invasor consiga obter a senha de um usuário, a MFA exigirá uma segunda forma de verificação, como um código enviado por mensagem de texto ou um aplicativo de autenticação, tornando muito mais difícil o acesso não autorizado. Portanto, sempre que possível, habilitar essa funcionalidade é altamente recomendado.

Outro ponto a se destacar é que criar senhas fortes é uma parte fundamental da segurança online (MATTHEWS, 2023), mas deve ser complementada com boas práticas de segurança geral. A educação contínua sobre as ameaças cibernéticas e a vigilância constante em relação a atividades suspeitas são essenciais. Investir tempo para desenvolver senhas seguras e adotar medidas de segurança adicionais pode fazer uma diferença significativa na proteção contra ataques cibernéticos, garantindo que as informações pessoais e financeiras permaneçam seguras em um ambiente digital cada vez mais arriscado.

5. RESULTADOS E DISCUSSÕES

Os resultados deste estudo evidenciam a crescente importância da segurança da informação em um mundo cada vez mais digitalizado. Com o aumento exponencial de transações online e o armazenamento de dados sensíveis em plataformas digitais, a necessidade de proteger essas informações contra ameaças cibernéticas se torna uma prioridade. A análise das principais ameaças e vulnerabilidades demonstrou que, apesar das tecnologias avançadas disponíveis, muitos usuários ainda não adotam práticas adequadas para se proteger online, o que aumenta a probabilidade de ataques bem-sucedidos. Tal contexto atingiu um nível tão crítico que existem autores que utilizam o termo “computação forense”, que consiste em uma ciência voltada à investigação criminal aplicada a determinados sistemas digitais, visando documentar, interpretar, analisar, identificar, validar, coletar e preservar todas as evidências a fim de lhes conferir a veracidade probatória em juízo. Também com esta abordagem, podemos afirmar que a organização precisa definir as questões externas e internas que são relevantes para o seu propósito e que afetam sua habilidade em alcançar o(s) resultado(s) pretendido(s) do seu sistema de gerência de segurança da informação.

Navegar na internet com segurança é essencial em um mundo digital repleto de ameaças cibernéticas. À medida que as atividades online se tornam mais comuns, desde compras até comunicações pessoais, a proteção de informações pessoais e a segurança contra ataques se tornam prioritárias. A adoção de boas práticas de navegação pode ajudar a reduzir significativamente os riscos e garantir uma experiência online mais segura.

Uma das primeiras medidas de segurança ao navegar na internet é garantir que a conexão seja sempre segura. Isso inclui usar redes privadas sempre que possível e evitar redes Wi-Fi públicas, que são frequentemente alvo de ataques Man in the Middle. Quando o uso de uma rede pública for necessário, é recomendável utilizar uma rede privada virtual (VPN) para criptografar o tráfego de dados e proteger a privacidade das informações transmitidas. Além disso, ao visitar sites, verifique se a URL começa com "https://" em vez de "http://", pois o "s" indica que a conexão é segura.

Outra prática importante é manter todos os dispositivos e softwares atualizados. Isso inclui o sistema operacional, navegadores e aplicativos, que frequentemente lançam atualizações para corrigir vulnerabilidades de segurança. A instalação de um software antivírus confiável também é fundamental para detectar e bloquear ameaças, como malware e spyware. Realizar varreduras regulares no dispositivo pode ajudar a identificar e remover qualquer software malicioso que possa ter sido instalado sem o conhecimento do usuário.

A conscientização sobre phishing e outros tipos de engenharia social é vital para uma navegação segura. Os usuários devem ser cautelosos ao clicar em links em e-mails ou mensagens, especialmente se forem de remetentes desconhecidos ou parecerem suspeitos. Além disso, nunca deve ser fornecida informação pessoal ou financeira a menos que se tenha certeza da legitimidade do site. O uso de navegadores que oferecem proteção contra sites fraudulentos pode ajudar a identificar e bloquear tentativas de phishing antes que o usuário seja enganado.

Além disso, a criação de senhas fortes e a utilização da autenticação multifatorial (MFA) em contas online são práticas fundamentais para proteger informações pessoais. Senhas únicas e complexas dificultam o acesso não

autorizado, e a MFA adiciona uma camada extra de segurança ao exigir uma segunda forma de verificação. Além disso, os usuários devem considerar o uso de gerenciadores de senhas para ajudar a organizar e proteger suas credenciais de forma eficiente.

Seguir essas melhores práticas não apenas protege os dados pessoais, mas também promove uma navegação mais tranquila e segura. A internet oferece uma infinidade de oportunidades e recursos, e navegar de maneira consciente e informada permite que os usuários aproveitem esses benefícios sem comprometer sua segurança. A vigilância constante e a educação sobre os riscos cibernéticos são fundamentais para garantir uma experiência online segura e protegida.

A pesquisa realizada também destaca a eficácia de medidas preventivas que podem ser implementadas tanto por indivíduos quanto por organizações. A criação de senhas fortes, a adoção de autenticação multifatorial e a conscientização sobre os diferentes tipos de ataques cibernéticos, como phishing e ransomware, são práticas que podem reduzir significativamente o risco de compromissos de segurança. Além disso, a atualização regular de softwares e sistemas operacionais é fundamental para proteger dispositivos contra vulnerabilidades conhecidas. Essas recomendações são importantes para promover uma cultura de segurança mais robusta.

A divulgação e adoção das recomendações apresentadas neste estudo aumenta a conscientização sobre a segurança da informação. Campanhas educativas voltadas para usuários e funcionários de empresas devem ser implementadas para disseminar informações sobre as melhores práticas de navegação e proteção de dados. A formação contínua e o treinamento sobre as ameaças cibernéticas devem ser uma prioridade nas organizações, para que os colaboradores se tornem a primeira linha de defesa contra ataques.

Além da educação, a colaboração entre empresas de tecnologia, governos e instituições de ensino fortalece a segurança cibernética em nível comunitário e nacional. A criação de parcerias e iniciativas conjuntas pode resultar em recursos e ferramentas mais eficazes, além de promover um intercâmbio de informações sobre ameaças emergentes. Este tipo de colaboração pode ajudar a desenvolver soluções

inovadoras e tecnologias de segurança mais eficazes, beneficiando todos os setores da sociedade.

A disseminação do conhecimento sobre segurança da informação deve ir além do ambiente corporativo. Instituições educacionais têm um papel fundamental na formação de cidadãos conscientes sobre a importância da proteção de dados desde a infância. A inclusão de temas relacionados à segurança cibernética nos currículos escolares pode preparar as novas gerações para navegar de maneira segura na internet e proteger suas informações pessoais.

Os resultados deste estudo também revelam que, apesar do aumento da conscientização sobre a segurança da informação, muitos usuários ainda subestimam os riscos associados ao compartilhamento de informações pessoais online. Deste modo, é importante que a comunicação sobre segurança cibernética seja clara e acessível, utilizando uma linguagem simples que possa ser compreendida por todos. Isso pode ajudar a eliminar mitos e desinformações que podem levar a comportamentos inseguros.

Outra conclusão importante é a necessidade de políticas e regulamentações mais robustas relacionadas à proteção de dados. A implementação de leis que exijam que empresas e organizações adotem práticas de segurança adequadas não apenas protegerá os consumidores, mas também incentivará a responsabilidade nas práticas de coleta e armazenamento de informações. Políticas que abordem diretamente a segurança da informação podem ajudar a criar um ambiente mais seguro para todos os usuários da internet.

O estudo também enfatiza que a tecnologia é uma aliada na segurança da informação, mas não deve ser vista como a única solução. A educação e a conscientização dos usuários são igualmente essenciais para a construção de um ecossistema digital seguro. Os ataques cibernéticos evoluem constantemente, e, portanto, os usuários devem estar sempre informados sobre as novas ameaças e as melhores práticas para mitigá-las.

A segurança da informação é uma responsabilidade compartilhada que envolve todos os usuários da internet. A proteção de dados pessoais e a segurança online não são apenas tarefas dos profissionais de TI, mas de todos que utilizam a tecnologia

diariamente. A promoção de uma cultura de segurança digital é fundamental para garantir que todos possam desfrutar dos benefícios da tecnologia de forma segura e responsável. A conscientização, a educação e a colaboração são as chaves para um futuro digital mais seguro e protegido.

6. CONCLUSÃO

Esta pesquisa destaca a crescente importância da segurança da informação em um cenário global marcado por rápidas inovações tecnológicas e um aumento significativo de atividades online. À medida que as empresas e os indivíduos se tornam mais dependentes da tecnologia para a realização de tarefas diárias, a proteção de informações sensíveis tornou-se uma questão crítica. As evidências apresentadas ao longo do estudo mostram que, apesar dos avanços em tecnologia de segurança, muitos usuários ainda não implementam práticas adequadas para proteger suas informações pessoais e profissionais.

Uma das principais constatações deste trabalho é a identificação das ameaças mais comuns enfrentadas por usuários e organizações, como phishing, ransomware e malware. Esses tipos de ataques não apenas comprometem a segurança dos dados, mas também podem ter consequências financeiras e reputacionais significativas. Portanto, a conscientização sobre essas ameaças é vital para preparar os usuários para reconhecer e responder a situações de risco. O conhecimento é, de fato, uma ferramenta poderosa na luta contra cibercrimes.

A pesquisa também revela a eficácia de medidas preventivas simples que podem ser adotadas por todos os usuários da internet. A criação de senhas fortes, a utilização de autenticação multifatorial e a realização de backups regulares são apenas algumas das práticas recomendadas que podem reduzir significativamente o risco de ataques cibernéticos. Além disso, a importância de atualizar regularmente sistemas e softwares não pode ser subestimada. Cada uma dessas medidas contribui para um ambiente digital mais seguro e resiliente.

Outro ponto de destaque é a relevância da educação e treinamento contínuos sobre segurança da informação, tanto em ambientes corporativos quanto acadêmicos. As empresas devem implementar programas de conscientização que não apenas informem seus funcionários sobre as melhores práticas, mas também simulem

ataques para avaliar a capacidade de resposta. Da mesma forma, as instituições educacionais têm o potencial de moldar uma nova geração de usuários mais informados e preparados para lidar com as ameaças digitais.

A colaboração entre diferentes setores é igualmente essencial para o fortalecimento da segurança cibernética. Empresas de tecnologia, governos e instituições educacionais devem unir esforços para criar um ecossistema seguro. Iniciativas conjuntas podem levar à criação de melhores recursos, ferramentas e políticas que protejam não apenas as organizações, mas também os consumidores. A troca de informações sobre vulnerabilidades e ataques recentes pode resultar em respostas mais rápidas e eficazes a novas ameaças.

Além disso, a regulamentação da segurança da informação precisa ser uma prioridade em todas as jurisdições. Leis que exijam que as organizações adotem práticas de segurança adequadas, bem como protejam os dados dos consumidores, são fundamentais para criar um ambiente de confiança. Tais regulamentações não apenas oferecem proteção aos usuários, mas também incentivam as empresas a levarem a segurança a sério, sabendo que estão sujeitas a penalidades em caso de não conformidade.

A pesquisa também ressalta que a responsabilidade pela segurança da informação não deve recair exclusivamente sobre profissionais de TI. Cada usuário tem um papel a desempenhar na proteção de suas informações pessoais. Isso significa que todos devem estar cientes dos riscos e dispostos a adotar as melhores práticas recomendadas. A promoção de uma cultura de segurança digital é, portanto, um esforço coletivo que requer engajamento de todos os usuários da internet.

Uma parte significativa deste estudo é dedicada à análise de incidentes recentes de segurança cibernética, que evidenciam a vulnerabilidade de sistemas e a rapidez com que os ataques podem se espalhar. Esses incidentes não apenas causam danos financeiros, mas também afetam a confiança do público nas instituições e serviços digitais. A natureza pública desses eventos ressalta a necessidade de uma resposta coordenada e eficaz para mitigar os efeitos de tais ataques. MARCIANO E MARQUES (2006), destacam que “o crescimento dos incidentes relacionados à segurança da informação alerta para a premente

necessidade de uma visão fundamentada em bases sólidas para este problema, a qual extrapola em muito o âmbito da tecnologia”.

Além de proteger informações e sistemas, a segurança da informação também desempenha um papel vital na preservação da privacidade dos usuários. Com o aumento do compartilhamento de dados pessoais online, é mais importante do que nunca que os usuários entendam como proteger suas informações. Isso inclui ser cauteloso com o que se compartilha em redes sociais e em outros serviços online, pois dados pessoais podem ser utilizados de forma maliciosa.

A prática da segurança da informação deve ser um processo contínuo, e não uma ação pontual. À medida que as tecnologias evoluem, assim como as táticas dos atacantes, a formação e a adaptação às novas realidades são essenciais. Para isso, a promoção de um diálogo aberto e contínuo sobre segurança cibernética, tanto em ambientes empresariais quanto pessoais, é fundamental.

Deste modo, podemos afirmar que a segurança da informação é um aspecto crítico da sociedade moderna que afeta todos os usuários da internet. A responsabilidade pela proteção de dados não pode ser negligenciada; todos têm um papel a desempenhar na construção de um ambiente digital seguro. Com as estratégias e práticas corretas, é possível não apenas mitigar os riscos, mas também construir uma cultura de segurança que beneficie a todos. A segurança da informação não é apenas uma questão técnica, mas uma questão social que requer a atenção de todos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27001:2013. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos.** Rio de Janeiro: ABNT, 2013. Disponível em: < https://www.abntcatalogo.com.br/>. Acesso dia 20 Out 2024.

BATISTELLA, Carla. **Confidencialidade Integridade e Disponibilidade (CID)**. São Paulo. 2020. Disponível em: < https://www.certifiquei.com.br/confidencialidade-integridade-disponibilidade/>. Acesso em 10 Out 2024.

BRASIL. **ANPD aplica a primeira multa por descumprimento à LGPD**. 2023. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>. Acesso em 20 Out 2024.

BRASIL. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. 2020. Disponível em: < https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf>. Acesso em 01 Out 2024.

CAVALCANTE, Lívia T. Canuto; OLIVEIRA, Adélia Augusto Souto de. **Métodos de revisão bibliográfica nos estudos científicos.** Belo Horizonte. 2020. Disponível em: <https://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682020000100006>. Acesso em 08 Out 2024.

CHIN, Kyle. **19 Most Common Types of Phishing Attacks in 2024**. EUA. Set, 2024. Disponível em < https://www.upguard.com/blog/types-of-phishing-attacks>. Acesso em 01 Out 2024.

CLOUDFLARE. **Como evitar ataques XSS**. EUA. Disponível em: < https://www.cloudflare.com/pt-br/learning/security/how-to-prevent-xss-attacks/ >. Acesso em 18 Out 2024.

CÓDIGO FONTE TV. **XSS Attack (Como Funciona e Como Prevenir Ataques) // Dicionário do Programador**. YouTube, 25 de julho de 2022. 9min27s. Disponível em: < https://www.youtube.com/watch?v=2LYPyUk-L0k&ab >. Acesso em: 03 Out 2024.

COLAÇO, Janize. **Veja quais são os principais ataques cibernéticos que podem roubar o seu dinheiro**. Jul, 2024 Disponível em: < https://einvestidor.estadao.com.br/educacao-financeira/apagao-cibernetico-ataques-hackers-roubar-dinheiro/>. Acesso em 20 Out 2024.

CONCEITO. **Dados - O que é, conceito e definição**. 2019. Disponível em: < https://conceito.de/dados>. Acesso em 20 Out 2024.

CUPRIK, Roman. **Dicas para criar uma política de senhas em uma empresa**. EUA. Mai, 2023. Disponível em: < https://www.welivesecurity.com/br/2023/05/04/dicas-para-criar-uma-politica-de-senhas-em-uma-empresa/ >. Acesso em 15 Out 2024.

DANTAS, Yuri Gil. **Estratégias para tratamento de ataques de negação de serviço na camada de aplicações em redes IP.** João Pessoa. 2015. Dissertação de mestrado.

FERNANDES, Mirian. **BRUTE FORCE: Tudo o que você precisa saber!** São Paulo. Agosto, 2022. Disponível em <https://blog.starti.com.br/brute-force/>. Acesso em 15 Out 2024.

FERREIRA, Vanessa. **Segurança de dados: o que é e como funciona a legislação**. São Paulo. Set, 2022. Disponível em: <https://www.serasa.com.br/premium/blog/seguranca-de-dados-como-funciona-a-legislacao/>. Acesso em 20 Out 2024.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas. Disponível em < https://veja.abril.com.br/coluna/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia#:~:text=Segundo%20especialistas%20em%20seguran%C3%A7a%20cibern%C3%A9tica,os%20dados%20que%20est%C3%A3o%20criptografados. Nov, 2020. Acesso em 24 Set. 2024.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas. Disponível em < https://veja.abril.com.br/mundo/hacker-holandes-diz-ter-invadido-twitter-de-trump-com-senha-facil. Out, 2020. Acesso em Set. 2024.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas. Disponível em < https://veja.abril.com.br/brasil/apos-ataque-hacker-stj-comeca-a-restabelecer-sistemas. Nov, 2020. Acesso em Set. 2024.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas. Disponível em < https://www.cnnbrasil.com.br/internacional/eua-acusam-china-de-realizar-ciberataque-para-roubar-pesquisas-sobre-coronavirus/. Abr, 2020. Acesso em Set. 2024.

Figura 1 - Compilado de notícias recentes sobre diversos ataques hackers em diferentes esferas públicas e privadas. Disponível em < https://www.cnnbrasil.com.br/economia/macroeconomia/depois-de-ataque-hacker-natura-tem-prejuizo-de-r-392-milhoes-no-2-trimestre/#:~:text=Macroeconomia-,Depois%20de%20ataque%20hacker%2C%20Natura%20tem%20preju%C3%ADzo%20de%20R,392%20milh%C3%B5es%20no%202%C2%BA%20trimestre&text=A%20Natura%26Co%20teve%20preju%C3%ADzo%20de,hacker%20sofrido%20pela%20controlada%20Avon. Aug, 2020. Acesso em Set. 2024.

Figura 2 - Incidentes de segurança com repercussão na mídia em 2022. Disponível em < https://www.ibraspd.org/incidentes/. 2022. Acesso em Set. 2024.

Figura 3 - Incidentes de segurança com repercussão na mídia em 2023. Disponível em < https://www.ibraspd.org/incidentes/. 2023. Acesso em Set. 2024.

Figura 4 - Incidentes de segurança com repercussão na mídia em 2023. Disponível em < https://www.ibraspd.org/incidentes/. 2023. Acesso em Set. 2024.

Figura 5 – Pilares de segurança da informação. Abr, 2020 . Disponível em < https://www.security.ufrj.br/dicas/o-que-e-um-incidente-de-seguranca-da-informacao/. Acesso em Set. 2024.

FRUHLINGER, Josh. **What is a cyber attack? Recent examples show disturbing trends.** EUA. Fev., 2018. Disponível em <https://www.csoonline.com/article/563595/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>. Acesso em 16 Out 2024.

HINTZBERGEN, Jule et al. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018. 201p.

HOGLUND, Greg; MCGRAW, Gary. **Como quebrar códigos: a arte de explorar (e proteger) software.** São Paulo: Pearson, 2006. 426p.

HUNT, Andrew; THOMAS, David. **O Programador Pragmático: de aprendiz a mestre**. São Paulo: Bookman, 2010. 348 p.

IBRASPD. **Resiliência Cibernética, Proteção de Dados e Privacidade: Navegando Pelos Impactos dos Ciberincidentes e Fraudes Emergentes.** 2° Congresso Nacional IBRASPD. São Paulo, 2023.

MANOEL, Sergio da Silva. **Governança de segurança da informação: como criar oportunidades para o seu negócio.** 1. ed. Rio de Janeiro: Brasport, 2014. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 02 set. 2024.

MARCHI, Wanderson da Silva. **A Importância do MFA**. Mar., 2024. Disponível em: <https://iamtechday.org/artigos/artigos-tecnicos/a-importancia-do-mfa/>. Acesso em 20 Out 2024.

MARCIANO, João Luiz; MARQUES, Mamede Lima. **O enfoque social da segurança da informação**. Brasília. Dez., 2006. Disponível em <https://www.scielo.br/j/ci/a/L8CqcznptmQK3jyqGqNpWMQ/?lang=pt>. Acesso em: 10 set 2024.

MATHIAS, Viny. **China e Irã ultrapassam limite e usam ChatGPT para criar malware e ataques de phishing; confirma OpenAI**. São Paulo, 2024. Disponível em: <https://br.ign.com/tech/131152/news/china-e-ira-ultrapassam-limite-e-usam-chatgpt-para-criar-malware-e-ataques-de-phishing-confirma-open>. Acesso em 20 out 2024.

MATTHEWS, Ruth. **Senhas fortes: dicas, exemplos e como gerenciá-las**. Panamá. Agosto, 2023. Disponível em < https://nordvpn.com/pt-br/blog/senhas-fortes/>. Acesso em 18 Out 2024.

NAKAMURA, Emilio Tissato. **Segurança da informação e de Redes**. Londrina: Editora e Distribuidora Nacional S.A., 2016. 224p.

NALIN, Carolina. **Brasil é o maior alvo de ataques cibernéticos na América Latina. Veja ranking**. Rio de Janeiro, 2023. Disponível em: <https://oglobo.globo.com/economia/tecnologia/noticia/2023/06/brasil-e-o-maior-alvo-de-ataques-ciberneticos-na-america-latina-veja-ranking.ghtml>. Acesso em 24 set 2024.

OLIVEIRA, Edward. **Ataque DDoS: como proteger a sua infraestrutura empresarial?** Fortaleza. Agosto, 2023**.** Disponível em < https://www.hostweb.com.br/ataque-ddos-como-proteger-a-sua-infraestrutura-empresarial/ >. Acesso em 19 Out 2024.

PAZ, Sarah Martins Ibrahim. **Ciência, Tecnologia e Inovação na Guerra: reflexões para a defesa cibernética brasileira a partir do estudo de casos internacionais.** Rio de Janeiro, 2019. Dissertação (Mestrado).

PRADA, Charles. Ataque cibernético: **O que é e como você pode proteger a sua empresa desse mal**. Blumenau. Mar., 2024. Disponível em: < https://www.euax.com.br/2024/03/ataque-cibernetico/ >. Acesso em 12 Out 2024.

PSAFE. **Drive-by download: um processo que infecta o seu PC com vírus e ameaças**. Out., 2013. Disponível em < https://www.psafe.com/blog/drive-by-download-processo-infecta-seu-pc-virus-ameacas/ >. Acesso em 12 Out 2024.

INSTITUTO PROPAGUE. **O que é phishing?** Disponível em < https://institutopropague.org/tecnologia-e-dados/o-que-e-phishing/>. Acesso em 01 Out 2024.

SANTINO, Renato. **Totvs é vítima de ataque com ransomware; dados podem ter sido roubados**. São Paulo, 2024. Disponível: <https://www.tecmundo.com.br/seguranca/290185-totvs-vitima-ataque-ransomware-dados-ter-sido-roubados.htm>. Acesso em 10 Out 2024.

SILVA, Michel Bernardo F. da. **Cibersegurança: uma visão panorâmica sobre a segurança da informação na Internet.** Rio de Janeiro: Freitas Bastos, 2023. 299p.

SILVESTRE, Caroline. **Como deixar o seu navegador de Internet o mais seguro possível**. 2022. Disponível em: < https://www.techtudo.com.br/listas/2022/09/como-deixar-o-seu-navegador-de-internet-o-mais-seguro-possivel.ghtml >. Acesso em 17 Out 2024.

SOLHA, Liliana E. V. Alegre; TEIXEIRA, Renata C.; PICCOLINI, Jácomo. B. **Tudo que você precisa saber sobre os ataques DDoS**. 2000. Disponível em: < https://memoria.rnp.br/newsgen/0003/ddos.html>. Acesso em 18 Out 2024.

SOUSA, Roberto. **O que é malware, tipos e como se proteger contra ataques de malware.** Disponível em: < https://bravotecnologia.com.br/o-que-e-malware/ >. Acesso em 19 Out 2024.

TECHTUDO. **O que é ransomware? Entenda como funciona e como remover o malware**. 2023. Disponível em: <https://www.techtudo.com.br/guia/2023/05/o-que-e-ransomware-entenda-como-funciona-e-como-remover-o-malware-edsoftwares.ghtml>. Acesso em: 19 Out 2024.

THOMAZ, Raphael. **Gestão estratégica e inteligência na segurança privada**. Curitiba: Editora Intersaberes. 2023. 205p.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. **LGPD nas relações de consumo**. Brasília, 2024. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/o-consumidor-na-internet/lei-geral-de-protecao-de-dados>. Acesso em 19 Out 2024.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). **Incidentes de Segurança da Informação**. Rio de Janeiro, 2020. Disponível em: <https://www.security.ufrj.br/dicas/o-que-e-um-incidente-de-seguranca-da-informacao >. Acesso em: 21 set 2024.