INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA:
DIRETORIA DE DESENVOLVIMENTO E ENSINO
CAMPUS MONTEIRO
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FRANCISCO GABRIEL OLIVEIRA

Ameaças à Segurança em Dispositivos Móveis: Análise de Vulnerabilidades e Estratégias de Proteção de Dados

Monteiro
2024

FRANCISCO GABRIEL OLIVEIRA

Ameaças à Segurança em Dispositivos Móveis: Análise de Vulnerabilidades e Estratégias de Proteção de Dados

Trabalho de Conclusão de Curso (TCC) apresentado ao Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, como pré-requisito para obtenção do Título de Tecnólogo em Análise e Desenvolvimento de Sistemas, sob orientação do Prof. Especialista Wagner de Oliveira Santos

Monteiro

2024

Dados Internacionais de Catalogação na Publicação – CIP
Bibliotecária responsável Porcina Formiga dos Santos Salgado CRB15/204
IFPB Campus Monteiro.

O48a Oliveira, Francisco Gabriel.
Ameaças à segurança em dispositivos móveis: análise de vulnerabilidades e estratégias de proteção de dados / Francisco Gabriel Oliveira – Monteiro-PB. 2024.
46fls. : il.

TCC (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - IFPB campus, Monteiro.

Orientador: Prof. Esp. Wagner de Oliveira Santos.

1. Segurança – dispositivos móveis 2. Ataques cibernéticos 3. Dados - proteção I. Titulo .

CDU 004.056.53

FRANCISCO GABRIEL OLIVEIRA

Ameaças à Segurança em Dispositivos Móveis: Análise de Vulnerabilidades e Estratégias de Proteção de Dados

Trabalho de Conclusão de Curso (TCC) apresentado ao Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Monteiro, como pré-requisito para obtenção do Título de Tecnólogo em Análise e Desenvolvimento de Sistemas, sob orientação do Prof. Especialista Wagner de Oliveira Santos.

Banca Examinadora

Prof. Especialista Wagner de Oliveira Santos
Professor do IFPB (Orientador)

Documento assinado digitalmente
gov.br GILVONALDO ALVES DA SILVA CAVALCANTI
Data: 30/10/2024 17:22:30-0300
Verifique em https://validar.iti.gov.br

Prof .Especialista Gilvonaldo Alves da Silva Cavalcanti
Professor do IFPB (Examinador)

Documento assinado digitalmente
gov.br GILMAR DE JESUS BARROS
Data: 07/11/2024 12:14:30-0300
Verifique em https://validar.iti.gov.br

Prof. Especialista Gilmar de Jesus Barros.
Professor do IFPB (Examinador)

Visto e permitida a impressão.

Monteiro-PB, 16 de outubro de 2024.

Documento assinado digitalmente
gov.br GILDO FERRUCIO SANTOS MAIA DANTAS
Data: 06/11/2024 14:07:05-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Gildo Ferrucio Santos Maia Dantas
Coordenador do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

AGRADECIMENTOS

Em primeiro lugar, gostaria de expressar minha gratidão às ideias que, por vezes, surgem de maneira inusitada e que, sem dúvida, tornaram este trabalho de conclusão de curso mais interessante e menos monótono.

Agradeço, de maneira especial, ao Prof. Diego Breno, que não apenas acreditou em meu potencial, mas também me ofereceu a oportunidade de demonstrar que sou capaz de realizar um trabalho de qualidade. Seu apoio foi fundamental, e sua paciência, admirável.

À minha mãe, Maria de Fátima Socorro, meu eterno agradecimento por todo o amor, incentivo e apoio incondicional. Sua presença em minha vida tem sido essencial, e sou grato por sua fé em mim, mesmo nos momentos em que eu duvidei de mim mesmo.

Agradeço também à minha família e amigos, que acreditaram na minha capacidade de concluir este curso, mesmo quando minhas ações pareciam indicar o contrário. Agradeço pela confiança e pelo apoio constante durante toda a minha jornada acadêmica.

Por fim, expresso minha gratidão a todos que, direta ou indiretamente, contribuíram para este momento, seja com conselhos valiosos, palavras de encorajamento ou um gesto de amizade.

"No momento em que você acha que deve desistir, é o momento em que você deve continuar lutando."— Shinji Ikari, Neon Genesis Evangelion

RESUMO

A explosão no uso de dispositivos móveis como *smartphone*s e tablets tem colocado em destaque a urgente necessidade de priorizar a segurança em dispositivos móveis. Estes aparelhos, que armazenam uma gama vasta de dados sensíveis, desde informações bancárias a fotos pessoais e senhas, são alvos irresistíveis para hackers e cibercriminosos. Este Trabalho de Conclusão de Curso tem como objetivo investigar as diversas ameaças à segurança que comprometem os dispositivos móveis, abrangendo desde malware e phishing até ataques de ransomware, força bruta e engenharia social. Cada uma dessas formas de ataques é dissecada, revelando suas peculiaridades, métodos de operação e os potenciais danos que podem causar. Com o intuito de salvaguardar os dados contra esses ataques inclementes, este estudo propõe uma série de estratégias eficazes. A implementação de autenticação multifatorial, a aplicação de criptografia robusta nos dados e o emprego de soluções de segurança confiáveis emergem como medidas cruciais para assegurar a integridade dos dispositivos e dos dados neles contidos. Além disso, o trabalho ressalta a importância crucial da conscientização do usuário na batalha contra os ataques cibernéticos. Educar os usuários sobre as ameaças à segurança digital e instruí-los sobre as melhores práticas para proteger seus dados não apenas reduz os riscos de violações, mas também fortalece a linha de defesa contra futuros ataques.

Palavras-chave: segurança em dispositivos móveis; ameaças de segurança; proteção de aplicativos; dados; ataques cibernéticos; estratégias de proteção.

ABSTRACT

The explosion in the use of mobile devices such as smartphones and tablets has highlighted the urgent need to prioritize security in these devices. These gadgets, which store a vast range of sensitive data—from banking information to personal photos and passwords—are irresistible targets for hackers and cybercriminals. This thesis aims to investigate the multiple security threats that plague mobile devices, encompassing everything from malware and phishing to ransomware attacks, brute force, and social engineering. Each of these attack methods is dissected, revealing their particularities, modes of operation, and potential damage they can cause. In order to safeguard data against these relentless attacks, this study proposes a series of effective strategies. Implementing multifactor authentication, applying strong data encryption, and employing reliable security solutions emerge as crucial measures to ensure the integrity of both the devices and the data they contain. Additionally, the study emphasizes the critical importance of user awareness in the fight against cyberattacks. Educating users about digital security threats and instructing them on best practices for protecting their data not only reduces the risk of breaches but also strengthens the defense against future attacks.

Keywords: mobile device security; security threats; application protection; data; cyber attacks; protection strategies.

LISTAS DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

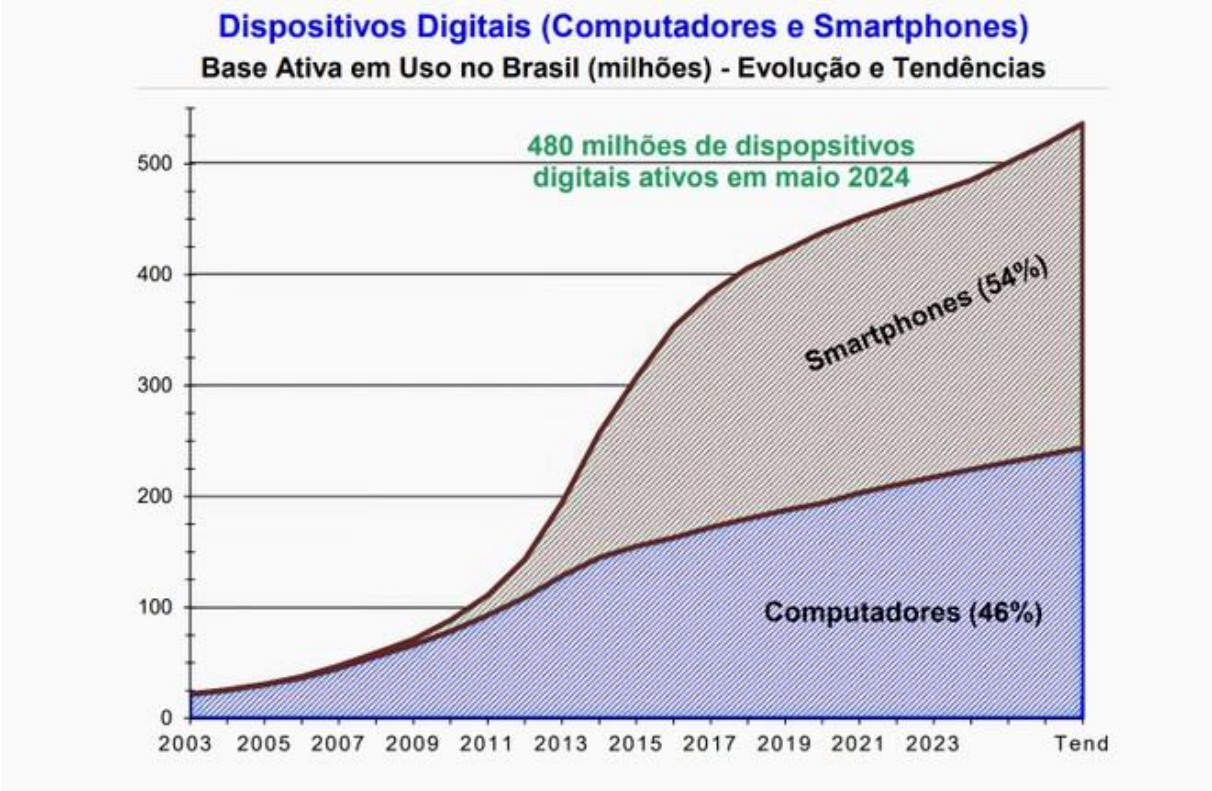
ABNT	Associação Brasileira de Normas Técnicas
AES	Advanced Encryption Standard (Padrão Avançado de Criptografia)
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes do Brasil
DES	Data Encryption Standard (Padrão de Criptografia de Dados)
EAESP	Escola de Administração de Empresas de São Paulo
FGV	Fundação Getúlio Vargas
IDS	Intrusion Detection System (Sistema de Detecção de Intrusões)
IFPB	Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
LGPD	Lei Geral de Proteção de Dados
MitM	Man-in-the-Middle
OWASP	Open Web Application Security Project
SDLC	Security Development LifeCycle
SMS	Short Message Service (serviço de mensagens curtas)
SPN	Smart Protection Network (Rede de Proteção Inteligente)
VPN	Virtual Private Network (Rede Privada Virtual)

SUMÁRIO

1 INTRODUÇÃO

A explosão do uso de dispositivos móveis, como *smartphone*s e tablets, tem tornado cada vez mais evidente que a prioridade da segurança desses dispositivos é uma questão de urgência.

Figura 1: Dispositivos Digitais Base Ativa em Uso no Brasil (milhões)



Fonte: FGV (2024)

O gráfico acima exibe dados de uma pesquisa realizada pela FGV, que aponta o crescimento do uso de *smartphones* no Brasil em comparação com computadores ao longo dos anos. Essa pesquisa integra o Fórum Permanente de Informações sobre o Uso de TI nas Empresas, com o objetivo de analisar a realidade tecnológica das organizações brasileiras. Os resultados obtidos são apresentados nos cursos de Tecnologia da Informação da FGV/EAESP, fornecendo *insights* sobre a evolução do uso de tecnologias nas empresas nacionais.

A segurança da informação é um tema recorrente na área da computação, especialmente à medida que a tecnologia avança e os invasores desenvolvem técnicas cada vez mais sofisticadas para acessar dados pessoais (Tomaél e De Jesus, 2010). Dessa forma, a proteção de dados é uma prioridade constante no cenário digital atual.

Figura 2:Primeiro modelo de dispositivo móvel Motorola DynaTAC 8000X

Fonte: WIKIPEDIA

A ideia de criar um aparelho que permitisse a comunicação em diferentes locais surgiu em 1947, mas enfrentou grandes dificuldades devido às limitações tecnológicas da época, resultando na sua transformação em um conceito sem continuidade (Nicolai *et al.* 2012). Foi apenas em 1973 que ocorreu a primeira experiência de ligação entre um dispositivo móvel e um telefone fixo, utilizando teorias desenvolvidas em 1947 (Morimoto 2009). A Motorola se destacou ao fabricar os primeiros modelos comerciais, lançando em 1983 o DynaTAC 8000x. No entanto, seu alto custo impediu o sucesso inicial entre os consumidores.

Com o tempo, o conceito de mobilidade rapidamente cresceu significativamente, permitindo que os dispositivos não só facilitassem a comunicação em diversos locais, mas também se tornassem mais agradáveis e versáteis. Isso exigiu melhorias no *hardware* e *software*, resultando em funcionalidades como armazenamento de contatos, calculadoras, identificação de chamadas, troca de

mensagens de texto, e, posteriormente, a introdução de telas coloridas, câmeras fotográficas, e reprodução de músicas. Essa evolução culminou na criação dos *smartphones*, dispositivos capazes de executar tarefas complexas, instalar e desinstalar aplicativos, e até mesmo superar o desempenho de alguns computadores (Morimoto 2009).

O termo mobilidade agora abrange aparelhos que podem ser facilmente transportados e operados em movimento, com características como tamanho reduzido, baixo consumo de energia, processamento de dados eficiente, e monitoramento do nível de energia para prevenir a perda de dados (Morimoto 2009) Além disso, para ser considerado móvel, um dispositivo deve realizar tarefas através de texto, áudio, vídeo e internet, ter características pessoais, receber informações constantemente, ser levado a qualquer lugar, ter canais de pagamento integrados, e estar presente nos momentos de impulso criativo (Fling 2009).

A portabilidade proporcionada pelos dispositivos móveis trouxe maior praticidade aos usuários, mas também resultou em diversas vulnerabilidades. Em 2023, o Brasil registrou 1,8 milhões de bloqueios de ataques em celulares, representando um aumento significativo nas tentativas de invasão, com 3,9 milhões de ataques em toda a América Latina no primeiro semestre de 2024 (Security Leaders, 2024).

O termo "segurança" refere-se à minimização da vulnerabilidade de bens e recursos (Barros, 2023). A comunidade tecnológica busca continuamente aprimorar a proteção das informações pessoais, antecipando possíveis falhas. Com o aumento do uso de dispositivos móveis, empresas de diversos setores, incluindo bancos, investem em aplicativos voltados para vendas e serviços especializados. Um exemplo é a realização de transações bancárias via *smartphone*, que, apesar das medidas de segurança, está sujeita a ataques que podem comprometer o usuário.

A transmissão de informações em redes sem fio possui sistemas de segurança, os protocolos de segurança de redes sem fio, visam proteger a integridade dos dados transmitidos, mas vulnerabilidades em seus sistemas podem ser exploradas por invasores, comprometendo tanto a segurança lógica quanto física dos dispositivos conectados (Moraes, 2010).

Diante disso esse estudo tem como questão norteadora investigar as principais vulnerabilidades que afetam a segurança dos dispositivos móveis. Quais são as brechas exploradas por invasores e quais métodos podem ser implementados para

mitigá-las de forma eficaz? Compreender essas questões não apenas permitirá uma proteção mais robusta dos dados sensíveis, mas também estimulará a conscientização dos usuários sobre práticas seguras, fundamental na batalha contra as ameaças digitais que permeiam nosso cotidiano.

Assim, organizamos o texto de acordo com a seguinte sequência de capítulos: no capítulo 1, exploramos as principais ameaças à segurança que afetam dispositivos móveis, incluindo *malware, phishing, ransomware*, ataques de força bruta e engenharia social. São discutidos os métodos de operação desses ataques e os potenciais danos que podem causar aos usuários.

No capítulo 2, são analisadas de forma crítica as diversas legislações brasileiras que abordam crimes cibernéticos, como a LGPD, a Lei Carolina Dieckmann, e o Marco Civil da Internet, além de uma visão sobre leis internacionais. O capítulo foca nas implicações dessas leis para a proteção contra crimes digitais e a relevância dessas normativas no contexto atual.

No capítulo 3, são apresentadas estratégias eficazes para a proteção de dispositivos móveis, como autenticação multifatorial, criptografia de dados e o uso de soluções de segurança confiáveis. Além disso, destaca-se a importância da conscientização dos usuários como parte essencial na defesa contra ataques cibernéticos.

E, por fim, o capítulo final sintetiza os principais achados da pesquisa, refletindo sobre as práticas de segurança discutidas e sugerindo possíveis áreas para estudos futuros, visando aprimorar as defesas contra ameaças em dispositivos móveis.

Em última análise, a segurança em dispositivos móveis é uma questão multidimensional que requer uma abordagem holística e colaborativa. Somente através da compreensão das ameaças, da implementação de medidas técnicas adequadas e do envolvimento ativo dos usuários podemos garantir um ambiente digital mais seguro e resiliente para todos.

A metodologia adotada neste trabalho combina pesquisa bibliográfica, explicativa e aplicada, conforme as orientações de Antônio Carlos Gil (2022) em seu livro "Como Elaborar Projetos de Pesquisa". A pesquisa explicativa tem como objetivo compreender as causas e efeitos de fenômenos, buscando explicar como diferentes ameaças cibernéticas afetam a segurança de dispositivos móveis. Além disso, a pesquisa aplicada foca na resolução de problemas práticos, propondo estratégias como autenticação multifatorial e criptografia robusta para mitigar esses riscos.

A pesquisa bibliográfica, baseada em materiais já publicados, como livros, artigos científicos e legislações, é usada para construir o referencial teórico, permitindo uma análise das lacunas no conhecimento existente sobre o tema. Dessa forma, o estudo une teoria e prática, proporcionando uma compreensão profunda das ameaças à segurança em dispositivos móveis e propondo soluções práticas para proteger os usuários e sistemas.

1.1 Justificativa

A segurança em dispositivos móveis é um tema de extrema relevância no contexto atual, considerando o crescente uso desses dispositivos para atividades pessoais e profissionais. Com o aumento das transações financeiras, comunicação e armazenamento de dados sensíveis via smartphones, a proteção contra ameaças cibernéticas torna-se uma prioridade. Este cenário ressalta a importância de estudar e desenvolver soluções que mitiguem os riscos associados a essas vulnerabilidades.

Acadêmicos e profissionais da área de segurança da informação enfrentam o desafio de criar tecnologias mais robustas e seguras, especialmente com a intensificação de legislações como a LGPD, que exige maior proteção de dados. Este trabalho busca contribuir com a compreensão das ameaças emergentes e sugerir práticas e ferramentas eficazes para proteger dispositivos e redes contra ataques.

Assim, o estudo se justifica pela necessidade de ampliar o conhecimento e a conscientização sobre a segurança móvel, oferecendo diretrizes tanto para a área acadêmica quanto para o mercado profissional. Ao investigar vulnerabilidades e soluções de segurança, o trabalho visa auxiliar empresas e usuários a protegerem suas informações e privacidade no ambiente digital.

1.2 Objetivos

O presente trabalho tem como objetivo geral analisar as principais ameaças à segurança de dispositivos móveis e propor estratégias para a proteção de dados e aplicativos. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos:

I. Identificar as principais vulnerabilidades presentes em dispositivos móveis, com foco nos sistemas operacionais Android e iOS.
II. Analisar os diferentes tipos de ataques que têm como alvo esses dispositivos, incluindo malware, ataques de phishing e exploração de vulnerabilidades de rede.

III. Avaliar as medidas de segurança atuais implementadas pelos fabricantes de dispositivos e desenvolvedores de software.
IV. Propor estratégias práticas para a mitigação de riscos, incluindo o uso de criptografia, autenticação multifator e conscientização do usuário.
V. Investigar o impacto das legislações de proteção de dados, como a LGPD, na segurança de dispositivos móveis, tanto no contexto empresarial quanto pessoal.

Esses objetivos são alinhados com a necessidade de promover um ambiente digital mais seguro, ao mesmo tempo que contribuempara o avanço do conhecimento acadêmico na área de segurança da informação.

2 DESAFIOS E RISCOS À SEGURANÇA EM DISPOSITIVOS MÓVEIS: UMA ANÁLISE DAS AMEAÇAS NO CONTEXTO DIGITAL ATUAL

No mundo atual, os dispositivos móveis se tornaram uma parte essencial de nossas vidas, armazenando informações confidenciais, dados bancários e até mesmo controlando aspectos cruciais da nossa rotina. No entanto, essa conveniência está associada a diversos riscos, representados pelas múltiplas ameaças à segurança que comprometem esses dispositivos e, consequentemente, seus usuários.

2.1 Uma Panorâmica das Ameaças

2.1.1 Malware

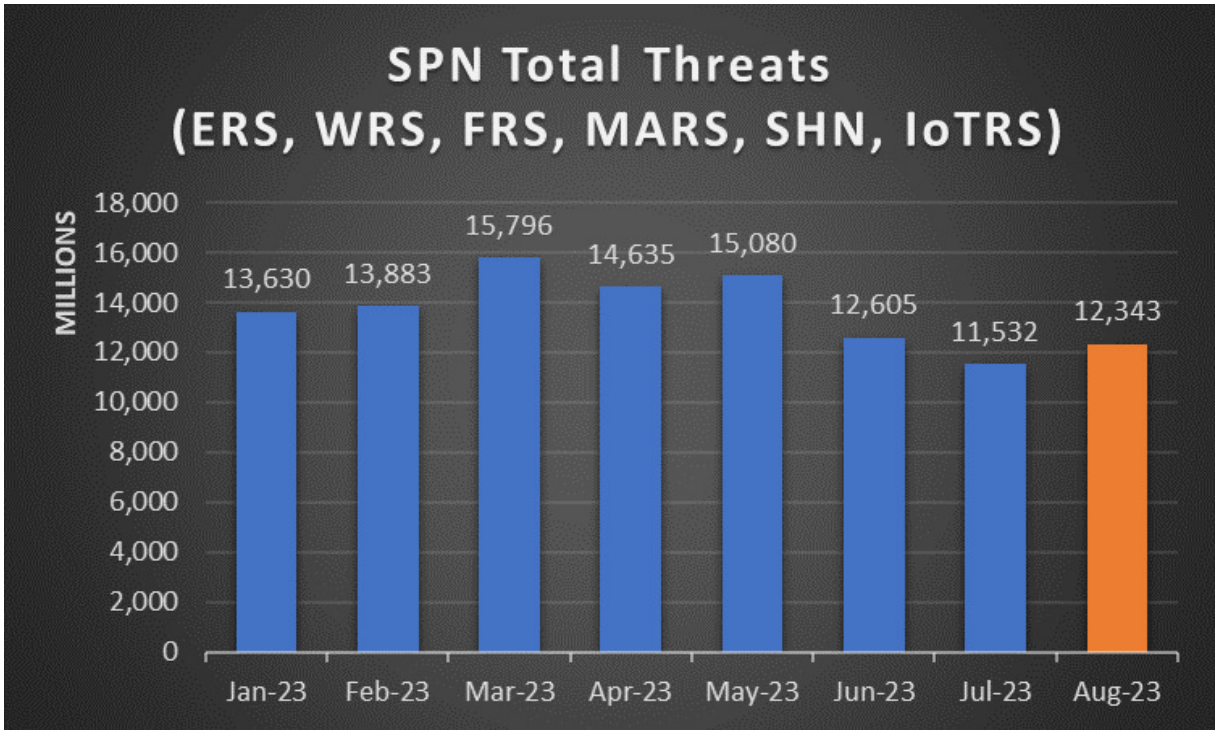
De acordo com Stallings (2020), os dispositivos móveis são alvos frequentes de diversos tipos de malware, incluindo vírus, *worms*, cavalos de Troia, *spyware* e *ransomware*. Esses programas maliciosos podem comprometer a segurança do dispositivo, danificar arquivos, roubar informações confidenciais ou até mesmo exigir resgates para liberar dados criptografados.

- Vírus: Programas que se replicam automaticamente e podem corromper arquivos ou comprometer o sistema, muitas vezes através de redes ou arquivos compartilhados (Stallings, 2020).
- Worms: Similar ao vírus, exploram falhas de segurança para se propagar de um dispositivo para outro, geralmente através da rede (Stallings, 2020).
- Cavalo de Tróia(Trojans): Se disfarçam como programas legítimos para enganar o usuário a instalá-los, liberando posteriormente o malware real (Stallings, 2020).
- Spyware: Monitora as atividades do usuário sem seu conhecimento ou consentimento, coletando informações confidenciais como senhas e dados bancários (Stallings, 2020).
- Ransomware: Criptografa os arquivos do dispositivo e exige o pagamento de um resgate para liberá-los (Stallings, 2020).

Conforme destacado no relatório "*Fast Facts*" de agosto de 2023 da Trend micro, as ameaças aos dispositivos móveis continuam a crescer em complexidade e número. Entre os tipos de malware mais preocupantes, estão os *ransomwares*, que atingiram um pico significativo no último ano, com um ligeiro aumento de 42% em ataques que tem sido direcionado a *smartphone*s e *tablets* (Trend micro, 2023).

Este crescimento se deve em parte à sofisticação das técnicas empregadas pelos criminosos, que utilizam engenharia social e explorações avançadas para enganar usuários desavisados. Além disso, o relatório revela uma preocupante expansão dos *malwares* de espionagem, ou *spywares*, que estão sendo cada vez mais utilizados para monitorar as atividades dos usuários, com um aumento de 37% nas detecções em comparação ao ano anterior (Trend micro, 2023). Esses números refletem um cenário em que a segurança digital não pode ser negligenciada, exigindo ações imediatas tanto por parte dos desenvolvedores de *software* quanto dos usuários.

Figura 3 - ameaças detectadas pela rede de proteção da Trend micro



Fonte: trendmicro (2023)

O gráfico mostra a quantidade de ameaças detectadas pela rede de proteção da Trend micro (SPN) entre janeiro e agosto de 2023. A SPN é um sistema que monitora a internet em busca de atividades maliciosas, como vírus, *worms* e *ransomware*. Além das ameaças diretas, o relatório destaca a crescente preocupação com a segurança das redes móveis, que se tornam alvos frequentes de ataques como *Man-in-the-Middle* (MitM). Esses ataques permitem que invasores interceptem comunicações entre o usuário e o servidor, potencialmente roubando dados sensíveis ou distribuindo malware. A segurança dos dispositivos móveis, portanto, não é apenas uma questão de proteger o aparelho em si, mas também de garantir que as conexões

e interações digitais sejam seguras. As estatísticas recentes mostram que 55% dos ataques a dispositivos móveis em 2023 envolveram algum tipo de comprometimento de rede (Trend micro, 2023), sublinhando a necessidade de soluções de segurança robustas e atualizadas para proteger os usuários nesse ambiente digital cada vez mais perigoso.

2.1.2 Phishing

Segundo Laudon (2022), o *phishing* é uma técnica que teve origem de engenharia social utilizada para enganar usuários e obter informações confidenciais, como senhas ou dados bancários, por meio de sites ou mensagens fraudulentas que imitam serviços legítimos. O *phishing* pode se manifestar de diversas formas, como o *smishing*, que envolve o envio de mensagens de texto fraudulentas, e o *pishing*, que utiliza chamadas telefônicas fraudulentas para obter informações sensíveis.

- SMS Phishing (Smishing): Mensagens de texto fraudulentas que aparentam vir de fontes confiáveis podendo ser pessoas próximas ou alguém conhecido, tentando convencer os usuários a clicar em links maliciosos ou fornecer informações pessoais (Laudon, 2022).
- Voice Phishing (Vishing): Chamadas telefônicas fraudulentas que tentam enganar os usuários para que forneçam informações sensíveis (Laudon, 2022).

1.1.3 Ataques de Força Bruta

De acordo com Lima (2021), o uso de ferramentas automatizadas para adivinhar senhas, conhecido como ataque de força bruta, envolve a tentativa repetida de diversas combinações de credenciais até encontrar a correta. Para mitigar esse tipo de ameaça, é essencial implementar políticas de senhas fortes, autenticação multifator e limitação do número de tentativas de login. Como podemos ver abaixo:

- Ferramentas Comuns: Programas automatizados que tentam rapidamente inúmeras combinações de senhas (Lima 2021).
- Prevenção: Inclui a implementação de políticas de senhas fortes, autenticação multifator e limitação de tentativas de *login* (Lima 2021).

2.1.4 Engenharia Social

A manipulação psicológica, também conhecida como engenharia social, envolve táticas como o pretexto fingir ser uma pessoa de confiança, *phishing* e *baiting*

oferecer algo atrativo para enganar a vítima (Business Tech Weekly, 2023). Essas técnicas visam induzir o usuário a divulgar informações confidenciais ou realizar ações que comprometam a segurança do sistema. Para prevenir esses ataques, é essencial realizar treinamentos regulares, promover a conscientização sobre segurança e implementar procedimentos de verificação adequados (Amorim 2023).

2.2 O Impacto das Ameaças:

Conforme Oliveira (2022), os impactos de ciberataques podem ser devastadores, afetando tanto indivíduos quanto organizações, com a perda de dados confidenciais, danos financeiros e à reputação, além de queda de produtividade sendo os principais prejuízos relatados. Estes são os principais impactos citados por Oliveira:

QUADRO 1 : Principais impactos citados por Oliveira

○ IMPACTOS	○ DESCRIÇÃO
Perda de dados confidenciais	Informações pessoais, senhas, dados bancários e até mesmo propriedade intelectual podem ser roubados e utilizados para fins maliciosos.
Danos financeiros	Ataques de *ransomware* podem levar à perda de acesso a arquivos importantes, causando prejuízos financeiros consideráveis
Danos à reputação	Vazamentos de dados e ataques cibernéticos podem manchar a reputação de empresas e indivíduos, afetando negativamente seus negócios e relacionamentos.
Perda de produtividade	Dispositivos infectados com malware podem se tornar lentos ou inoperantes, impactando diretamente na produtividade do usuário.

FONTE: Oliveira (2022).

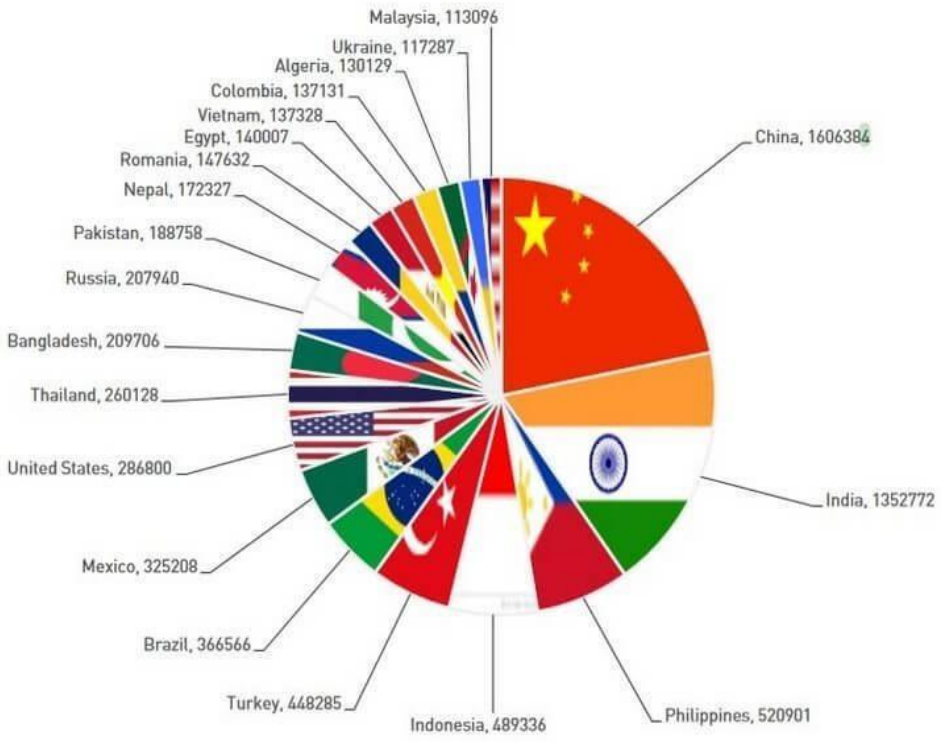
2.2.1 Mitigação de Ameaças

Conforme Gonzalez (2021), para mitigar ameaças no desenvolvimento de software, é fundamental que as empresas adotem práticas de segurança em todo o ciclo de vida do desenvolvimento (SDLC), incluindo testes de segurança contínuos e revisão de código. Além disso, políticas robustas de segurança da informação, associadas ao treinamento de funcionários e à implementação de tecnologias como criptografia e firewalls, são essenciais para garantir a proteção contra ameaças cibernéticas.

2.3 HummingBad: O Maior Ataque de Malware a Dispositivos Móveis

Entre os ataques mais devastadores na história da segurança móvel, destaca-se o *HummingBad*, um *malware* que afetou milhões de dispositivos Android em 2016. Desenvolvido por um grupo de cibercriminosos chamado Yingmob, o *HummingBad* foi projetado para ganhar controle *root* sobre os dispositivos infectados, permitindo que ele instalasse *softwares* maliciosos adicionais, gerasse cliques fraudulentos em anúncios e espionasse dados dos usuários (Kaspersky, 2017).

Figura 4: Apresenta os vinte países mais afetados pelo HummingBad



Fonte: SHOWMETECH (2016)

O principal objetivo do *HummingBad* era gerar receitas por meio de cliques fraudulentos em anúncios. Estima-se que o grupo responsável pelo ataque lucrava cerca de 300 mil *dólares* por mês, tornando-se um esquema altamente lucrativo e de grande escala. Além disso, o *malware* possibilitava a coleta de dados sensíveis dos usuários, ampliando os riscos de privacidade e segurança.

O impacto do *HummingBad* foi global e expôs milhões de dispositivos à invasão, afetando a privacidade e a segurança de seus usuários. Esse ataque destacou as fragilidades do ecossistema *Android*, particularmente no que diz respeito

ao uso de aplicativos de lojas de terceiros, e evidenciou a crescente sofisticação das técnicas empregadas por cibercriminosos em dispositivos móveis (Kaspersky, 2017).

Diante do que foi exposto, consideramos que as ameaças à segurança em dispositivos móveis são diversas e em constante evolução, exigindo vigilância contínua e práticas de segurança abrangentes. Este capítulo serviu como um guia introdutório ao tema, explorando as principais categorias de ameaças e seus impactos devastadores.

3 LEGISLAÇÃO E CIBERCRIMES: UM ESTUDO DAS NORMAS BRASILEIRAS

Embora a internet tenha proporcionado uma maior conexão global, também introduziu desafios significativos. A cada dia, ouvimos falar de vazamentos de dados, ataques a sistemas e crimes virtuais que afetam milhões de pessoas.

A história dos crimes cibernéticos remonta à década de 1960, quando surgiram as primeiras menções sobre o tema. Nesse período, foram observados delitos como a alteração, cópia e sabotagem de sistemas computacionais, que passaram a ser estudados pela doutrina internacional como os primeiros indícios de crimes virtuais, conforme descrito por diversos autores na literatura especializada (Jesus, 2016). Desde os primórdios da computação, pessoas mal-intencionadas já exploravam as vulnerabilidades dos sistemas. Hoje, essa ameaça se tornou global e exige respostas eficazes.

> Na década de 70 a figura do Hacker já era citada com o advento de crimes como invasão de sistema e furto de *software*, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso à necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo. (Souza,2015, p. 45)

Em 2001, o Conselho da Europa elaborou a Convenção de Budapeste sobre Crimes Cibernéticos, com o objetivo de uniformizar a legislação europeia e estabelecer um padrão internacional para a cooperação em crimes digitais. Embora não seja uma legislação interna, essa convenção desempenhou um papel crucial na harmonização das leis sobre crimes cibernéticos, servindo como referência para a legislação nacional e promovendo a colaboração internacional (Convenção sobre Cibercrime, 2001).

No Brasil, a legislação voltada para a proteção de dados e a segurança no ambiente digital é composta por um conjunto de normas que buscam mitigar os riscos associados aos crimes cibernéticos. Entre as principais regulamentações destacam-se a Lei Geral de Proteção de Dados (LGPD), a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e o Marco Civil da Internet (Lei nº 12.965/2014). No entanto, questiona-se se essas normas são suficientemente robustas para enfrentar os desafios impostos pelo mundo conectado, onde as ameaças são cada vez mais sofisticadas e transnacionais.

Diante disso, este capítulo propõe uma análise crítica dessas legislações, a fim de avaliar sua eficácia e identificar possíveis lacunas. O objetivo é compreender como o Brasil pode aprimorar suas estratégias de defesa cibernética e contribuir para a construção de um futuro digital mais seguro para todos.

3.1 Lei azeredo

A Lei Azeredo, nome popular dado ao Projeto de Lei 2.126/2011, propôs diretrizes para a segurança na internet no Brasil, tendo sido apresentada pelo deputado federal Eduardo Azeredo. Inicialmente, o projeto tinha como objetivo combater crimes digitais como fraudes bancárias, pornografia infantil e invasão de sistemas (Brasil, 2011). No entanto, ao longo de sua tramitação, a proposta recebeu diversas críticas de especialistas em direito digital, defensores dos direitos humanos e a sociedade civil, que apontaram possíveis violações à privacidade e à liberdade de expressão.

Uma das críticas mais significativas foi a exigência de que provedores de serviços de internet armazenassem os dados dos usuários por longos períodos, o que poderia comprometer a privacidade e facilitar o acesso indevido a informações pessoais. Outra preocupação central era a falta de clareza nos critérios para o bloqueio de sites, o que poderia levar a abusos.

Diante das intensas críticas, o Projeto de Lei 2.126/2011 foi arquivado em 2018. Embora o Brasil ainda careça de uma legislação específica para crimes cibernéticos, aspectos relacionados à segurança digital e delitos online foram incorporados em outras legislações, como o Código Penal e o Marco Civil da Internet (Paganotti, 2014, p. 143-160).

Apesar da Lei 12.735 de 2012, conhecida também como Lei Azeredo, ter sido sancionada com a intenção de coibir crimes cibernéticos, poucos estados criaram delegacias ou setores especializados para essa finalidade. Na maioria das unidades federativas, faltam tanto a expertise necessária quanto estruturas físicas e pessoal capacitado para lidar com essas questões. A criação de delegacias especializadas tende a concentrar as ocorrências em um único local, mas o direcionamento dos casos pode ocorrer de forma inadequada, sem a devida compreensão dos fatos.

3.2 Lei Carolina Dieckmann (Lei 12.737/12)

A Lei Carolina Dieckmann criminaliza a invasão de dispositivos eletrônicos e a obtenção, divulgação ou comercialização não autorizada de dados pessoais.

Popularmente conhecida como "Lei Carolina Dieckmann", a legislação foi impulsionada após o caso em que fotos íntimas da atriz Carolina Dieckmann foram ilegalmente obtidas e divulgadas na internet sem seu consentimento. Embora o nome popular da lei tenha surgido devido a esse incidente, ela foi desenvolvida como uma resposta à crescente onda de crimes cibernéticos no Brasil. O caso da atriz evidenciou a urgência de uma legislação mais severa para proteger os cidadãos no mundo digital.

A lei traz o acréscimo de dois artigos ao Código Penal, os artigos 154-A e o 154-B. o artigo 154-A definido que:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012).

A Lei Carolina Dieckmann, ao tipificar a invasão de dispositivos eletrônicos, como *smartphone*s, trouxe para o ordenamento jurídico brasileiro uma proteção que antes não existia. Antes dessa legislação, não havia normas específicas para criminalizar tais atos, o que deixava um vazio significativa na proteção dos direitos dos indivíduos no ambiente digital.

A lei também complementou o Código Penal ao incluir dispositivos informáticos nos crimes de interrupção de serviços, e reconheceu cartões de crédito como documentos particulares, ampliando o alcance da punição para falsificadores. Essas mudanças demonstram um grande esforço na modernização das normas jurídicas para acompanhar os avanços tecnológicos.

No entanto, apesar desses avanços, a legislação ainda está longe de atender as necessidades impostas pelos desenvolvimentos tecnológicos. As penas estabelecidas, embora um progresso, ainda são consideradas brandas diante dos danos irreparáveis causados às vítimas, como a perda de privacidade e a exposição indevida de dados pessoais.

Além disso, o processo para responsabilizar os criminosos ainda é burocrático, exigindo a representação da vítima para que a ação penal tenha início, o que pode ser um obstáculo para à justiça. A ineficácia em lidar de forma mais rigorosa com essas infrações contribui para um sentimento de impunidade.

Portanto, embora a Lei Carolina Dieckmann tenha sido um passo crucial na proteção contra crimes cibernéticos, é evidente que há necessidade de reformas

adicionais para fortalecer a resposta legal às ameaças digitais, garantindo maior proteção às vítimas e mais rigor na punição dos culpados.

3.3 Lei do marco civil da internet

O Marco Civil da Internet, surgido em 2009, foi uma resposta à crescente necessidade de regulamentar o uso da internet no Brasil, estabelecendo princípios, direitos e deveres para garantir uma navegação mais segura e democrática. Complementando a Lei Carolina Dieckmann, o Marco Civil reforça a proteção à privacidade e à liberdade de expressão, ao mesmo tempo em que é definida a neutralidade da rede e a responsabilidade dos provedores. Juntas, essas legislações formam a base para a regulação do ambiente digital no país, abordando tanto a proteção dos direitos dos usuários quanto o combate aos crimes cibernéticos.

Embora o Marco Civil da Internet tenha começado a ser desenvolvido em 2009, ele foi oficialmente sancionado como a Lei nº 12.965 em 23 de abril de 2014. Essa lei estabelece as diretrizes para o uso da internet em todo o território nacional, garantindo direitos e definindo deveres para acompanhar a evolução tecnológica. Nos artigos 1º e 3º, a lei destaca os princípios e garantias fundamentais que regem o uso da internet no Brasil:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (BRASIL, 2014) Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - Proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - Preservação e garantia da neutralidade de rede; V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (Brasil, 2014)

De acordo com Teixeira (2016), preocupado com a possibilidade de haver limitações à liberdade de expressão ou violações à privacidade dos usuários, o Marco Civil estabelece que a garantia desses direitos constitucionais é essencial para o pleno exercício do acesso à internet. A violação desses direitos compromete a própria finalidade do Marco Civil como uma lei federal que visa proteger os usuários da rede.

Com a introdução do Marco Civil da Internet, o Brasil se tornou um dos poucos países a adotar a neutralidade da rede como uma norma legal. Esta regra garante que os usuários não sofram redução na velocidade de conexão por razões econômicas, como acontece quando empresas limitam o acesso a serviços de voz sobre IP, como o Skype, ou reduzem a banda de produtos concorrentes. A neutralidade da rede é, portanto, a norma geral, e qualquer provedor que discrimine o tráfego precisa justificar essa prática. O artigo 11 da Lei nº 12.965/2014 (Marco Civil da Internet) estabelece algumas exceções à coleta de dados pessoais, sendo que os critérios técnicos para essas exceções devem ser definidos por decreto presidencial:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...] § 4o Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (Brasil, 2014)

Essas disposições são essenciais para a criação de um ambiente digital mais seguro e equitativo, onde os direitos dos usuários são protegidos e as práticas de discriminação ou abuso por parte dos provedores de internet são reguladas. Apesar dos avanços significativos trazidos pelo Marco Civil, a contínua adaptação e regulamentação são necessárias para lidar com as novas demandas e desafios impostos pela rápida evolução da tecnologia e do cenário digital.

3.4 Lei geral de proteção de dados pessoais (LGPD)

No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, publicada em 15 de agosto de 2018, foi criada com o objetivo de aprimorar a governança de dados pessoais, aplicando-se tanto a instituições públicas quanto privadas, incluindo universidades e outras instituições de ensino. Segundo Castro (2021) e Lima (2022), a LGPD é fundamental para assegurar que essas instituições sigam regras rigorosas no tratamento de dados pessoais, especialmente no que se refere a dados sensíveis. De acordo com a LGPD, as universidades e faculdades devem seguir diretrizes específicas para o tratamento de dados pessoais, em conformidade com os artigos 7º e 11, que limitam o uso desses dados ao anonimato garantido, especialmente em pesquisas conduzidas por órgãos responsáveis pela segurança da informação, sendo proibida a transferência para terceiros (Castro, 2021).

O artigo 16º da LGPD reforça que esses dados devem ser preservados por instituições de pesquisa, desde que a anonimização seja garantida sempre que possível, promovendo a segurança e a privacidade dos titulares dos dados.

A LGPD se destaca por oferecer ao titular o controle sobre como seus dados são coletados e utilizados, sendo este princípio conhecido como "autodeterminação informativa". Lima (2022) aponta que essa abordagem garante que as pessoas tenham o poder de decidir sobre a manipulação de seus próprios dados, tornando a LGPD uma das leis mais abrangentes nesse sentido, aplicável não apenas em território brasileiro, mas a qualquer operação de tratamento de dados que envolva indivíduos no Brasil, independentemente de sua nacionalidade.

Por fim, a lei visa regulamentar o uso de dados pessoais por empresas e órgãos governamentais, evitando abusos e garantindo que as informações dos indivíduos sejam tratadas com responsabilidade. No entanto, como destaca Castro (2021), a implementação da LGPD enfrenta desafios, especialmente para pequenas e médias empresas que nem sempre dispõem de recursos para garantir plena conformidade com a legislação. Lima (2022) também ressalta que a lei levanta debates sobre o equilíbrio entre a proteção de dados e a inovação tecnológica, já que, em alguns casos, a regulamentação pode ser vista como um entrave para o desenvolvimento de novas tecnologias

No século atual, em que uma rede crescente de dispositivos interconectados permite o monitoramento e regulação remota de sistemas, o potencial de otimização dos processos é grande, como aponta Teffé (2018). Essas inovações melhoram significativamente a qualidade de vida, mas também ampliam os riscos associados à privacidade e segurança de dados. A LGPD, portanto, desempenha um papel crucial na proteção dessas informações, mas deve ser constantemente atualizada para acompanhar a evolução tecnológica e garantir que a proteção de dados caminhe junto à inovação, promovendo segurança e confiança sem frear o progresso.

4 PRÁTICAS DE PREVENÇÃO

Desenvolver um plano robusto para garantir a segurança de dispositivos móveis pode ser uma tarefa desafiadora, devido à constante evolução tecnológica e à velocidade com que surgem novos produtos e ameaças. Embora esse cenário seja incerto, algumas práticas que serão citadas nesse capitulo já estão integradas ao cotidiano e ao amadurecimento das estratégias adotadas por diversas organizações.

Para iniciar a proteção adequada, é fundamental compreender o que precisa ser resguardado. A informação, composta por dados processados que geram valor dentro de um contexto específico, é amplamente considerada um dos ativos mais valiosos. Seu valor está diretamente relacionado aos recursos e benefícios que ela proporciona (Silva, 2020).

Nesse contexto, em dispositivos móveis, a segurança da informação ganha ainda mais relevância, considerando a crescente dependência de smartphones e tablets para atividades pessoais e profissionais. A proteção deve envolver não apenas os dados armazenados, mas também a comunicação e o uso de aplicativos, onde medidas como criptografia, autenticação multifator e atualização constante de *software* se tornam essenciais para mitigar vulnerabilidades.

4.1 Conceito de segurança da informação

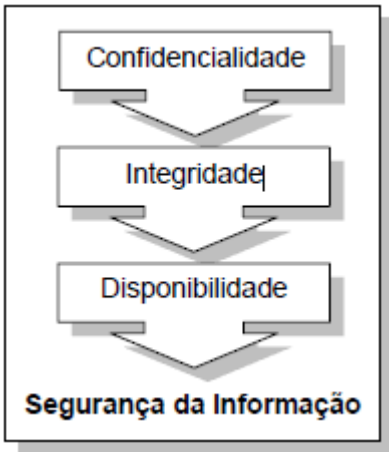
A Segurança da Informação é uma área dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade, conforme definido por Sêmola (2003). Isso envolve a aplicação de dispositivos e processos para garantir que a confidencialidade, integridade e disponibilidade (CID) das informações sejam preservadas. Esses três pilares são fundamentais para qualquer estratégia eficaz de segurança da informação: a confidencialidade visa garantir que apenas pessoas autorizadas tenham acesso às informações, a integridade assegura que os dados sejam exatos e não corrompidos, e a disponibilidade garante o acesso aos dados por usuários autorizados sempre que necessário (ABNT NBR ISO/IEC 27000, 2006).

Manter esses princípios requer não apenas a criação de políticas bem definidas, mas também a sua atualização contínua. Conforme Simch e Tonetto (2008), a política de segurança da informação deve ser clara, flexível e abrangente, prevendo possíveis adaptações futuras. Isso significa que as revisões e melhorias precisam ser constantes, à medida que novas ameaças surgem e as tecnologias evoluem.

A construção de uma política eficiente começa pela identificação dos ativos que precisam ser protegidos e dos riscos envolvidos, tanto em termos físicos quanto digitais. Da Silva (2009) destaca que as ameaças podem ser naturais, como incêndios e enchentes, ou relacionadas à vulnerabilidade dos sistemas, como falhas humanas ou ataques cibernéticos. Dessa forma, a análise de risco, que considera vulnerabilidades e ameaças, é fundamental para a criação de uma política de segurança robusta. Além disso, todos os colaboradores de uma organização devem estar envolvidos no processo, já que a negligência ou a falta de conhecimento podem comprometer seriamente a integridade dos dados.

Por fim, a segurança da informação não se limita apenas aos sistemas ou aplicativos eletrônicos. Ela também abrange a proteção de dados armazenados em diferentes formatos, sejam físicos ou digitais, conforme observado por Bastos & Caubit (2009). Isso reforça a importância de uma abordagem abrangente e integrada para a proteção dos dados em qualquer contexto organizacional.

Figura 5: Classificação da Informação



Fonte: Da Silva (2009)

A Figura ilustra que os três pilares essenciais da segurança da informação são garantir que os dados de uma empresa sejam acessíveis apenas às pessoas autorizadas, sejam confiáveis e estejam sempre disponíveis para quem tem permissão. Esses princípios são cruciais para estruturar uma política de segurança eficaz, permitindo a continuidade dos negócios e criando um ambiente seguro para os ativos da organização.

Para estabelecer uma política de segurança da informação, as empresas podem adotar diferentes abordagens, sendo uma das mais reconhecidas a certificação pela ABNT NBR ISO/IEC 27000. Conhecida como "Gestão de Segurança

da Informação – Especificação e Diretrizes para Uso", essa certificação fornece um conjunto de normas que orienta a criação, implementação, monitoramento, revisão e melhoria contínua de sistemas de gestão de segurança da informação.

Independentemente da abordagem adotada, todas as estratégias de segurança se baseiam em três pilares interdependentes: Pessoas, Processos e Tecnologias. Uma falha em qualquer um desses elementos pode comprometer toda a estrutura de segurança. As pessoas desempenham um papel crucial, pois erros humanos ou falta de conhecimento sobre as políticas podem expor a empresa a riscos. Os processos são as diretrizes e procedimentos que garantem a aplicação correta das medidas de segurança. Por fim, as tecnologias proporcionam as ferramentas necessárias para proteger os dados e manter a integridade do sistema. A integração eficaz desses três pilares é essencial para a proteção contínua e eficiente da informação.

4.2 Desafios e Soluções: O Papel das Pessoas na Segurança da Informação

A principal ameaça para qualquer segurança é o próprio ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema, não é preciso ser especialista para entender que as pessoas são um dos maiores pontos vulneráveis quando se trata de segurança da informação. Conforme o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), muitos incidentes ocorrem devido à falta de cuidado dos próprios usuários autorizados (CERT.br, 2024).

No contexto dos dispositivos móveis, essa realidade se torna ainda mais evidente. É comum ver pessoas armazenando senhas em lugares inseguros, como aplicativos de blocos de notas no próprio celular, ou usando a mesma senha para diferentes aplicativos e serviços. Além disso, o uso de redes *Wi-Fi* públicas sem qualquer tipo de proteção, como uma VPN, facilita o acesso de terceiros às informações.

Essas práticas descuidadas criam brechas que criminosos cibernéticos exploram facilmente. A falta de atenção a essas pequenas atitudes pode comprometer a segurança dos dados armazenados em dispositivos móveis, destacando a importância de maior conscientização e responsabilidade por parte dos usuários. Para Kevin Mitnick em seu livro *A arte de enganar: controlando o fator humano na segurança da informação*:

> "Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis." (Mitnick, 2003, p. 3).

As pessoas tendem a ajustar seu comportamento em situações de risco, tomando decisões com base na confiança. A engenharia social se aproveita dessas vulnerabilidades e da falta de atenção dedicada à segurança, especialmente no uso de dispositivos móveis. Santos Junior (2018) destaca que o combate à engenharia social deve começar pela conscientização dos colaboradores. Segundo o autor, investir apenas em tecnologias de segurança não é suficiente se os funcionários não forem treinados para reconhecer e evitar golpes baseados em manipulação psicológica. Ele argumenta que, sem esse conhecimento, todo o esforço para proteger a infraestrutura da empresa pode ser facilmente comprometido por um ataque de engenharia social.

Embora o termo "engenharia social" possa parecer superestimado, ele é bastante pertinente no contexto da segurança da informação. "Engenharia" refere-se ao uso de conhecimento técnico aplicado com habilidade, seja na construção civil, na mecatrônica ou em outras áreas, enquanto "social" se refere à interação entre pessoas. A combinação desses termos pode parecer desconfortável, mas na segurança da informação, "engenharia social" descreve precisamente as táticas que criminosos utilizam para manipular pessoas e obter informações confidenciais sem que elas percebam (Santos Junior, 2018).

A engenharia social caracteriza-se como uma forma de intrusão não técnica, que enfatiza a interação humana e frequentemente envolve o uso de engano para comprometer procedimentos de segurança (Silva Filho, 2004). Um "engenheiro social" é alguém que usa fraude, influência e persuasão para atacar empresas, geralmente com o objetivo de acessar informações valiosas (Mitnick, 2003). Segundo Mitnick (2003), a principal diferença entre o engenheiro social e um golpista comum é que o primeiro foca em enganar empresas, enquanto o segundo visa enganar indivíduos.

No contexto dos dispositivos móveis, esses ataques são ainda mais perigosos, pois os smartphones e tablets tornaram-se ferramentas essenciais nas atividades

pessoais e profissionais. Isso expõe informações críticas a riscos, especialmente quando os usuários não estão cientes das táticas de engenharia social aplicadas por criminosos. Portanto, além de soluções tecnológicas, a conscientização e o treinamento contínuo dos colaboradores são fundamentais para fortalecer a segurança em dispositivos móveis.

A segurança das informações não deve ser vista apenas como uma responsabilidade da equipe de tecnologia da informação, mas sim como um compromisso compartilhado por todos os colaboradores de uma empresa. É fundamental criar a consciência de que cada funcionário é uma linha de defesa essencial na proteção do sistema. Assim, incentivar a cultura de segurança deve ser um objetivo constante dentro das organizações.

A colaboração de todos os envolvidos nos processos e sistemas é fundamental para fortalecer a política de segurança da informação. De acordo com Santos Junior (2018), a seleção de profissionais com acesso privilegiado deve ir além das qualificações técnicas, envolvendo uma avaliação criteriosa de seu histórico e comportamento ético. O autor enfatiza que essa abordagem é essencial para reduzir riscos, garantindo que apenas pessoas de confiança tenham acesso a áreas críticas da organização. Além disso, ele aponta que, ao abrir um sistema para o público, é igualmente importante fornecer orientações claras e acessíveis aos usuários sobre as melhores práticas de segurança, a fim de minimizar vulnerabilidades internas e externas.

Frequentemente, os usuários esquecem ou ignoram essas práticas, resultando em falhas significativas, como aceitar termos sem leitura ao instalar aplicativos, o que pode expô-los a riscos desnecessários (Santos Junior, 2018).

Para se proteger contra ataques de engenharia social, os usuários devem adotar técnicas preventivas, como a cautela ao fornecer informações pessoais e a verificação da autenticidade de solicitações. A educação contínua é uma estratégia vital; treinamentos em segurança cibernética ajudam os colaboradores a reconhecer sinais de engenharia social e a reagir adequadamente. O uso de senhas fortes e a habilitação da autenticação em dois fatores oferecem camadas adicionais de segurança contra acessos não autorizados (Santos Junior, 2018).

4.3 Processos e Modelos de Segurança da Informação

Os processos de segurança da informação demandam atenção especial dos profissionais da área, especialmente no que se refere à Classificação de Informação e Dados (CID). Para que esses processos atinjam seus objetivos, é essencial seguir um ciclo de gerenciamento de segurança.

A primeira fase desse ciclo é o planejamento, que envolve a criação e revisão das políticas gerais de segurança da informação e das políticas de apoio. Nessa etapa, é fundamental avaliar e estabelecer acordos de nível de serviço e contratos de apoio, sempre em sintonia com a gestão de nível de serviço (Santos Junior, 2018).

O resultado desse planejamento reflete a "visão" da empresa, ou seja, o que ela busca alcançar. Para transformar essa visão em realidade, é necessário elaborar um projeto e um plano de ações. Assim, ao analisarmos as empresas que se propõem a definir estrategicamente como lidar com suas informações e quais ações são necessárias para garantir sua segurança, encontramos o Plano Estratégico de Segurança da Informação (PESI). Este plano tem como objetivo identificar a situação atual da organização em relação à informação e, a partir desse diagnóstico, traçar um caminho claro para onde se deseja chegar em termos de segurança. Como destaca Sérgio Manoel (2014, p. 69):

> "O Plano Estratégico de Segurança da Informação (PESI) é um processo utilizado para desenvolver e elaborar atividades, a fim de saber o que deve ser executado e de qual maneira deve ser executado, para comunicar e implantar a estratégia escolhida pela organização. Além disso, deve responder a três perguntas básicas: onde estamos? Para onde vamos? Como chegaremos lá? Esse plano é (...) um dos principais fatores para o sucesso de SI em uma organização."

É importante que o plano seja flexível e esteja preparado para mudanças, uma vez que o ambiente empresarial está em constante evolução. Frequentemente, sistemas tornam-se obsoletos e necessitam ser substituídos por soluções mais atuais. Nesse contexto, um plano estratégico bem estruturado é essencial para garantir que a transição ocorra sem interrupções no serviço.

A implementação das políticas de segurança planejadas é crucial e envolve comunicar as diretrizes estabelecidas, classificar e gerenciar todos os ativos de informação.

Os principais tópicos a serem considerados incluem: a definição da propriedade da informação, determinando quem é responsável pelo acesso e pela realização de *backup*s; a classificação da informação com base na disponibilidade,

confidencialidade e integridade; e o controle de acesso, que deve seguir o princípio do menor privilégio, documentando todos os pedidos de acesso e evitando a segregação de funções (OGC, 2006). Além disso, a gerência de usuários e senhas deve garantir que senhas únicas e fortes sejam utilizadas, enquanto a segurança física requer controles rigorosos nas áreas de servidores e a elaboração de normatizações internas.

Na fase de avaliação, é essencial monitorar e gerenciar incidentes que possam comprometer a segurança, gerando e analisando relatórios sobre o volume e impacto dos incidentes, além de realizar auditorias internas e externas e testes de segurança (OGC, 2006). A segurança da informação deve atender aos interesses do sistema, avaliando a importância relativa das informações, equilibrando as medidas de segurança com o valor das informações. A eficácia do sistema depende de informações completas e corretas, e a segurança deve assegurar a disponibilidade dessas informações tanto internamente, para o funcionamento eficaz, quanto externamente, para atender ao mercado e à sociedade.

Por fim, a manutenção dos processos de segurança envolve a coleta de lições aprendidas e o planejamento de melhorias contínuas. É fundamental criar um modelo de segurança a ser seguido e alocar responsabilidades adequadamente durante todo o processo. O gerenciamento eficaz da segurança da informação é essencial para reduzir a vulnerabilidade a riscos conhecidos, assegurando a integridade, a disponibilidade e a confidencialidade das informações (Santos Junior, 2018).

4.3.1 Modelos de processos

Modelos de processos de segurança são fundamentais para proteger sistemas e informações em um ambiente digital complexo. Eles fornecem *frameworks* estruturados que orientam as organizações na mitigação de riscos e na integração de práticas de segurança ao longo do desenvolvimento de *software* (Edo *et al*., 2022).

Além de promover a colaboração entre diferentes equipes, esses modelos garantem que a segurança seja uma parte contínua e essencial do ciclo de vida das aplicações, podendo citar alguns deles:

- Zero Trust Security: O modelo de segurança "*Zero Trust*" pressupõe que nenhum usuário ou dispositivo deve ser automaticamente confiável, independentemente de sua localização. Isso implica em autenticação

rigorosa, monitoramento contínuo e validação de todos os acessos, tanto internos quanto externos (Mandal, 2021).

- DevSecOps: Integrar práticas de segurança no ciclo de vida de desenvolvimento de *software* (SDLC) é fundamental. O *DevSecOps* promove a colaboração entre equipes de desenvolvimento, operações e segurança, garantindo que a segurança seja uma parte integral desde a fase de design até a implementação e monitoramento (Mandal, 2021).
- OWASP Mobile Security Project: A *Open Web Application Security Project* (OWASP) fornece diretrizes e ferramentas específicas para a segurança de aplicativos móveis. O OWASP *Mobile Security Testing Guide* (MSTG) e a lista de Top 10 Vulnerabilidades Móveis são recursos valiosos para desenvolvedores e testadores de segurança (Mandal, 2021).
- Security Development Lifecycle (SDL): O SDL é uma abordagem que integra práticas de segurança ao desenvolvimento de *software*, abrangendo desde a concepção até a desativação do aplicativo. Envolve atividades como análise de riscos, treinamento em segurança, testes de segurança e gestão de incidentes (Mandal, 2021).

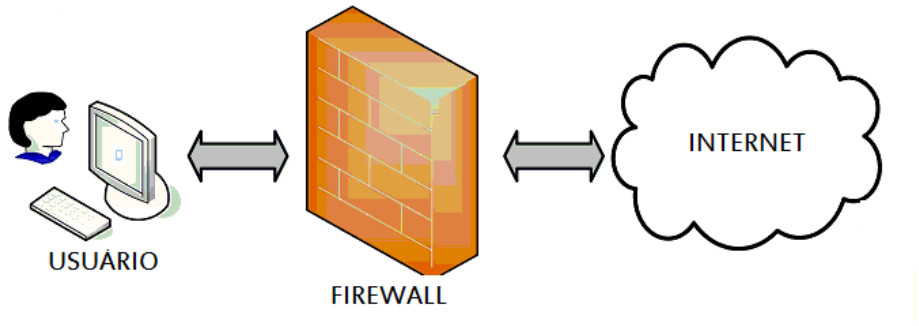
Esses modelos são fundamentais para a resiliência das infraestruturas digitais, oferecendo camadas adicionais de proteção e colaboração entre diferentes equipes, de modo a mitigar riscos desde o início dos processos de desenvolvimento (Edo et al., 2022).

4.4 Tecnologias e Meios de Proteção da Segurança da Informação

A segurança da informação evolui constantemente com o surgimento de novas ameaças. Embora seja difícil mitigar todos os riscos, algumas ferramentas são essenciais para proteger redes corporativas. Esta seção aborda as principais defesas em sistemas computacionais e recursos que usuários podem utilizar para reduzir a eficácia de ataques (Boteon, 2006).

4.4.1 Firewall

Figura 6: Funcionamento FIREWALL



Fonte: HARDTEC (2022)

O *firewall* é uma aplicação implementada na camada de rede que atua como uma barreira de controle de acessos, filtrando o tráfego de dados entre redes públicas e privadas. Pode ser implementado tanto em *software* quanto em *hardware* especializado, oferecendo uma camada adicional de proteção contra acessos não autorizados. Além disso, o *firewall* pode ser configurado para permitir ou bloquear o tráfego com base em regras definidas pelo administrador da rede, proporcionando uma defesa personalizada contra ameaças externas (Alecrim, 2013).

4.4.2 Sistema Detector de Intrusão (IDS)

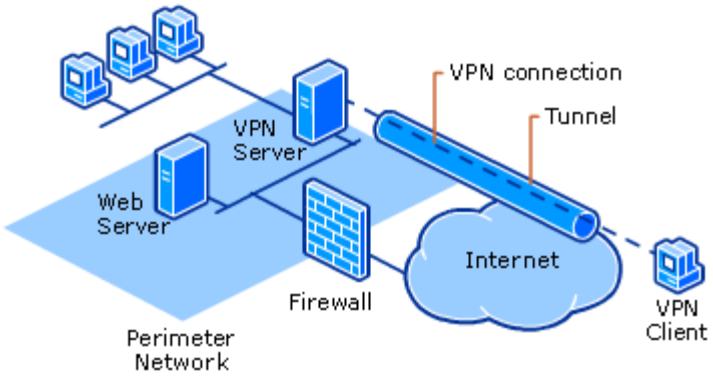
Complementando o *firewall*, o Sistema Detector de Intrusão (IDS) monitora continuamente o tráfego de dados em busca de comportamentos suspeitos ou padrões de ataque. Utilizando dados dinâmicos, como pacotes de dados com comportamentos anômalos ou códigos de ataque, o IDS é capaz de identificar e alertar sobre possíveis invasões, permitindo uma resposta rápida para mitigar os riscos antes que a segurança seja comprometida (Alecrim, 2013).

4.4.3 Varredura de Vulnerabilidades

A varredura de vulnerabilidades envolve a realização de verificações regulares em componentes críticos da rede, como servidores e roteadores. Ferramentas especializadas permitem identificar e corrigir falhas de segurança antes que sejam exploradas por atacantes. Este processo é fundamental para manter a integridade e a segurança das operações, prevenindo possíveis brechas que poderiam comprometer os dados corporativos (Alecrim, 2013).

4.4.4 Rede Virtual Privada (VPN)

Figura 7: Arquitetura de uma VPN



Fonte: UFRJ (2015)

As Redes Virtuais Privadas (VPN) são amplamente adotadas pelas empresas como uma forma de criar canais seguros para o tráfego de dados criptografados entre diferentes divisões ou parceiros de negócios. Utilizando túneis fechados, as VPNs garantem que as informações transmitidas estejam protegidas contra interceptações e acessos não autorizados, proporcionando uma comunicação segura mesmo em ambientes de rede pública

4.4.5 Criptografia

A criptografia é uma ferramenta essencial para garantir a confidencialidade das informações trocadas na rede. Existem dois tipos principais de criptografia:

- Criptografia Simétrica: Utiliza a mesma chave para criptografar e descriptografar os dados. É eficiente para a troca massiva de mensagens e é amplamente utilizada em sistemas operacionais móveis e dispositivos corporativos. Exemplos incluem o *Data Encryption Standard* (DES) e o *Advanced Encryption Standard* (AES), que oferecem diferentes níveis de segurança conforme o tamanho da chave utilizada (Bine e Kuk, 2016).
- Criptografia Assimétrica: Utiliza chaves diferentes para criptografar e descriptografar os dados, aumentando a segurança ao dificultar o acesso indevido. A chave pública é utilizada para criptografar a mensagem, enquanto a chave privada é usada para descriptografá-la, garantindo que apenas o destinatário pretendido possa acessar a informação original (Bine e Kuk, 2016).

A implementação eficaz da criptografia é fundamental para proteger dados sensíveis tanto em redes corporativas quanto em dispositivos móveis, prevenindo acessos não autorizados e garantindo a privacidade das informações.

4.4.6 Software de Backup

Os *software*s de *backup* são programas que realizam cópias de segurança dos dados, permitindo a recuperação em caso de perda ou ataque, falha de equipamentos ou incidentes inesperados. Manter *backup*s atualizados em locais seguros é uma prática indispensável para garantir a continuidade das operações e a integridade das informações corporativas (Alecrim, 2013).

4.4.7 Antivírus

Os antivírus desempenham um papel crucial na proteção de dispositivos contra ameaças como *malwares*, vírus e outras formas de *software* malicioso. Esses programas são constantemente atualizados para detectar e neutralizar as mais recentes ameaças, oferecendo uma camada adicional de segurança (Silva, 2020). Além disso, alguns antivírus oferecem funcionalidades avançadas, como a proteção contra roubo de dados e a capacidade de apagar informações remotamente em caso de perda ou roubo do dispositivo (Bine e Kuk, 2016).

Estudos indicam que os impactos de antivírus no desempenho dos dispositivos são mínimos, contrariando a percepção comum de que esses programas consomem excessivamente a bateria ou reduzem significativamente a velocidade dos aparelhos. A eficácia dos antivírus na detecção de *malwares* é comprovada, com taxas de acerto superiores a 90% na maioria dos testes realizados (Bine e Kuk, 2016).

CONCLUSÕES E TRABALHOS FUTUROS

A análise das ameaças à segurança em dispositivos móveis realizada ao longo deste trabalho destaca a complexidade crescente do ambiente digital. A explosão no uso desses dispositivos para atividades sensíveis, como transações financeiras e acesso a redes corporativas, expõe vulnerabilidades que demandam respostas urgentes. Ao longo da pesquisa, foi evidenciado que as ameaças não se limitam apenas a ataques diretos como *malware, phishing* e força bruta, mas também envolvem a engenharia social e a negligência no comportamento dos usuários. Esses fatores são explorados por invasores, aproveitando-se da falta de conscientização e de políticas de segurança pouco robustas.

Além disso, este trabalho destacou a importância das legislações brasileiras como a LGPD, a Lei Carolina Dieckmann e o Marco Civil da Internet. Embora essas leis representem avanços significativos na proteção de dados e na punição de crimes cibernéticos, ainda há lacunas, especialmente no que diz respeito à aplicação prática dessas normas e à sua adequação ao ritmo acelerado da evolução tecnológica. A necessidade de uma constante revisão das legislações para acompanhar novas ameaças cibernéticas é evidente.

No campo técnico, as práticas de prevenção abordadas neste estudo – como a implementação de *firewalls*, sistemas de detecção de intrusões (IDS), criptografia forte e VPNs – são fundamentais, mas não suficientes se não forem acompanhadas de políticas eficazes de conscientização e treinamento contínuo dos usuários. A segurança em dispositivos móveis exige uma abordagem multidimensional, que una esforços tecnológicos, legislativos e comportamentais.

A pesquisa identificou algumas lacunas e áreas que podem ser exploradas em estudos futuros. A primeira está relacionada ao desenvolvimento de *software* seguro. A integração de práticas como o DevSecOps e o modelo de Zero Trust desde o início do ciclo de desenvolvimento de aplicativos móveis pode garantir uma maior resiliência contra ataques. Investigações mais aprofundadas sobre a eficácia dessas práticas no contexto de dispositivos móveis são cruciais para melhorar a segurança.

Outra área promissora para futuras pesquisas é a criação de metodologias mais eficazes para a conscientização dos usuários. Estudos voltados para entender o comportamento dos usuários e como incentivá-los a adotar melhores práticas de

segurança podem oferecer insights valiosos para combater a engenharia social, que se mostrou uma das principais formas de intrusão não técnica.

Por fim, a legislação brasileira, embora avançada em alguns aspectos, ainda precisa de ajustes. Pesquisas focadas na harmonização entre as leis de proteção de dados e as exigências tecnológicas do ambiente móvel podem contribuir para uma defesa jurídica mais robusta. O impacto da LGPD no setor educacional e em pequenas empresas também demanda uma análise mais profunda, visando soluções que facilitem a conformidade sem inibir a inovação tecnológica.

Dessa forma, o trabalho não apenas aborda os desafios atuais da segurança em dispositivos móveis, mas também lança luz sobre as direções que futuras pesquisas e iniciativas devem seguir, reforçando a importância de uma abordagem integrada entre tecnologia, comportamento humano e regulação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27000. Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2006.

ALECRIM, E. O que é firewall? - Conceito, tipos e arquiteturas. Disponível em: https://www.infowester.com/firewall.php. Acesso em: 8 out. 2024.

AMORIM, J. Engenharia social: *como proteger informações sensíveis contra ataques psicológicos.* 2. ed. São Paulo: Novatec, 2023.

BARROS, F. C.; VICTORA, C. G.; HORTA, B. L.; LIMA, R. M.; SILVA, P. A. Saúde pública no Brasil: avanços e desafios. *Cadernos de Saúde Pública*, v. 39, n. 9, p. e00000000, 2023. Disponível em: https://www.scielo.br/j/csp/a/ywYD8gCqRGg6RrNmsYn8WHv/. Acesso em: 11 out. 2024.

BASTOS, A.; CAUBIT, R. Gestão de segurança da informação: ISO 27001 e 27002 – Uma visão prática. Rio Grande do Sul: Zouk, 2009.

BINE, J.; KUK, J. N. Estudo de segurança em dispositivos móveis. In: Seminário de Computação e Tecnologia da Informação, 2016, Guarapuava. Anais [...]. Guarapuava: UNICENTRO, 2016. Disponível em: https://semanaacademica.org.br/system/files/artigos/jamilson_bine-estudo_de_seguranca_em_dispositivos_moveis.pdf. Acesso em: 8 out. 2024.

BOTEON, A. Análise de ferramentas para segurança de redes. Universidade Federal de Santa Catarina, Florianópolis, 2006. Disponível em: https://repositorio.ufsc.br/handle/123456789/184352. Acesso em: 3 nov. 2023.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 26 out. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 set. 2024.

BUSINESS TECH WEEKLY. What is the best countermeasure against social engineering?. Disponível em: https://www.businesstechweekly.com/cybersecurity/phishing/what-is-the-best-countermeasure-against-social-engineering/. Acesso em: 12 out. 2024.

CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 24 ago. 2024.

CASTRO, R. G. *Proteção de Dados Pessoais no Brasil: Uma Análise da LGPD*. São Paulo: Editora Jurídica, 2021.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para internet. Disponível em: https://cartilha.cert.br/. Acesso em: mai. 2024.

CISCO. Capítulo 7: Protegendo a conectividade de site para site. Disponível em: https://www.cisco.com/c/pt_br/about/csr.html. Acesso em: 3 jul. 2015.

CONVENÇÃO SOBRE CIBERCRIME, Conselho da Europa, 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 24 set. 2024.

EDO, N.; MEDEIROS, R. S.; SILVA, V. B. A importância de frameworks de segurança no desenvolvimento de software. Anais do XX Congresso Nacional de Segurança da Informação, Tecnologia e Inovação, 2022.

FGV EAESP. Panorama Estratégico de Tendências e Inovações (PESTI) 2024. São Paulo: Fundação Getulio Vargas, 2024. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti-fgvcia-2024_0.pdf. Acesso em: 18 out. 2024.

FILING, B. Mobile design and development: practical techniques of creating mobile sites and web apps. 2009. p. 37-39.

GIL, A. C. Como elaborar projetos de pesquisa. 7. ed. São Paulo: Atlas, 2022.

GONZALEZ, R. Cybersecurity in Software Development: Best Practices for Threat Mitigation. New York: Tech Press, 2021.

HARDTEC. Firewall: o que é e para que serve? 2022. Disponível em: https://hardtec.com.br/firewall-o-que-e-e-pra-que-serve/. Acesso em: 8 out. 2024.

KASPERSKY. The HummingBad malware: A detailed analysis of one of the most significant mobile threats. 2017. Disponível em: https://www.kaspersky.com/resource-center/threats/hummingbad. Acesso em: 11 out. 2024.

LAUDON, K. C.; LAUDON, J. P. Sistemas de informação gerenciais. 15. ed. São Paulo: Pearson, 2022.

LIMA, A. F. *Governança de Dados e Segurança da Informação: Desafios da LGPD no Setor Educacional*. Rio de Janeiro: Editora Tecnos, 2022.

LIMA, R. Segurança da informação: proteção de dados em redes e sistemas. 3. ed. Rio de Janeiro: LTC, 2021.

MANDAL, A.; KHAN, N.; JAIN, P. Implementing Secure Development Lifecycle (SDL) in modern web applications. International Journal of Software Engineering and Computer Systems, v. 7, n. 3, p. 12-22, 2021.

MITNICK, K. *A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação*. São Paulo: Pearson Education, 2003.

MORAES, F. *Criptografia e segurança em redes wireless.* Revista de Informática Aplicada, São Paulo, v. 10, n. 2, p. 123-158, 2010.

ORIMOTO, C. E. *Smartphones: guia prático*. Porto Alegre: GDH Press e Sul Editores, 2009. 432 p.

OFFICE OF GOVERNMENT COMMERCE (OGC). Introdução ao ITIL. Norwich: OGC, 2006.

OLIVEIRA, R. *Segurança cibernética: proteções essenciais para empresas e usuários.* 3. ed. Rio de Janeiro: Alta Books, 2022.

SANTOS JUNIOR, M. A. *Crimes cibernéticos: ameaças virtuais e práticas de prevenção*. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas de Computação) – Universidade Federal Fluminense, Niterói, 2018.

SECURITY LEADERS. Ataques contra celular crescem 70% e atingem número histórico na América Latina. 2024. Disponível em: https://www.securityleaders.com.br/ataques-contra-celular-crescem-70/. Acesso em: 11 out. 2024.

SÊMOLA, M. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003. 11ª reimpressão.

SHOWMETECH. Malware HummingBad infecta mais de 10 milhões de dispositivos Android. 2016. Disponível em: https://www.showmetech.com.br/malware-hummingbad-infecta-mais-de-10-milhoes-de-dispositivos-android/. Acesso em: 3 out. 2024.

SILVA FILHO, A. M. Entendendo e evitando a engenharia social: protegendo sistemas e informações. Disponível em: http://www.espacoacademico.com.br/043/43amsf.htm. Acesso em: 24 set. 2024.

SILVA, J. C. *Segurança da informação: proteção e gestão de ativos digitais*. 2. ed. Rio de Janeiro: Editora Tech, 2020. 250 p.

SILVA, V. T. *Gestão de segurança da informação: um estudo de caso da política de segurança da informação (POL-01-100) da Cia do Metropolitano de São Paulo*. Monografia apresentada no curso de Tecnologia em Informática para Gestão de Negócios – Faculdade de Tecnologia da Zona Leste, São Paulo, 2009.

SIMCH, M. R. V.; TONETTO, T. S. Auditoria dos sistemas de informação aliada à gestão empresarial. Revista Eletrônica de Contabilidade, [S. l.], v. 4, n. 2, p. 49, 2012. DOI: 10.5902/198109465882. Disponível em: https://periodicos.ufsm.br/contabilidade/article/view/39. Acesso em: 24 set. 2024.

STALLINGS, W. *Segurança em computadores: princípios e prática.* 5. ed. São Paulo: Pearson, 2020.

TEFFÉ, C. S. *Proteção de dados pessoais na rede: resenha à obra "A internet das coisas"*, de Eduardo Magrani. São Paulo: FGV Editora, 2018.

TREND MICRO. Stepping Ahead of Risk: Trend Micro 2023 Midyear Cybersecurity Threat Report. 2023. Disponível em: https://www.trendmicro.com/vinfo/br/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report. Acesso em: 12 out. 2024.

TOMAÉL, M. I.; JESUS, José A. G. Informação em múltiplas abordagens: acesso, compartilhamento e gestão. Londrina: EDUEL, 2010.

UFRJ. Redes Privadas Virtuais (VPN): Arquitetura VPN. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2015. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/Redes-Privadas-Virtuais-VPN/Arquitetura-VPN.html. Acesso em: 21 out. 2024.

WIKIPEDIA. Motorola DynaTAC. Disponível em: https://pt.wikipedia.org/wiki/Motorola_DynaTAC. Acesso em: 19 out. 2024.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Monteiro - Código INEP: 25284940
Pb-264, S/N, Serrote, CEP 58500-000, Monteiro (PB)
CNPJ: 10.783.898/0008-41 - Telefone: (83) 3351-3700

Documento Digitalizado Restrito

TCC corrigido

Assunto:	TCC corrigido
Assinado por:	Gabriel Oliveira
Tipo do Documento:	Relatório
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Direito Autoral (Art. 24, III, da Lei no 9.610/1998)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Francisco Gabriel Oliveira**, **DISCENTE (202215020006) DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS - MONTEIRO**, em 21/01/2025 18:56:47.

Este documento foi armazenado no SUAP em 21/01/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1366451
Código de Autenticação: 7c3e1cef55