

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SUDESTE
DE MINAS GERAIS - CAMPUS RIO POMBA

VICTOR DA LUZ RIBEIRO

**IMPACTOS SOCIOECONÔMICOS DOS ATAQUES CIBERNÉTICOS E MEDIDAS DE
SEGURANÇA**

RIO POMBA - MG
2025

VICTOR DA LUZ RIBEIRO

**IMPACTOS SOCIOECONÔMICOS DOS ATAQUES CIBERNÉTICOS E MEDIDAS DE
SEGURANÇA**

Trabalho de Conclusão de curso apresentado ao Campus Rio Pomba, do Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais, como parte das exigências do curso de Bacharelado em Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação.

Orientadora: Me. GUSTAVO HENRIQUE DA ROCHA REIS

Coorientador: Dra. ALESSANDRA MARTINS COELHO

RIO POMBA - MG

2025

FICHA CATALOGRÁFICA TEMPORÁRIA

VICTOR DA LUZ RIBEIRO

IMPACTOS SOCIOECONÔMICOS DOS ATAQUES CIBERNÉTICOS E
MEDIDAS DE SEGURANÇA/ VICTOR DA LUZ RIBEIRO. – RIO POMBA -
MG, 2025-

Orientadora: Me. GUSTAVO HENRIQUE DA ROCHA REIS

Trabalho de Conclusão de Curso – Instituto Federal de Educação,
Ciência e Tecnologia do Sudeste de Minas, Campus Rio Pomba

Dedico à memória das pessoas queridas que partiram antes de
ver este momento se realizar, mas que deixaram marcas
profundas e inesquecíveis na minha vida: aos meus avós Evanir
Faria da Luz e Paulo José J. da Luz, e ao meu tio Paulo Sérgio
Faria da Luz, que tornaram minha infância incrível com sua
presença e carinho; à minha tia Denise Ribeiro Albuquerque,
que me estendeu a mão nos dias mais difíceis, quando eu mais
precisava; e ao meu grande amigo João Augusto Souza dos
Santos, que, com sua sinceridade firme e verdadeira, me
inspirou a seguir em frente e nunca duvidar do meu potencial.
Vocês seguem vivos nas minhas lembranças, e é com elas que
alcanço esta conquista.

Agradecimentos

Aos meus pais, Juscilaine Faria da Luz e Marco Antônio Ribeiro, minha mais profunda gratidão por todo o amor, dedicação e, principalmente, pela luta diária para me manter firme e tornar tudo isto possível.

À minha irmã Caroline Luz Rodrigues, agradeço pela presença, pelo companheirismo e pelo apoio incondicional ao longo de toda esta caminhada.

Sou também imensamente grato à minha companheira Maria Eduarda Bhering da Silva Coura, por ter enfrentado comigo todos os desafios deste percurso, mesmo diante da distância e das adversidades.

Aos amigos que estiveram ao meu lado, tanto os de longa data quanto aqueles que surgiram durante o curso, agradeço por cada momento compartilhado, pelas conversas, pela ajuda mútua e por tornarem esta trajetória mais leve e significativa.

Ao professor Gustavo Henrique da Rocha Reis, meu orientador, e à professora Alessandra Martins Coelho, coorientadora, deixo meu sincero agradecimento pela escuta atenta e pelas contribuições decisivas que me guiaram durante todo o processo de construção deste trabalho.

Por fim, agradeço a todas as pessoas que, direta ou indiretamente, fizeram parte e me auxiliaram de alguma forma nesta jornada.

Resumo

O crescente avanço no mundo digital tem impulsionado transformações significativas na sociedade contemporânea, mas também ampliado os riscos associados à segurança cibernética. Este trabalho tem como proposta investigar os impactos socioeconômicos decorrentes de ataques virtuais e analisar as estratégias adotadas para mitigar seus efeitos. A pesquisa, de natureza qualitativa e caráter exploratório, fundamenta-se em revisão bibliográfica e na análise de casos reais, como os incidentes envolvendo o STJ, o ConecteSUS, a Colonial Pipeline e a empresa Dyn. São abordadas ameaças como ransomware, ataques de negação de serviço (DDoS) e engenharia social, bem como os prejuízos causados e as vulnerabilidades exploradas. Entre as medidas observadas para mitigação de danos, destacam-se o uso de backups, autenticação multifator, políticas internas de segurança, capacitação contínua de usuários e parcerias com órgãos especializados. Conclui-se que os ataques analisados transcendem o ambiente digital, afetando setores críticos da sociedade, e que sua contenção depende de uma abordagem estratégica contínua, pautada em gestão de riscos, cultura organizacional e integração entre tecnologia e governança. Os resultados obtidos contribuem para o fortalecimento das práticas de segurança da informação e oferecem subsídios relevantes a gestores, pesquisadores e profissionais da área.

Palavras-Chave: Cibersegurança; Segurança da Informação; Ataques Cibernéticos; Impactos Socioeconômicos; Mitigação de Ameaças.

Abstract

The growing advancement of the digital world has driven significant transformations in contemporary society, but has also increased the risks associated with cybersecurity. This work aims to investigate the socioeconomic impacts resulting from cyberattacks and to analyze the strategies adopted to mitigate their effects. The research, qualitative in nature and exploratory in character, is based on a literature review and the analysis of real cases, such as the incidents involving the STJ, ConecteSUS, Colonial Pipeline, and the company Dyn. Threats such as ransomware, denial-of-service attacks (DDoS), and social engineering are addressed, as well as the damages caused and the vulnerabilities exploited. Among the observed measures for damage mitigation, the use of backups, multi-factor authentication, internal security policies, continuous user training, and partnerships with specialized agencies stand out. It is concluded that the analyzed attacks go beyond the digital environment, affecting critical sectors of society, and that their containment depends on a continuous strategic approach, based on risk management, organizational culture, and the integration between technology and governance. The results obtained contribute to strengthening information security practices and offer relevant support to managers, researchers, and professionals in the field.

Key-words: Cybersecurity. Information Security. Cyberattacks. Socioeconomic Impacts. Threat Mitigation.

Lista de ilustrações

Figura 1 – Pilares da Segurança da Informação.	16
Figura 2 – Taxas de infecção por malware em diferentes países.	19
Figura 3 – Exemplo de tela de resgate exibida pelo ransomware WannaCry, solicitando pagamento em Bitcoin.	29
Figura 4 – Mensagem de extorsão deixada pelo grupo Lapsus\$ nos sistemas do Ministério da Saúde após o ataque.	31
Figura 5 – Funcionamento do malware utilizado no ataque ao Banco de Bangladesh.	32
Figura 6 – Modelo de seis fases de um ciberataque.	33
Figura 7 – Mapa de interrupções de serviço causadas pelo ataque à Dyn em 2016 nos Estados Unidos.	35
Figura 8 – Mapa do sistema Colonial Pipeline, com o sistema de dutos, subdutos e pontos de entrega nos finais de semana.	36
Figura 9 – Tela de resgate exibida pelo grupo DarkSide para liberação dos sistemas da Colonial Pipeline.	37
Figura 10 – Integração entre SIEM, SOAR e XDR na resposta a incidentes.	41

Lista de quadros

Quadro 1 – Panorama dos ataques baseados em engenharia social.	18
Quadro 2 – Principais tipos de malware e suas descrições.	19
Quadro 3 – Variação do perfil e motivação de ataques DDoS ao longo de 2024. . .	21
Quadro 4 – Síntese dos casos.	39
Quadro 5 – Comparação entre as ferramentas SIEM, SOAR e XDR.	40

Lista de tabelas

Tabela 1 – Notificações formais de incidentes e vulnerabilidades em órgãos públicos entre 2021 e 2025.	14
--	----

Lista de abreviaturas e siglas

AES	Advanced Encryption Standard
API	Application Programming Interface
APT	Advanced Persistent Threat
BEC	Business Email Compromise
CEO	Chief Executive Officer
CIS	Center for Internet Security
CMS	Content Management System
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IoT	Internet of Things
ISO/IEC	International Organization for Standardization / International Electro-technical Commission
JNZ	Jump if Not Zero
LGPD	Lei Geral de Proteção de Dados Pessoais
MD5	Message Digest 5
MFA	Multi-Factor Authentication
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NOP	No Operation
OSI	Open Systems Interconnection
PCN	Plano de Continuidade de Negócios
PDF	Portable Document Format

PRI	Plano de Resposta a Incidentes
RaaS	Ransomware as a Service
RSA	RivestShamirAdleman
SIEM	Security Information and Event Management
SMB	Server Message Block
SMBv1	Server Message Block version 1
SOAR	Security Orchestration, Automation and Response
SQL	Structured Query Language
SQLi	SQL Injection
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SYN	Synchronize
TBps	Terabits per second
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
XDR	Extended Detection and Response

Sumário

1	Introdução	14
2	Fundamentação Teórica	16
2.1	Conceitos Fundamentais de Segurança Cibernética	16
2.2	Principais Ameaças Digitais	17
2.2.1	Engenharia social	17
2.2.2	<i>Malware</i>	18
2.2.3	Ataque DDoS	20
2.2.4	Injeção de SQL	22
2.2.5	Aspectos Legais e Regulatórios	22
3	Trabalhos Relacionados	24
3.1	O aumento dos ataques cibernéticos em função da pandemia de COVID-19	24
3.2	Engenharia Social e a Segurança da Informação	24
3.3	Estudo Exploratório sobre os Ataques Cibernéticos e a Ineficiência Penal	25
3.4	Segurança Cibernética em Redes Modernas: Como Proteger e Mitigar Ataques Cibernéticos	25
3.5	Análise dos Impactos dos Crimes Cibernéticos na Sociedade Brasileira: Desafios e Perspectivas de Combate	26
3.6	Síntese dos Trabalhos Relacionados	26
4	Metodologia	28
5	Casos Relevantes de Incidentes Cibernéticos	29
5.1	WannaCry (2017)	29
5.2	STJ e Conectsus (2020-2021)	30
5.3	BANGLADESH BANK (2016)	31
5.4	HBGary (2011)	33
5.5	Dyn (2016)	35
5.6	Colonial pipeline (2021)	36
5.7	Resultado da Análise	38
5.8	Controles Técnicos e Automatização de Defesa	40
5.9	Conscientização e Cultura de Segurança	41
5.10	Resposta a Incidentes e Recuperação	42
6	Conclusão	43

1 Introdução

Ocorrências recentes envolvendo exposição de informações sigilosas, falhas em serviços governamentais e fraudes virtuais passaram a ocupar um espaço frequente na mídia, despertando a atenção para a fragilidade de muitas estruturas digitais. Questões antes restritas a profissionais da área de Tecnologia da Informação (TI) passaram a fazer parte do cotidiano de muitas pessoas e corporações. Isso demonstra não só o avanço das técnicas utilizadas por agentes mal-intencionados, mas também o grau de dependência que sociedades modernas desenvolveram em relação à evolução eletrônica.

Segundo a ??), apenas no primeiro semestre daquele ano foram detectadas mais de 16,2 bilhões de tentativas de ataque no Brasil, número que reflete o volume bruto de ameaças identificadas por sistemas de segurança. Dados mais recentes indicam que o Brasil foi alvo de aproximadamente 356 bilhões de tentativas de invasões cibernéticas ao longo de 2024, representando um aumento expressivo na sua intensidade. No mesmo período, a América Latina acumulou cerca de 921 trilhões de atividades cibercriminosas, sendo o Brasil (38,73%) o país mais afetado da região, seguido por México (35,22%), Colômbia (8,72%) e Peru (4,94%) (??).

Os dados do Centro de Tratamento de Incidentes de Segurança da Administração Pública Federal (CTIR Gov) referem-se a notificações formais de vulnerabilidades e incidentes em órgãos públicos federais, conforme a Tabela 1.

Tabela 1 – Notificações formais de incidentes e vulnerabilidades em órgãos públicos entre 2021 e 2025.

Ano	Vulnerabilidades	Incidentes	Total de notificações
2025	1994	4859	6853
2024	5115	9803	14918
2023	10225	4905	15130
2022	5128	3402	8530
2021	4964	4903	9867
Total	27426	27872	55298

Fonte: ??).

De acordo com o próprio CTIR Gov, um incidente de segurança corresponde a qualquer evento adverso, confirmado ou suspeito, que comprometa a integridade, disponibilidade ou confidencialidade de sistemas e redes computacionais, como ataques, vazamentos de dados ou indisponibilidades de serviços. Já as vulnerabilidades são notificações de caráter preventivo, emitidas para alertar sobre falhas técnicas que podem ser exploradas, mesmo que ainda não tenham sido utilizadas em ações concretas.

Ainda em consonância com a Tabela 1, em 2021 foram registradas 9.867 notificações. Esse número caiu para 8.530 em 2022, mas cresceu significativamente em 2023 (15.130)

e manteve-se elevado em 2024 (14.918). Em 2025, foram reportados 6.853 casos até o final de junho, data de referência da última atualização disponível. Caso a tendência de notificações se mantenha no segundo semestre, projeta-se que o número total de casos em 2025 poderá se igualar ou até mesmo superar os registrados nos anos anteriores.

Embora as informações apresentadas anteriormente retratarem o cenário brasileiro, episódios internacionais ajudam a dimensionar o alcance e a gravidade do problema em escala global. Em 2018, por exemplo, a empresa britânica de consultoria política Cambridge Analytica, obteve acesso indevido a dados de cerca de 50 milhões de usuários do Facebook nos Estados Unidos, por meio de um aplicativo de teste psicológico. As informações foram utilizadas sem consentimento para fins de propaganda eleitoral, segmentando eleitores com base em perfis comportamentais (??).

Diante desse contexto, esta pesquisa tem como finalidade analisar os riscos cibernéticos mais recorrentes e suas repercussões sociais e financeiras, com base em exemplos concretos de ataques que afetaram instituições, além de avaliar estratégias eficazes para a prevenção de ciberameaças. Para isso, propõe-se:

- Identificar e descrever os principais vetores de ameaça cibernética e seus efeitos sobre organizações e sociedade;
- Analisar acontecimentos históricos relevantes que exibem suas incidências na perspectiva nacional e internacional;
- Apresentar as melhores práticas técnicas, políticas e regulatórias para reduzir vulnerabilidades e aprimorar a segurança tecnológica.

O texto dessa monografia está organizado em seis seções. A Seção 1 apresenta o tema, os objetivos, a justificativa e a problemática do estudo. A Seção 2 traz a fundamentação teórica, abordando os principais conceitos de segurança cibernética, tipos de ameaças digitais, aspectos legais e trabalhos relacionados. Na Seção 3 descreve-se a metodologia utilizada na pesquisa. A Seção 4 analisa casos relevantes de ciberataques, suas consequências e como as organizações solucionaram os problemas. Na Seção 5 discute-se medidas de prevenção e boas práticas para a preservação de dados. Por fim, a Seção 6 apresenta as considerações finais e sugestões para estudos futuros.

2 Fundamentação Teórica

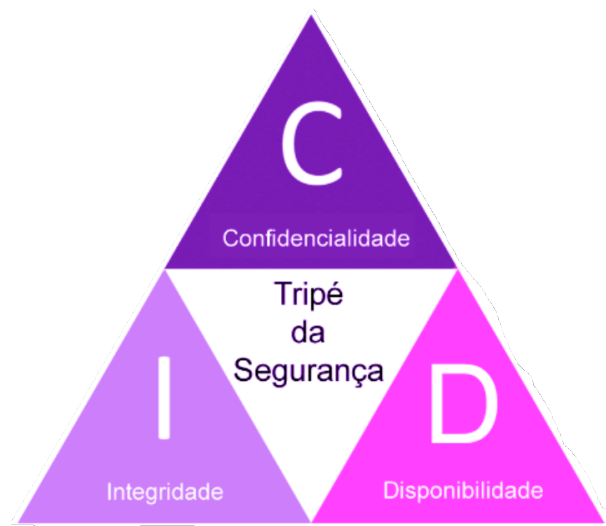
Esta seção aborda os conceitos essenciais e o estado da arte relacionados à cibersegurança, contemplando diferentes tipos de ciberataques, o contexto regulatório brasileiro e estudos correspondentes.

2.1 Conceitos Fundamentais de Segurança Cibernética

A cibersegurança pode ser entendida como o conjunto de práticas, políticas e tecnologias destinadas à proteção de sistemas, redes e dados contra acessos indevidos, falhas de funcionamento, interrupções e atividades hostis. Uma defesa eficaz é crucial para assegurar a continuidade das operações e a confiabilidade de infraestruturas conectadas (??, p. 7).

Essa área abrange tanto dimensões técnicas, como o uso de criptografia, que codifica dados para impedir acessos não autorizados; autenticação multifator, que exige múltiplas formas de verificação para liberação de entrada; firewalls, que bloqueia tráfego anômalo; e redes segmentadas, que isolam partes da infraestrutura para limitar danos. Também envolve aspectos organizacionais e humanos, como o estabelecimento de políticas internas; controle de acessos, que define quem pode visualizar ou modificar informações; e programas de capacitação de usuários, treinando pessoas para evitar tentativas de invasão (??).

Figura 1 – Pilares da Segurança da Informação.



Fonte: ??).

No centro dessas medidas está a chamada Tríade da Segurança da Informação, representada na Figura 1. Ela é composta pelos pilares de Confidencialidade, Integridade e Disponibilidade, os quais são amplamente reconhecidos por normativas internacionais, como a ISO/IEC 27002:2022, e por frameworks consolidados no setor.

A tríade compreende: (i) Confidencialidade, que se refere à proteção dos dados contra acessos não autorizados, assegurando que apenas indivíduos ou sistemas válidos possam visualizá-los ou manipulá-los; (ii) Integridade, que diz respeito à garantia de que as informações permaneçam precisas, completas e inalteradas ao longo do tempo, protegidas contra modificações acidentais ou intencionais; e (iii) Disponibilidade, que assegura que as informações e serviços estejam acessíveis e operacionais sempre que necessário, mesmo diante de falhas técnicas ou tentativas de interrupção (??, p. 8).

2.2 Principais Ameaças Digitais

As instituições contemporâneas lidam com ofensivas virtuais que exploram vulnerabilidades tanto em sistemas quanto no comportamento humano. A seguir, são apresentadas algumas das táticas maliciosas que são frequentemente empregadas.

2.2.1 Engenharia social

A engenharia social compreende um conjunto de técnicas que exploram aspectos psicológicos com o intuito de manipular indivíduos e obter acesso não autorizado a sistemas ou recursos. Ao contrário das vulnerabilidades puramente virtuais, esse tipo de atividade nociva se baseia na exploração da confiança, medo ou distração das vítimas, tornando-se uma das abordagens mais eficazes em campanhas criminosas (??).

Dentre os métodos mais comuns se destacam o phishing (envio de e-mails fraudulentos), o spear phishing (mensagens personalizadas e direcionadas a indivíduos ou organizações específicas), smishing (mensagens SMS), vishing (ligações telefônicas), pretexting¹, baiting², tailgating³ e dumpster diving⁴. Com a sofisticação da tecnologia com o passar dos anos, esses métodos passaram a incorporar recursos como inteligência artificial generativa, que é capaz de criar textos, imagens ou áudios com aparência real (????).

Conforme exposto pelo IBM X-Force Threat Intelligence Index (??), houve um aumento de 84% na disseminação de infostealers (programas maliciosos projetados para coletar informações de forma furtiva) utilizando essas técnicas, muitas vezes ocultos em arquivos PDF. O relatório ainda aponta, por indicativos de dados preliminares no início de 2025, que esse número sugere uma projeção de aumento para 180% até o final do ano.

O Quadro 1 reúne algumas estatísticas que mostram a incidência dessas ações, os principais atores envolvidos, os objetivos por trás das ofensivas e os tipos de informações mais expostas, levando em conta apenas os episódios em que houve comprometimento confirmado, ou breaches.

¹ Uso de identidades falsas

² iscas com código malicioso

³ acesso físico não autorizado

⁴ coleta de dados descartados

Quadro 1 – Panorama dos ataques baseados em engenharia social.

Categoria	Resultado
Frequência	3.661 incidentes, sendo (82,8%) com vazamento confirmado de dados.
Atores de ameaça	(100%) externos (breaches).
Motivações	(95%) financeiras, (5%) espionagem (breaches).
Dados comprometidos	Credenciais (50%), pessoais (41%), internos (20%), outros (14%).

Fonte: ??), adaptado.

Os dados apresentados ilustram a predominância de agentes externos com motivação financeira nos ataques baseados em engenharia social, além de destacar a alta taxa de vazamentos confirmados. O comprometimento regular de credenciais e dados pessoais reforça a efetividade dessas ações e os perigos que representam tanto para usuários quanto para organizações. Em 2023, esse golpe foi responsável por prejuízos de aproximadamente US\$ 2,9 bilhões em 21.489 ocorrências. Da análise, destacou-se o pretexting, frequentemente associado ao golpe conhecido como Business Email Compromise (BEC), no qual o atacante utiliza identidades falsas para enganar empresas e induzir transferências bancárias indevidas (??).

Preocupa-se também a rapidez com que as vítimas são enganadas. Estudos indicam que, após receberem um e-mail fraudulento, os usuários levam em média 21 segundos para clicar em um link e 28 segundos para inserir informações solicitadas, tempo suficiente para a consumação da ação criminosa (??).

Além da questão corporativa, a engenharia social tem-se mostrado igualmente eficaz contra indivíduos, especialmente os mais vulneráveis. O relatório do Internet Crime Complaint Center (IC3) publicado pelo ??) revelou que, em 2023, foram registradas 880.418 denúncias, totalizando US\$ 12,5 bilhões em perdas. Um número expressivo dessas fraudes envolve táticas baseadas em manipulação psicológica, como os golpes de suporte técnico e falsos representantes de órgãos governamentais. Essas práticas atingiram fortemente a população idosa, responsável por mais de US\$ 3,1 bilhões em danos econômicos. Esses números revelam a dimensão e o papel central da engenharia social no cenário atual do cibercrime.

2.2.2 Malware

O termo malware, originado da junção de malicious e software, designa qualquer programa ou código criado com a finalidade de comprometer o funcionamento de sistemas computacionais. Pode causar danos a dispositivos, interromper serviços, espionar usuários, subtrair informações ou assumir o controle de redes, muitas vezes sem o conhecimento da vítima (??).

Essa categoria abrange desde ciberameaças discretas até invasões altamente destrutivas. A seguir, o Quadro 2 apresenta os tipos mais comuns e suas formas de atuação.

Quadro 2 – Principais tipos de malware e suas descrições.

Ameaça	Descrição
Vírus	Anexa-se a arquivos ao ser executado, então se replica e pode corromper informações ou assumir funções do sistema.
Worm	Propaga-se automaticamente por redes, sem ação do usuário, explorando falhas de segurança.
Trojan (Cavalo de Troia)	Finge ser legítimo; permite acesso remoto, coleta indevida de informações e instalação de outros softwares nocivos.
Spyware	Espiona o usuário e envia conteúdos sensíveis ao invasor, como senhas ou padrões de navegação.
Adware	Exibe anúncios indesejados e pode instalar programas ou alterar configurações do sistema.
Ransomware	Criptografa arquivos e exige resgate; pode também ameaçar divulgar os dados.
Rootkit	Oculto malwares e dá ao criminoso controle total, sendo difícil de detectar e remover.
Keylogger	Registra teclas digitadas para capturar senhas e dados confidenciais sem a vítima perceber.
Bot/Botnet	Controla o dispositivo infectado remotamente como parte de uma rede (botnet), usada para ataques coordenados como DDoS.

Fonte: (???) e ??).

Segundo a ??), o malware permanece entre as ameaças mais comuns, frequentemente servindo como ponto de partida para ataques mais avançados. A disseminação pode ocorrer por diversos meios, como anexos de e-mail, páginas contaminadas, dispositivos externos ou falhas em softwares sem atualização. A Figura 2 ilustra a disseminação do malware em termos geográficos, revelando o Brasil entre os países com maiores taxas de incidência (34,68%), superado apenas por nações como China, Taiwan e Rússia.

Figura 2 – Taxas de infecção por malware em diferentes países.

Fonte: ??).

Vírus e worms continuam explorando vulnerabilidades em sistemas desatualizados ou mal protegidos, sendo frequentes em ambientes corporativos que carecem de políticas eficazes de backup e atualização. Seus impactos variam desde falhas de desempenho e instabilidades até o comprometimento de dados sensíveis, perdas financeiras e danos à reputação. Enquanto os vírus dependem da ativação do usuário para iniciar sua ação, os worms se replicam de forma autônoma e silenciosa, favorecendo sua disseminação em larga escala e potencializando riscos como interrupções operacionais, sobrecarga de redes e infecções sucessivas em dispositivos vulneráveis (???)

O ransomware tem se destacado pelos prejuízos financeiros e operacionais que causa às vítimas. Apenas no último trimestre de 2022, de acordo com o relatório Cyber Threat Report da ??), foram contabilizadas 154,9 milhões de tentativas desse ciberataque, com forte presença da estratégia de dupla extorsão, que combina o sequestro de dados com ameaças de exposição. No total anual, identificou-se 493,3 milhões de tentativas de ransomware em todo o mundo, sendo o segundo maior volume da história monitorada pela empresa. Além disso, o pagamento de resgates, prática comum no ransomware, não assegura a recuperação do que foi perdido e ainda pode financiar mais atividades criminosas, perpetuando ciclos cada vez mais complexos (??).

Os trojans aproveitam-se de vetores como phishing, spam e aplicativos falsos para atingir plataformas como Windows, macOS e Android. Famílias como o Emotet, que distribui outros malwares, e o Trickbot, voltado ao roubo de credenciais bancárias, permanecem em atividade mesmo após operações globais para sua neutralização. Em dispositivos móveis, destacam-se variantes com acesso remoto que conseguem se disfarçar até em lojas oficiais, executando ações sem o conhecimento da vítima (??).

Os efeitos dessas ciberameaças vão além da esfera digital. Entidades como o ??) e o ??) alertam para as graves consequências, que podem comprometer a segurança nacional, afetar serviços de saúde pública e gerar danos expressivos à economia global.

2.2.3 Ataque DDoS

Ataques de negação de serviço distribuída (DDoS) visam tornar serviços online indisponíveis ao sobrecarregá-los com um volume excessivo de tráfego gerado por múltiplas fontes comprometidas. No quarto trimestre de 2023, operações desse tipo atingiram níveis recordes, especialmente em períodos comerciais críticos, afetando diferentes níveis do modelo OSI⁵ (??).

Esse ciberataque se divide em duas categorias principais. A primeira, nas camadas de infraestrutura (três e quatro), responsáveis pelo roteamento e transporte de dados na rede, é caracterizada por grandes volumes de pacotes mal-intencionados que visam congestionar a rede. Destacam-se as inundações SYN, que enviam repetidos pedidos de conexão TCP sem finalização, sobrecarregando o servidor; e as inundações UDP, que direcionam pacotes não solicitados a portas aleatórias, exigindo respostas contínuas e esgotando os recursos do sistema (Hanák,??). A segunda categoria atinge a camada de aplicação (seis e sete), voltadas à apresentação e interação com o usuário, com vulnerabilidades mais sofisticadas e sutis, voltadas a sobrecarregar funções específicas, como páginas de login e APIs (interfaces que permitem a comunicação entre softwares), mesmo com menor volume de tráfego (Amazon Web Services, ??).

⁵ Uma estrutura em sete camadas que padroniza a comunicação entre dispositivos em redes de computadores

Essa diferenciação é crucial para identificar os vetores utilizados e os obstáculos envolvidos na identificação e neutralização. Enquanto as ofensivas na infraestrutura são volumosas e possuem assinaturas claras, as voltadas à aplicação tendem a ser mais discretas e difíceis de identificar.

Em 2024, o número global de ataques DDoS cresceu 108% em comparação ao ano anterior, com duração média dos incidentes em torno de 23 minutos. Ataques com duração superior a uma hora aumentaram 120%. Áreas como finanças, governo e telecomunicações, alvos frequentes, enfrentaram ataques de alta intensidade, alguns ultrapassando 1,8 TBps (terabits por segundo). No setor de telecomunicações, por exemplo, o tempo médio de uma investida DDoS chegou a 16 horas em junho de 2024. Além disso, aproximadamente 59% das ocorrências concentraram-se na camada de aplicação, dificultando a detecção devido à baixa intensidade de requisições, mas ainda prejudicando serviços essenciais (??).

Mais do que o crescimento em volume e complexidade, as motivações por trás desses ciberataques também variaram ao longo de 2024. Nos primeiros seis meses, os principais alvos foram recursos governamentais, com forte atuação de hacktivistas, isto é, indivíduos ou grupos que realizam ofensivas por motivações políticas ou ideológicas, e de grupos APT (Ameaças Persistentes Avançadas), que operam de forma contínua e coordenada, geralmente com apoio estatal e alto nível de refinamento.

Já no segundo semestre, o setor bancário passou a ser o mais destacado, com ataques direcionados à extorsão e à disrupção de serviços, geralmente perpetrados por organizações criminosas e concorrentes corporativos.

O Quadro 3 mostra essa mudança de motivação e perfil dos cibercriminosos ao longo do ano, conforme relatório da ??):

Quadro 3 – Variação do perfil e motivação de ataques DDoS ao longo de 2024.

Período	Atacantes mais típicos	Objetivo	Proporção estimada de hacktivistas versus criminosos
1º semestre de 2024	Hacktivistas e grupos APT patrocinados por Estados	Causar interrupções e atrair atenção para causas políticas	73% / 27%
2º semestre de 2024	Organizações criminosas, grupos APT e concorrentes	Extorsão por interrupção de serviços ou distração para outros ataques	42% / 58%

Fonte: ??), adaptado.

A análise demonstra que os ataques DDoS acompanham transformações políticas e econômicas, exigindo respostas que evoluam na mesma velocidade que seus propósitos e métodos.

2.2.4 Injeção de SQL

A injeção de SQL (SQLi) é uma das vulnerabilidades mais antigas e críticas em aplicações web, permitindo que invasores insiram comandos indevidos em campos de entrada para manipular bancos de dados e obter acesso não autorizado (??). Essa falha ocorre geralmente pela falta de validação adequada dos dados fornecidos pelo usuário, como em formulários de login ou pesquisa.

Os ataques de injeção SQL podem ser classificados em três modalidades principais, conforme suas estratégias de extração de informações: em banda, inferencial (ou cega) e fora de banda (??).

No SQLi em banda, o mesmo canal é usado para injeção e extração, tornando o ataque direto e eficiente. Divide-se em duas formas: o SQLi baseado em erro, que explora mensagens detalhadas para revelar a estrutura do banco; e o SQLi baseado em união, que utiliza o operador UNION, responsável por combinar os resultados de diferentes consultas em uma só. Isso viabiliza acessar conteúdos sensíveis por meio de respostas HTTP (mensagens trocadas entre navegador e servidor) (??).

O SQLi inferencial (ou cego) não fornece retorno explícito. O invasor deduz informações através da reação do sistema. Pode ocorrer de forma booleana, onde se verifica se o comportamento do servidor muda diante de condições verdadeiras ou falsas, ou baseada em tempo, analisando atrasos intencionais na resposta (??).

Já o SQLi fora de banda é mais refinado e depende de recursos específicos da aplicação. Ele utiliza requisições DNS (sistema responsável por traduzir nomes de domínio em endereços IP) ou HTTP para canais externos, o que possibilita a coleta de elementos sensíveis de forma indireta e sutil (??).

Em 2021, mais de 274 mil ocorrências de SQLi foram registradas, sendo esta considerada a terceira ameaça mais grave para aplicações web (??). Casos notórios incluem a falha no Fortinet, em 2019, que expôs contas de usuários ao permitir conexões intrusivas por meio de injeção de SQL; e o ataque ao site da Tesla, em 2014, quando pesquisadores obtiveram privilégios administrativos da mesma forma (??).

2.2.5 Aspectos Legais e Regulatórios

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, foi criada para resguardar direitos fundamentais como liberdade, privacidade e a livre formação da personalidade de cada indivíduo.

A lei regula o tratamento de dados pessoais, seja em meio físico ou digital, por pessoas físicas ou jurídicas, públicas ou privadas. Conforme a LGPD, o Controlador define as finalidades e os meios do tratamento; o Operador executa as ações seguindo as instruções do Controlador; e o Encarregado atua como intermediário entre Controlador, titulares dos

dados e a Autoridade Nacional de Proteção de Dados (ANPD) (??).

O tratamento de dados deve possuir uma finalidade clara e explícita, e o titular precisa ser informado sobre os propósitos da operação. No setor público, o tratamento está vinculado à execução de políticas públicas previstas em lei ou regulamento, assegurando transparência no compartilhamento de informações entre órgãos, que deve ser justificado e respaldado legalmente (??).

Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios fundamentais para o uso da internet no Brasil, como garantia da liberdade de expressão, proteção da privacidade e dos dados pessoais dos usuários, neutralidade da rede e responsabilização dos provedores conforme suas atividades. Também reforça o direito à inviolabilidade da intimidade e da vida privada, reconhecendo o acesso à internet como indispensável ao exercício da cidadania e protegendo o usuário contra o fornecimento não autorizado de seus registros pessoais a terceiros, salvo em situações previstas em lei (??).

3 Trabalhos Relacionados

Esta seção reúne e analisa pesquisas relevantes que dialogam com o tema central deste trabalho, abordando a evolução dos riscos cibernéticos, seus desdobramentos sociais, econômicos e jurídicos, bem como as estratégias para mitigá-los.

Os estudos selecionados fornecem uma base comparativa e crítica, contribuindo para a compreensão dos desafios contemporâneos da cibersegurança e fundamentando as discussões desenvolvidas nas seções posteriores.

3.1 O aumento dos ataques cibernéticos em função da pandemia de COVID-19

??) analisaram o impacto da pandemia de Covid-19 sobre o aumento de ataques cibernéticos, com foco na intensificação do trabalho remoto, ensino a distância e adoção massiva de plataformas online. A pesquisa destaca que essa digitalização apressada ocorreu sem preparo técnico adequado, ampliando a exposição de redes e dispositivos pessoais a criminosos virtuais. O estudo identificou um crescimento de até 350% nas campanhas de phishing durante a pandemia, impulsionadas por temas como vacinação e auxílio emergencial. Esses vetores foram utilizados para distribuir malwares com o objetivo de captura de credenciais bancárias, instalação de ransomwares, entre outros. Os autores também verificaram um aumento de 148% nos ataques por ransomware no início de 2020, com destaque para instituições hospitalares, cujos sistemas críticos foram criptografados, causando interrupções em atendimentos médicos.

Além disso, apontou-se vulnerabilidades em plataformas de videoconferência, especialmente no Zoom, que apresentou falhas como ausência de criptografia ponto a ponto, permitindo que pessoas não autorizadas participassem de reuniões. Como medidas mitigatórias, os autores destacam a necessidade de correção de falhas de segurança, atualização das políticas institucionais e adoção de recursos como a autenticação em duas etapas. Reforça-se ainda a importância da conscientização dos colaboradores e da orientação contínua como ferramentas essenciais para mitigar riscos diante de cenários emergenciais, como o vivenciado durante a pandemia de Covid-19.

3.2 Engenharia Social e a Segurança da Informação

??) investigaram a Engenharia Social como uma das estratégias mais recorrentes e eficazes em ataques cibernéticos modernos. Com base em dados da GatInfoSec (2021), os autores registraram um aumento de aproximadamente 30% nos ataques de phishing durante o ano de 2020, em parte impulsionado pela intensificação do uso de plataformas digitais no contexto da pandemia. Observou-se ainda que usuários recém-admitidos ou menos familiarizados com políticas de segurança são mais suscetíveis a esse tipo de abordagem,

mesmo após treinamentos básicos.

Segundo os autores, a consequência disso resultou em prejuízos financeiros às empresas que foram de US\$380 mil a US\$1,7 milhão. A pesquisa defendeu a implementação de treinamentos periódicos, simulações de ataques e protocolos institucionais claros, de modo a reforçar a capacidade de identificação e reação dos usuários frente a tentativas de manipulação.

3.3 Estudo Exploratório sobre os Ataques Cibernéticos e a Ineficiência Penal

??) realizaram uma análise crítica sobre os entraves legais enfrentados pelo sistema penal brasileiro diante da crescente sofisticação dos ataques cibernéticos. Eles destacam que, embora legislações específicas tenham sido promulgadas, como a Lei nº 12.737/2012 (tipifica a invasão de dispositivos eletrônicos) e a Lei nº 14.155/2021 (agrava penas para fraudes digitais), tais normas ainda não acompanham a velocidade, complexidade e alcance global das condutas criminosas no ambiente virtual. Entre os principais obstáculos à efetiva responsabilização penal, os autores mencionaram o uso de recursos tecnológicos como proxies, redes privadas virtuais (VPNs) e outros mecanismos de anonimização digital por dificultarem a identificação precisa dos agentes causadores dos ataques.

Além disso, foi observada uma defasagem entre o avanço tecnológico e a atualização normativa, gerando lacunas jurídicas e, desta forma, causando um descompasso na capacidade de resposta do Estado. Para enfrentar esses desafios, recomendou-se a reformulação de modelos jurídicos tradicionais por meio de um arcabouço normativo mais dinâmico e adaptável, defendendo uma abordagem multidisciplinar, com a colaboração entre o Estado, setor privado e sociedade civil, como estratégia essencial para reduzir os efeitos da cibercriminalidade.

3.4 Segurança Cibernética em Redes Modernas: Como Proteger e Mitigar Ataques Cibernéticos

??) realizou uma análise aprofundada sobre os desafios da segurança cibernética em redes modernas, destacando vulnerabilidades críticas exploradas por ciberataques de grande escala. O estudo partiu de um levantamento técnico de incidentes como o WannaCry, um ransomware que se espalhou globalmente em 2017 explorando uma falha no protocolo SMB do Windows; o NotPetya, que causou prejuízos bilionários ao se disfarçar como ransomware, mas com finalidade destrutiva; o Stuxnet, malware altamente sofisticado desenvolvido para sabotagem de sistemas industriais iranianos; o DarkHotel, focado em espionagem contra executivos por meio de redes Wi-Fi de hotéis; e o Mirai, que transformava dispositivos IoT mal protegidos em botnets para realizar ataques DDoS massivos. Esses riscos foram contextualizados na pós-pandemia, no qual o crescimento acelerado do teletrabalho expôs

redes domésticas e corporativas a novas ameaças.

Foi avaliada a maturidade cibernética de um setor industrial por meio da aplicação prática do NIST CSF, utilizando a ferramenta NIST CSF Maturity Tool, além de discutir metodologias como a ISO/IEC 27001 e os CIS Controls. O estudo conclui que a mitigação eficaz dos riscos cibernéticos exige mais do que ferramentas técnicas: embora frameworks como o NIST CSF sejam aliados relevantes nesse processo, seus benefícios só se concretizam quando acompanhados de práticas contínuas, como atualizações de sistemas, uso de antivírus, senhas fortes, backups regulares e atenção aos hábitos digitais dos usuários. É essencial também uma abordagem estratégica e institucional, pautada em boas práticas normativas, conscientização organizacional e fortalecimento da segurança em todos os níveis.

3.5 Análise dos Impactos dos Crimes Cibernéticos na Sociedade Brasileira: Desafios e Perspectivas de Combate

Araújo (??) apresentou um estudo abrangente sobre os efeitos dos crimes cibernéticos no contexto brasileiro, com ênfase nas consequências sociais, econômicas e jurídicas decorrentes da evolução do cibercrime. O autor destacou que, mais do que ataques técnicos, essas ações refletem desigualdades sociais e geram desconfiança generalizada no uso das tecnologias digitais, afetando especialmente populações vulneráveis, como idosos e usuários com baixa alfabetização digital. Entre os principais vetores identificados estão o phishing e ransomwares, cuja capacidade de causar enormes prejuízos tem sido documentada em relatórios como o da Axur (2021), que aponta perdas globais ultrapassando trilhões de dólares. Chamou-se atenção para a falta de profissionais qualificados em segurança da informação como um dos maiores entraves ao combate eficaz da cibercriminalidade no Brasil. Essa escassez afeta desde o desenvolvimento de políticas públicas até a aplicação das normas existentes, contribuindo para um ambiente de impunidade. Em 2022, mais de 200 milhões de ataques cibernéticos foram registrados no país, com destaque para o setor financeiro, que figura entre os mais afetados.

Como medidas estratégicas, Araújo sugeriu uma abordagem multidisciplinar que envolve Estado, setor privado e sociedade civil. Dentre as recomendações, destacam-se os programas de educação digital, modernização do arcabouço legal, cooperação internacional para troca de inteligência e investimento na formação de especialistas em cibersegurança.

3.6 Síntese dos Trabalhos Relacionados

Os trabalhos analisados convergem na identificação dos riscos cibernéticos como fenômeno multidimensional, afetando desde a segurança técnica das redes até a estabilidade jurídica e social. Ainda que cada pesquisa tenha abordado aspectos específicos, observa-se

uma complementaridade entre as abordagens técnicas, humanas, legais e organizacionais.

??) abordam as consequências da transformação digital emergencial durante a pandemia, mostrando como a falta de preparo estruturado abriu espaço para a proliferação de malwares e ataques a plataformas críticas. Já ??) enfatizam a centralidade do fator humano, destacando a engenharia social como vetor recorrente para exploração de vulnerabilidades cognitivas e comportamentais.

Do ponto de vista jurídico, ??) evidenciam que o arcabouço legal brasileiro permanece defasado diante da sofisticação dos crimes digitais, o que compromete a responsabilização penal e favorece a impunidade. Em paralelo, ??) propõe uma abordagem mais estruturada e técnica, com foco na adoção de frameworks como o NIST CSF para avaliação de maturidade cibernética. Por fim, Araújo (??) amplia a discussão ao destacar os impactos sociais dos crimes digitais, sobretudo sobre populações vulneráveis, e aponta a carência de profissionais como obstáculo estratégico à mitigação.

Em conjunto, os estudos indicam que as ameaças virtuais devem ser enfrentadas com ações coordenadas entre tecnologia, legislação, educação e gestão. Soluções isoladas se mostram insuficientes, sendo necessária uma abordagem sistêmica e interdisciplinar que envolva todos os setores da sociedade conectada.

4 Metodologia

Este trabalho adota uma abordagem qualitativa, de natureza exploratória e descritiva, centrada na análise das implicações socioeconômicas provocadas por ciberataques e nas medidas de mitigação empregadas por entidades variadas.

A pesquisa foi conduzida por meio de revisão bibliográfica, com base em artigos acadêmicos, relatórios técnicos, documentos oficiais e fontes especializadas. As informações foram obtidas principalmente através do Google Acadêmico, ResearchGate e portais reconhecidos na área de cibersegurança, priorizando materiais publicados nos últimos 15 anos.

O processo metodológico envolveu as seguintes etapas:

- Definição do tema e delimitação do escopo do estudo: Escolha do foco central e dos limites da investigação;
- Formulação da pergunta-problema e dos objetivos da pesquisa: Estruturação do questionamento principal e metas do estudo.
- Levantamento bibliográfico com base nos últimos 15 anos: Mapeamento inicial das publicações relevantes ao tema.
- Seleção e filtragem de materiais com aderência à temática: Priorização das fontes conforme sua pertinência e qualidade.
- Análise crítica e sistematização dos conteúdos mais relevantes: Organização dos achados com base em sua contribuição para os objetivos.
- Estruturação das informações em seções temáticas: Distribuição do conteúdo em blocos estruturados, com ênfase na clareza e coerência.

Para representar os efeitos reais, foram selecionados casos concretos de ataques com repercussão nacional e internacional. Durante esse processo, buscou-se garantir a diversidade das fontes de informação, a variedade dos tipos de ciberameaças, a notoriedade dos ataques estudados e o perfil das vítimas envolvidas.

Ao reunir falhas recorrentes e as lições extraídas, pretende-se incentivar um futuro mais resiliente aos crimes virtuais, reforçando a atuação preventiva em contextos diversos.

5 Casos Relevantes de Incidentes Cibernéticos

Esta seção explora cinco ciberataques significativos, selecionados por suas consequências no âmbito global e por evidenciarem diferentes fragilidades, em diferentes setores, no ecossistema digital.

5.1 WannaCry (2017)

O ransomware WannaCry destacou-se como um dos ataques cibernéticos mais marcantes da última década, infectando cerca de 230 mil computadores em aproximadamente 150 países em maio de 2017 (??).

O ataque explorou uma falha conhecida como EternalBlue, uma vulnerabilidade no protocolo SMBv1 do Windows, protocolo esse que compartilha arquivos em redes locais. Essa falha foi inicialmente descoberta pela Agência de Segurança Nacional dos Estados Unidos (NSA) e mantida em sigilo até ser vazada pelo grupo hacker Shadow Brokers, o que permitiu cibercriminosos propagarem o malware (??). Embora a Microsoft tenha lançado um patch para corrigir a vulnerabilidade meses antes do ataque, a falta de atualização em grande parte dos sistemas afetados contribuiu para a magnitude do incidente. Estima-se que os prejuízos globais ultrapassaram US\$ 4 bilhões, incluindo custos de recuperação e perdas operacionais (??).

O WannaCry destacou-se também pela sua capacidade de se espalhar automaticamente entre computadores vulneráveis, sem necessidade de interação do usuário, uma característica conhecida como "wormable". Para sequestrar os dados, utilizou técnicas de criptografia híbrida: o algoritmo AES-128 para codificar os arquivos da vítima e RSA-2048 para proteger as chaves de decodificação.

Essa combinação dificultava a recuperação do que foi perdido sem o pagamento do resgate, solicitado em Bitcoin, entre US\$ 300 e US\$ 600 (??). A Figura 3 retrata a mensagem típica de extorsão exibida às vítimas, com o endereço de carteira para envio da quantia exigida.

Figura 3 – Exemplo de tela de resgate exibida pelo ransomware WannaCry, solicitando pagamento em Bitcoin.

Fonte: ??), adaptado.

A sua proliferação foi parcialmente interrompida graças à descoberta de um kill switch acidental, um mecanismo no código que tentava acessar um domínio de internet não registrado. Quando um pesquisador britânico registrou esse domínio, o malware passou a interromper sua própria ação ao detectar a resposta do servidor (??).

No entanto, variantes posteriores eliminaram esse mecanismo, mantendo o ransomware ativo em sistemas desprotegidos.

Sua repercussão foi particularmente grave no Serviço Nacional de Saúde do Reino Unido (NHS), onde 80 hospitais sofreram interrupções, sendo 34 diretamente bloqueados. Estima-se que quase 20 mil procedimentos médicos foram cancelados, incluindo tratamentos urgentes, e ambulâncias precisaram ser desviadas para outras unidades hospitalares (United Kingdom, ??).

Mais que os efeitos técnicos, o caso levantou dilemas éticos sobre a responsabilidade dos governos na gestão de vulnerabilidades. ??) criticam a postura adotada pela NSA ao optar por manter em sigilo a vulnerabilidade EternalBlue, priorizando interesses estratégicos de inteligência em detrimento da segurança da infraestrutura civil. Segundo os autores, tal decisão contribuiu significativamente para a ampliação dos riscos globais associados à exploração da falha. Nesse sentido, os pesquisadores defendem a adoção de diretrizes éticas mais rigorosas, baseadas em transparência, cooperação internacional e responsabilidade compartilhada na divulgação e gestão de vulnerabilidades.

Como resposta, diversas entidades passaram a investir em estratégias de resiliência cibernética, incluindo segmentação de redes para limitar o alcance de ataques, backups frequentes e redundantes, monitoramento contínuo das atividades na rede e testes regulares de resposta a incidentes. Adicionalmente, a consolidação de boas práticas estruturadas em frameworks amplamente utilizados, como o NIST Cybersecurity Framework, e normas como a ISO/IEC 27001, tem se mostrado eficaz na padronização de procedimentos e no fortalecimento da maturidade cibernética diante de ameaças similares (??).

5.2 STJ e Conectsus (2020-2021)

Os ataques cibernéticos ao Superior Tribunal de Justiça (STJ) e ao sistema ConecteSUS, entre 2020 e 2021, revelam os perigos associados à digitalização acelerada dos serviços públicos em um contexto de crise sanitária global, sem a devida maturidade em segurança da informação. Esses episódios comprometeram diretamente a prestação de serviços essenciais, afetando o acesso da população à Justiça e à saúde durante a pandemia do Covid-19.

No caso do STJ, em três de novembro de 2020, a rede institucional foi comprometida por um ransomware que criptografou os dados e paralisou aproximadamente 255 mil processos em andamento (??). Como resposta imediata, os julgamentos foram suspensos, e os acessos à internet da Corte foram desativados internamente como medida de emergência. A reconstrução da infraestrutura envolveu a aplicação de autenticação multifator nos sistemas internos, revisão da arquitetura tecnológica e início de auditorias internas, visando mitigar novos riscos. Essas medidas foram complementadas por ações de conscientização

dos usuários e adequação contínua à LGPD (Conselho da Justiça Federal, ??; Superior Tribunal de Justiça, ??).

Já em dezembro de 2021, o Ministério da Saúde sofreu um ataque de ransomware que afetou o ConecteSUS, sistema responsável por registrar e disponibilizar os dados de saúde dos cidadãos, incluindo o comprovante de vacinação contra a Covid-19 (??). A ação criminosa também comprometeu plataformas complementares, como o e-SUS Notifica, utilizado para registrar casos suspeitos ou confirmados de doenças como a Covid-19, e o SI-PNI (Sistema de Informação do Programa Nacional de Imunizações), que gerencia o histórico de vacinação da população brasileira.

Como está indicado na Figura 4, a ofensiva foi reivindicada pelo grupo Lapsus\$, que alegou ter copiado e excluído informações, além de deixar mensagens de chantagem nos portais da instituição. O incidente inviabilizou temporariamente a emissão de certificados de vacinação, gerando transtornos para a (Agência Brasil, ??).

Figura 4 – Mensagem de extorsão deixada pelo grupo Lapsus\$ nos sistemas do Ministério da Saúde após o ataque.

Fonte: ??).

Diante da gravidade da invasão, o Ministério da Saúde apresentou um plano de ação estruturado com foco na recuperação e no reforço da segurança dos sistemas. As medidas incluíram: atualização de todas as credenciais administrativas, aprimoramento dos controles de acesso, análise de riscos e vulnerabilidades nos sistemas críticos, implantação de um comitê gestor da LGPD e a migração da Rede Nacional de Dados em Saúde (RNDS) para uma empresa pública federal, visando fortalecer a governança e ampliar as contratações voltadas à proteção da infraestrutura de dados sensíveis (Ministério da Saúde, ??).

Esses casos dialogam diretamente com a análise de ??), que identificou um aumento expressivo de atividade cibercriminosa no início da pandemia, impulsionado pela adoção apressada de plataformas digitais sem infraestrutura adequada de proteção.

5.3 BANGLADESH BANK (2016)

O incidente digital ao Banco Central de Bangladesh, ocorrido em fevereiro de 2016, é considerado um dos maiores crimes digitais contra instituições financeiras já registrados. Os criminosos conseguiram emitir 35 ordens de transferência fraudulentas por meio do sistema Society for Worldwide Interbank Financial Telecommunication (SWIFT), totalizando US\$ 1 bilhão em tentativas, das quais US\$ 101 milhões foram efetivamente desviados, sendo US\$ 81 milhões destinados a contas nas Filipinas e US\$ 20 milhões ao

Sri Lanka. Este último valor foi recuperado graças a um erro de digitação que levantou suspeitas na transação (??).

A ofensiva foi caracterizada por um planejamento meticuloso e pela exploração de múltiplas vulnerabilidades técnicas e operacionais.

Os criminosos infiltraram-se na rede interna do Banco Central de Bangladesh um mês antes da execução do ataque, por meio de e-mails de phishing direcionados que instalaram keyloggers e outros malwares, com o objetivo de capturar credenciais de funcionários com permissão ao sistema SWIFT.

Após o acesso inicial e o mapeamento da infraestrutura, os invasores implantaram um trojan personalizado altamente sofisticado, projetado especificamente para manipular o sistema. Essa fase de reconhecimento explorou diversas fragilidades, como a ausência de autenticação multifator, o uso de softwares obsoletos, a inexistência de firewall e comunicações internas desprotegidas, o que permitiu aos atacantes permanecerem indetectáveis por semanas. Uma impressora comprometida, responsável por registrar as transações em tempo real, também foi utilizada estrategicamente para ocultar movimentações suspeitas (??).

Figura 5 – Funcionamento do malware utilizado no ataque ao Banco de Bangladesh.

Fonte: ??), adaptado.

O funcionamento desse trojan implantado é ilustrado na Figura 5, que apresenta o processo de localização de processos sensíveis no sistema e a identificação do módulo liboradb.dll, do software SWIFT Alliance Access.

Em seguida, sobrescreve dois bytes específicos na memória que correspondem à instrução condicional Jump if Not Zero (JNZ), uma verificação típica que determina se uma operação foi bem-sucedida. Esses bytes são substituídos por comandos NOP (No Operation), que não executam nenhuma ação. Essa modificação faz com que o aplicativo host interprete falhas de verificação como sucessos, validando automaticamente transações não autorizadas. Com isso, o malware obtém controle direto sobre as operações bancárias realizadas via SWIFT, conduzindo movimentações fraudulentas sem gerar alertas visíveis (??).

O ataque foi temporizado com precisão. As ordens de transferência ocorreram numa quinta-feira, véspera de um feriado prolongado em Bangladesh, nos Estados Unidos e nas Filipinas. Esse intervalo dificultou as respostas institucionais e permitiu o envio de valores a contas falsas no Rizal Commercial Banking Corporation (RCBC), onde os recursos foram sacados rapidamente, convertidos em fichas de cassino e lavados com apoio de brechas legais no sigilo bancário (????).

Além das falhas técnicas, a resposta institucional também foi marcada por ne-

gligência. O Banco de Bangladesh levou semanas para tornar o ataque público, o que comprometeu a investigação. A rede SWIFT afirmou não ter sido violada, apesar de mensagens fraudulentas terem sido validadas. O Federal Reserve de Nova York autorizou transações sem validação do banco de origem, mesmo após alertas de bancos intermediários (??) .

Com base em evidências técnicas e padrões de operações, investigações internacionais atribuíram a autoria ao grupo Lazarus, frequentemente associado ao governo norte-coreano. Supõe-se que a motivação tenha relação com a obtenção de divisas estrangeiras, como forma de driblar sanções econômicas impostas ao país (??).

Em resposta ao incidente, a SWIFT lançou o programa Customer Security Programme (CSP), estabelecendo controles obrigatórios de segurança para todas as instituições participantes. Foram implementadas medidas como o Payment Controls Service, capaz de bloquear automaticamente transações atípicas, e o Daily Validation Report, utilizado para detectar divergências entre registros internos e mensagens enviadas pelo SWIFT.

Além disso, criou-se um canal de inteligência colaborativa por meio do SWIFT ISAC, permitindo o compartilhamento anônimo de informações sobre ameaças emergentes. Essas iniciativas fortaleceram a capacidade de detecção e prevenção de ciberataques subsequentes, que passaram a ser interrompidos ainda na fase de preparação (??).

Todo o ocorrido esclarece como a engenharia social, nesse caso representada pelo phishing, pode ser a porta de entrada para crimes altamente estruturados, conforme discutido por ??). A ausência de medidas básicas de proteção, aliada à descoordenação institucional, criou o cenário ideal para uma fraude internacional de grande escala.

5.4 HBGary (2011)

Em fevereiro de 2011, a empresa norte-americana HBGary Federal, contratada por agências governamentais dos Estados Unidos para fornecer serviços de segurança da informação, foi submetida a uma ofensiva coordenada pelo grupo Anonymous.

O episódio foi deflagrado após o CEO da empresa, Aaron Barr, afirmar publicamente que teria identificado membros do coletivo hacktivista Anonymous e que pretendia compartilhar essas informações com o FBI. A declaração foi interpretada como uma afronta direta aos princípios do grupo, que respondeu com uma ofensiva coordenada (??).

Figura 6 – Modelo de seis fases de um ciberataque.

Fonte: ??), adaptado.

Conforme o modelo de seis fases proposto por ??), como representado na Figura 6, a invasão seguiu uma estrutura típica de ataques cibernéticos complexos: (i) Identificação

do alvo, com a definição estratégica da HBGary como objetivo, após a exposição pública feita por seu CEO; (ii) Reconhecimento, baseado no mapeamento da infraestrutura e coleta de informações por meio de varreduras de rede; (iii) Preparação, com a instalação de ferramentas de ataque e elaboração de métodos de infiltração, como phishing e automação de scripts; (iv) Dano, que envolveu a execução da investida, invasão dos sistemas, vazamento de dados e destruição de backups; (v) Resíduo, com manutenção do controle e trocas de mensagens durante a crise; e (vi) Pós-ataque, quando os invasores verificaram os danos e divulgaram o que obtiveram. Esse ciclo evidencia o nível de planejamento e a abordagem sistemática adotada, demonstrando que o ciberataque não foi aleatório, mas sim parte de uma operação estruturada com objetivos bem definidos.

O ataque iniciou-se com a exploração de uma falha de injeção de SQL em um sistema de gerenciamento de conteúdo (Content Management System (CMS), utilizado para editar e administrar sites. O CMS da HBGary era personalizado, encontrava-se desatualizado e sem auditorias, o que facilitou a invasão por meio da manipulação de URLs legítimas (??).

Com o acesso inicial, os invasores encontraram senhas fracas e repetidas, armazenadas com o algoritmo MD5, uma função de hash considerada obsoleta por não aplicar práticas de segurança como salting (adição de dados aleatórios antes da criptografia) ou hashing iterativo (repetição do processo de codificação). A ausência dessas camadas adicionais permitiu que as senhas fossem quebradas com facilidade por meio de rainbow tables (arquivos pré-computados que associam senhas comuns aos seus respectivos valores criptografados). Ao encontrar uma correspondência com os dados armazenados, os ciberinvasores puderam recuperar rapidamente as credenciais originais, viabilizando o acesso a servidores internos, contas administrativas e ao domínio rootkit.com, vinculado à infraestrutura digital da empresa (??).

A invasão foi complementada por técnicas de engenharia social, como o envio de e-mails falsos (phishing) que simulavam comunicações legítimas, e enganaram funcionários, permitindo o escalonamento de privilégios dentro da rede. De posse do controle da infraestrutura, o grupo assumiu o site institucional da empresa, substituindo a página inicial por mensagens de escárnio, e acessou contas corporativas em redes sociais (??).

Posteriormente, os atacantes vazaram mais de 70 mil e-mails corporativos, os quais revelaram comunicações sensíveis com órgãos como a NSA e o FBI, além de propostas internas que envolviam campanhas contra jornalistas, ativistas e sindicatos (????).

A resposta da HBGary foi lenta e desorganizada. A empresa não utilizava autenticação multifator, as redes não eram segmentadas e não havia políticas rigorosas de auditoria ou atualização de sistemas. O ataque se estendeu por vários dias sem qualquer contenção eficaz (??).

As consequências institucionais e econômicas foram severas. O CEO Aaron Barr renunciou ao cargo, a reputação da empresa foi irremediavelmente abalada, contratos governamentais foram cancelados e, meses depois, a HBGary Federal encerrou suas atividades.

O caso ganhou grande repercussão na mídia especializada e acentuou os riscos da terceirização de serviços de segurança digital sem fiscalização adequada, além de indicar como a soberba institucional pode agravar cenários de vulnerabilidade e como práticas negligentes internas podem comprometer até empresas especializadas em cibersegurança (??).

5.5 Dyn (2016)

Em 21 de outubro de 2016, a empresa norte-americana Dyn, uma das principais provedoras de serviços de DNS (Domain Name System), foi atingida por um enorme ataque DDoS. A ciberameaça foi conduzida pela botnet Mirai, composta por aproximadamente 100 mil dispositivos conectados à internet, como câmeras de segurança, roteadores domésticos e outros equipamentos de Internet das Coisas (IoT), comprometidos por falhas básicas de segurança (????). Conforme pode ser visualizado na Figura 7, as regiões mais afetadas se concentraram em partes específicas dos Estados Unidos, com interrupções críticas em áreas como a Costa Leste, Centro-Oeste e o Texas, refletindo o alcance e a gravidade do ataque DDoS.

Figura 7 – Mapa de interrupções de serviço causadas pelo ataque à Dyn em 2016 nos Estados Unidos.

Fonte: ??), adaptado.

O tráfego gerado atingiu picos estimados em 1,2 terabit por segundo (TBps), afetando os servidores DNS da Dyn, responsáveis pela tradução de nomes de domínio (como twitter.com) em endereços IP. Como resultado, empresas como Twitter, Netflix, Amazon, GitHub, Spotify e PayPal enfrentaram interrupções severas em seus serviços, afetando milhões de usuários principalmente na América do Norte (????). Além de interromper o funcionamento de serviços digitais amplamente utilizados, o ataque também causou instabilidade no sistema de roteamento da internet, que é responsável por direcionar o tráfego de dados entre diferentes redes ao redor do mundo. Houve um aumento expressivo nas alterações de rotas durante o incidente, o que gerou atrasos e dificuldades no acesso a diversos sites e sistemas. Embora a capacidade geral da rede global não tenha sido completamente comprometida, a instabilidade contribuiu para ampliar os prejuízos do ataque, afetando o desempenho de empresas que dependiam de conectividade constante (??).

Do ponto de vista técnico, o ataque evidenciou duas fragilidades centrais: a facilidade com que dispositivos IoT inseguros podem ser transformados em ferramentas de ataque em larga escala, e a dependência excessiva de uma única provedora de DNS. Muitas organizações afetadas não utilizavam práticas de redundância, como o multihoming, que consiste em configurar múltiplos provedores DNS para garantir continuidade do serviço em caso de falhas. Após o incidente, apenas 18% dos domínios existentes passaram a adotar esse tipo de estratégia, número considerado baixo diante da dimensão dos prejuízos (??).

O impacto sobre a Dyn foi imediato: ela perdeu cerca de 8% de sua base de clientes logo após o incidente, e aproximadamente 25% dos domínios hospedados migraram para concorrentes, como AWS e Cloudflare, nos meses seguintes. Mesmo que a perda financeira direta não tenha sido divulgado oficialmente, o dano reputacional foi significativo, com diversos clientes relatando perda de confiança na empresa (????) .

A resposta da empresa ao ataque foi considerada rápida e eficaz. Em poucas horas, ela conseguiu restabelecer os serviços essenciais ao empregar sua infraestrutura anycast, redistribuindo o tráfego entre servidores de forma estratégica. Técnicas emergenciais, como filtragem interna, redirecionamento de tráfego e serviços de mitigação foram aplicadas com sucesso (??).

5.6 Colonial pipeline (2021)

Em maio de 2021, a Colonial Pipeline, empresa responsável por operar o maior sistema de oleodutos de combustíveis dos Estados Unidos, enfrentou um ataque de ransomware que paralisou completamente suas atividades.

Figura 8 – Mapa do sistema Colonial Pipeline, com o sistema de dutos, subdutos e pontos de entrega nos finais de semana.

Fonte: ??), adaptado.

A companhia era responsável por cerca de 45% do combustível consumido na Costa Leste, transportando gasolina, diesel e querosene de aviação por mais de 8.800 km de dutos, que interligavam os principais polos de refino da região sul aos centros urbanos do nordeste americano, como é mostrado na Figura 8. A imagem também destaca os principais locais de entrega utilizados nos finais de semana, o que evidencia a criticidade da operação da Colonial Pipeline, que precisava manter sua logística ativa mesmo fora do expediente comercial (????).

A intrusão digital foi atribuída ao grupo DarkSide, conhecido por atuar no modelo de ransomware como serviço (RaaS), no qual ferramentas maliciosas são desenvolvidas e distribuídas a afiliados que executam os ataques. No caso da Colonial, o ponto de entrada foi uma credencial de VPN comprometida e sem autenticação multifator, o que permitiu

o acesso remoto à rede corporativa. Uma vez infiltrados, os criminosos implantaram o ransomware e ameaçaram vaziar dados sensíveis, utilizando a tática de double extortion (Olorunlana; Mohammed, ??, United States Department of Justice, ??).

Figura 9 – Tela de resgate exibida pelo grupo DarkSide para liberação dos sistemas da Colonial Pipeline.

Fonte: ??).

A Figura 9 expõe a mensagem exibida pelos criminosos no momento do ataque, na qual exigiam um pagamento de US\$ 2 milhões como resgate inicial, sob ameaça de dobrar o valor para US\$ 4 milhões, caso o pagamento não fosse efetuado rapidamente.

A paralisação imediata das operações foi uma medida preventiva, já que os sistemas industriais não haviam sido diretamente comprometidos. Ainda assim, os efeitos foram rapidamente sentidos: houve escassez de combustível em diversos estados, aumento de preços e longas filas em postos de gasolina, principalmente na região sudeste dos Estados Unidos. Setores como o transporte aéreo, operações militares e cadeias logísticas hospitalares foram gravemente afetados, evidenciando a dependência crítica da infraestrutura comprometida pela invasão (??).

Para tentar mitigar a crise, a empresa optou por pagar um resgate de US\$ 4,4 milhões em Bitcoin, com o objetivo de acelerar a restauração dos sistemas. No entanto, a ferramenta de descryptografia fornecida pelos criminosos mostrou-se ineficaz, e a Colonial teve que realizar a maior parte da recuperação manualmente (??).

Pouco tempo depois, o FBI e o Departamento de Justiça anunciaram a recuperação de US\$ 2,3 milhões do valor pago, graças a técnicas avançadas de rastreamento de blockchain (tecnologia que permite o registro descentralizado e seguro de transações digitais) e à apreensão de 63,7 bitcoins vinculados ao grupo DarkSide (United States Department of Justice, ??).

A interpretação especializada de todo o ocorrido revelou falhas estruturais na segurança da empresa: ausência de segmentação de rede, políticas de senha frágeis, falta de autenticação robusta e inexistência de um plano eficaz de resposta a incidentes. A decisão de pagar o resgate, contrariando as diretrizes do governo norte-americano, também gerou críticas quanto à preparação estratégica da organização (??).

Como solução ao problema, a Colonial Pipeline iniciou a implementação de uma série de medidas corretivas, incluindo autenticação multifator, arquitetura Zero Trust, segmentação avançada das redes internas e realização de simulações regulares de incidentes.

No âmbito institucional, o ataque impulsionou a criação do Cyber Incident Reporting for Critical Infrastructure Act, que obriga empresas de setores estratégicos a reportarem incidentes cibernéticos de forma mais rápida e estruturada (????). Segundo ??,

p.8),

O ciberataque à Colonial Pipeline foi um divisor de águas que expôs a fragilidade das infraestruturas críticas diante de ameaças cibernéticas sofisticadas. Embora a recuperação técnica e operacional imediata tenha sido louvável, o incidente evidenciou desafios profundamente enraizados, desde a fragmentação de políticas até a limitada prontidão para incidentes e a coordenação tardia (Tradução nossa).

5.7 Resultado da Análise

Esta seção reuniu sete ciberataques de grande repercussão global, selecionados por sua capacidade de evidenciar com clareza as repercussões socioeconômicas geradas por falhas de segurança digital em setores críticos. O Quadro 4 apresenta uma síntese dos principais aspectos de cada ocorrência, organizando os dados de forma comparativa e objetiva, de modo a facilitar a análise entre os casos.

A coluna "Categoria da Ameaça" do quadro traz a técnica ou combinação predominante explorada em cada caso. Em diversos episódios, como no Bangladesh Bank, o ataque não se restringiu a uma única abordagem, mas articulou múltiplas vulnerabilidades, desde engenharia social até malwares diferentes, ampliando a complexidade da resposta e os prejuízos dos envolvidos. As ocorrências descritas apresentam não apenas a variedade de táticas empregadas, mas também a amplitude dos danos causados. Observa-se que as consequências ultrapassam a esfera tecnológica e atingem diretamente a economia, a governança pública e o bem-estar da população.

O destaque do ransomware em pelo menos quatro dos sete exemplos sinaliza sua consolidação como ferramenta recorrente de extorsão digital. Mais do que danos econômicos imediatos, esse tipo de malware coloca em risco a operação de serviços essenciais, a confiança institucional e a segurança nacional.

As consequências variaram desde o bloqueio de processos judiciais (STJ), a paralisação de sistemas de saúde pública (ConecteSUS), até o comprometimento de redes logísticas e de abastecimento energético (Colonial Pipeline). Também se observaram crises reputacionais severas, como no caso da HBGary, e impactos sistêmicos no comércio digital global (Dyn).

Casos adicionais, não explorados em profundidade neste estudo, reforçam ainda mais o impacto dos ciberataques em contextos geopolíticos e informacionais. Um exemplo é o NotPetya, que em 2017 teve como alvo inicial a Ucrânia, mas atingiu empresas como Maersk (logística global), Merck (indústria farmacêutica) e Rosneft (setor energético), com prejuízos globais superiores a US\$ 10 bilhões. Embora se apresentasse como ransomware, o ataque foi destrutivo e atribuído a forças militares russas, demonstrando como conflitos

Quadro 4 – Síntese dos casos.

Ataque	Categoria da Ameaça	Resumo
WannaCry (2017)	Malware (Ransomware + Worm)	Ataque global que explorou falha no Windows e causou prejuízos de US\$ 4 bilhões.
STJ (2020)	Malware (Ransomware)	Paralisou o funcionamento do tribunal e criptografou dados sensíveis.
ConecteSUS (2021)	Malware (Ransomware)	Comprometeu serviços do SUS e suspendeu emissão de certificados.
Bangladesh Bank (2016)	Engenharia Social (Phishing) + Malware (Keylogger + Trojan)	Desvio de US\$ 81 milhões após roubo de credenciais e acesso ao SWIFT.
HBGary (2011)	Engenharia Social (Phishing) + Injeção de SQL	Vazamento de dados e colapso da empresa por falhas técnicas e internas.
Dyn (2016)	DDoS (Botnet via IoT)	Ataque DDoS derrubou grandes serviços online e afetou milhões de usuários.
Colonial Pipeline (2021)	Malware (Ransomware)	Paralisou oleoduto nos EUA, causando escassez e alta nos preços.

Fonte: Elaborado pelo autor.

geopolíticos podem gerar danos colaterais em setores civis essenciais (????). Outro exemplo significativo é o da Cambridge Analytica, já citado na introdução, que expôs os riscos da manipulação algorítmica e da exploração indevida de dados pessoais para fins políticos.

Além da intervenção de agências federais e do pagamento de resgates milionários, os eventos cibernéticos destacados evidenciam a necessidade de respostas organizacionais maduras.

Entre as práticas adotadas ou recomendadas estão: formação de equipes de resposta a incidentes (CSIRTs), uso de autenticação multifator, segmentação de rede, monitoramento contínuo das atividades nos sistemas e aderência a padrões internacionais como a ISO/IEC 27001, o NIST CSF e frameworks de governança da informação. Diversas organizações também passaram a realizar auditorias internas periódicas, revisar a arquitetura de suas redes, migrar sistemas críticos para estruturas mais seguras, implementar criptografia de dados sensíveis e controles de acesso mais rígidos.

Em alguns casos, como o ConecteSUS, houve ainda a criação de comitês gestores de privacidade e a migração de ambientes para instituições públicas com maior capacidade técnica. No caso da Colonial Pipeline, além de adotar a arquitetura Zero Trust, foram iniciadas simulações regulares de resposta a incidentes. Já a SWIFT estruturou serviços de validação automática e criou canais de inteligência colaborativa para detecção precoce de ameaças.

Embora muitas dessas medidas tenham sido implementadas de forma reativa após

os incidentes, elas representam avanços significativos no fortalecimento da postura de segurança das organizações.

A seguir, são apresentadas abordagens fundamentais para a construção de um ambiente digital seguro, com base em recomendações de especialistas e instituições reconhecidas na área da segurança da informação.

5.8 Controles Técnicos e Automação de Defesa

A adoção de controles técnicos robustos é uma das principais estratégias para neutralizar invasões virtuais. Práticas como autenticação multifator, firewalls, segmentação de rede, como visto anteriormente, e listas de permissões de aplicações autorizadas (whitelisting) dificultam significativamente a movimentação lateral de agentes criminosos e reduzem a superfície de ataque.

A inclusão de backups regulares e automatizados, isolados da rede principal, também garante maior resiliência perante ransomwares por exemplo.

De acordo com o United Kington (??), a aplicação eficaz desses controles deve ser complementada por políticas de senhas complexas, desativação de serviços desnecessários e atualização constante de dispositivos.

Soluções integradas e automatizadas de resposta a incidentes também tornam-se essenciais para garantir uma postura de segurança eficaz. Nesse contexto, destaca-se o papel de ferramentas como o SIEM, SOAR e XDR, que atuam de forma complementar na detecção, análise e contenção de agentes maliciosos. O Quadro 5 compara as funcionalidades de cada uma dessas ferramentas.

Quadro 5 – Comparação entre as ferramentas SIEM, SOAR e XDR.

SIEM	SOAR	XDR
Coleta, agrega e analisa dados de eventos de várias fontes	Analisa e prioriza dados de eventos para acionar respostas automatizadas	Coleta e analisa dados de eventos de múltiplos pontos da infraestrutura de TI
Usa IA para estabelecer uma linha de base dos dados para análise	Baseia-se nos dados dos eventos para acelerar o processo de resposta a incidentes	Correlaciona todos os dados para análise e seleção de resposta
Os dados coletados podem ser usados pelo SOAR para uma resposta mais eficaz	Usa os dados do SIEM em uma resposta automatizada	Lida com todas as etapas do processo, desde a coleta e análise dos dados até a resposta ao evento

Fonte: ??), adaptado.

O Security Information and Event Management (SIEM) atua como ponto inicial, sendo responsável por coletar, agregar e analisar grandes volumes de informações provenientes de diferentes fontes da infraestrutura de TI. Ele utiliza inteligência artificial

para estabelecer uma linha de base e identificar comportamentos anômalos, além de gerar alertas que podem ser aproveitados por outras ferramentas (??).

Já o Security Orchestration, Automation and Response (SOAR) entra em cena para acelerar o processo de resposta. Ele integra diversas ferramentas de segurança, orquestrando e automatizando fluxos de trabalho a partir dos dados recebidos do SIEM. Isso reduz significativamente o tempo de resposta e a carga operacional sobre as equipes de segurança, permitindo que falhas eventuais sejam tratadas de forma padronizada e eficiente (??).

Por fim, o Extended Detection and Response (XDR) amplia a visibilidade da organização ao coletar e correlacionar dados de múltiplas camadas, como endpoints, redes e ambientes em nuvem, com o objetivo de identificar comportamentos suspeitos complexos e investidas multivetoriais. Com apoio de machine learning e análise avançada, o XDR consegue automatizar tanto a detecção quanto a resposta a essas suspeitas, lidando com todas as etapas do processo de forma integrada (??).

Figura 10 – Integração entre SIEM, SOAR e XDR na resposta a incidentes.

Fonte: ??), adaptado.

A Figura 10 representa de forma esquemática como essas três soluções se articulam em uma cadeia de resposta coordenada. O SIEM capta os dados iniciais da ameaça em questão, que são repassados ao SOAR para orquestração e automação da resposta. O XDR, por sua vez, coleta informações adicionais e realiza ações mitigatórias baseadas na correlação dos eventos detectados.

O ataque à Colonial Pipeline expôs a importância de estratégias estruturadas, pois as falhas de autenticação e a ausência de segmentação facilitaram o comprometimento da rede corporativa.

5.9 Conscientização e Cultura de Segurança

Grande parte dos ataques bem-sucedidos explora fragilidades humanas. O chamado fator humano representa um elemento importante na superfície de exposição das organizações, sendo um vetor recorrente de disseminação de ameaças quando não é adequadamente considerado nas estratégias de segurança. A educação contínua dos colaboradores, portanto, é uma das estratégias mais custo-efetivas para sua minimização, além de representar um investimento essencial na construção de uma cultura organizacional resiliente.

Segundo o Government of Canada (??), ações educativas devem incluir: (i) Treinamentos periódicos sobre phishing e engenharia social; (ii) Simulações controladas de ciberataques para testar o preparo dos usuários; e (iii) Campanhas de sensibilização e canais de denúncia internos. Além dessas medidas, outras práticas também integram a construção de uma cultura mais preparada, tais como o uso de passphrases (frases longas

e de fácil memorização compostas por múltiplas palavras) em substituição a senhas curtas e previsíveis; o bloqueio de conexões inseguras, como redes Wi-Fi públicas ou dispositivos não autorizados conectados à rede corporativa, e a limitação do uso de dispositivos pessoais em redes institucionais, reduzindo pontos de entrada para malwares e vazamento de dados.

No caso do Bangladesh Bank, a engenharia social por meio de e-mails de phishing foi o ponto de partida para a fraude multimilionária. A ausência de treinamentos e políticas de verificação levou à instalação de malwares e ao roubo de credenciais. Isso aponta como medidas básicas de conscientização poderiam ter evitado ou ao menos atrasado a operação criminosa.

De maneira semelhante, no ataque à HBGary, o sucesso da ofensiva também envolveu táticas de phishing contra funcionários e senhas fracas, expondo a falta de zelo da própria empresa de segurança diante de boas práticas que ela recomendava a seus clientes.

5.10 Resposta a Incidentes e Recuperação

Mesmo em ambientes altamente protegidos, a possibilidade de uma invasão cibernética não pode ser descartada. Por isso, como destaca a ??), é essencial dispor de um Plano de Resposta a Incidentes (PRI), com ações coordenadas desde a detecção inicial até a recuperação dos sistemas.

Esse plano deve contemplar: (i) definição clara de papéis e responsabilidades; (ii) criação de um CSIRT (Computer Security Incident Response Team), com equipe capacitada para conter e investigar ocorrências (Araujo e Rossi, 2020); (iii) procedimentos formais para comunicação com autoridades, reguladores e stakeholders (clientes, parceiros e colaboradores) afetados; e (iv) a existência de um Plano de Continuidade de Negócios (PCN), com backups isolados, rotinas de testes e cenários simulados, aumenta significativamente a capacidade de recuperação após violações.

Nesse contexto, a norma ISO/IEC 27035 descreve um modelo estruturado de gerenciamento de incidentes, dividido em cinco fases: preparação, identificação, avaliação, resposta e aprendizagem. Essas diretrizes fornecem uma abordagem sistemática e adaptável, voltada tanto para a contenção dos impactos quanto para a melhoria contínua do processo de segurança da informação (??).

A ausência de um plano estruturado foi evidente no caso do ConecteSUS. Por outro lado, a resposta rápida da Dyn, diante de um massivo ataque DDoS, mostrou a importância de um plano eficaz.

6 Conclusão

O presente trabalho se debruçou sobre as vulnerabilidades no meio digital, destacando não apenas sua relevância nos dias atuais, mas, sobretudo, como alteraram negativamente a sociedade e as respostas institucionais adotadas diante delas.

A partir da análise de diferentes episódios que afetaram organizações em abrangência territorial e setorial, foi possível observar como a segurança da informação se tornou um elemento crítico para a sustentabilidade das operações em setores vitais da sociedade.

A pesquisa contemplou exemplos vivenciados por organizações, como o ataque do ransomware WannaCry (2017), além de incidentes menos abordados na literatura especializada. Essa variedade de exemplos possibilitou a identificação de diferentes categorias de ameaças, incluindo ataques por ransomware, DDoS, falhas humanas e manipulações em infraestruturas críticas. Também permitiu analisar as consequências econômicas e sociais enfrentadas por organizações de diversos setores e regiões.

A análise revelou padrões recorrentes de vulnerabilidade, como ausência de autenticação multifator, falhas de configuração, baixa maturidade organizacional em segurança e respostas tardias. Por outro lado, também foram identificadas boas práticas de mitigação após as invasões, como resposta coordenada a incidentes, reforço de políticas de segurança, uso de backups e colaboração com autoridades especializadas. Tais elementos reforçam a importância de ações preventivas baseadas em gestão de riscos, conscientização interna e alinhamento estratégico entre TI e os demais setores institucionais.

Este estudo contribui para a área de segurança da informação ao reunir, em uma abordagem comparativa, os principais aprendizados de eventos que transcenderam o ambiente digital e provocaram efeitos no cotidiano das populações. Ao apresentar um panorama crítico das falhas e acertos observados nos acontecimentos analisados, o trabalho visa fomentar uma cultura de cibersegurança mais sólida, tanto no setor público quanto no privado.

Entre as principais contribuições está a proposta de disseminar conhecimentos práticos sobre ciberataques e suas consequências, servindo como material de apoio para profissionais qualificados e o leitor casual. A escolha por estudar casos menos difundidos também ampliou o escopo da reflexão, permitindo observar diferentes vulnerabilidades, inclusive as que afetam organizações especializadas em segurança da informação.

Como limitações do trabalho, destaca-se a dificuldade de acesso a dados técnicos completos em alguns dos episódios observados no estudo, especialmente em incidentes com informações sigilosas ou restritas. Além disso, a constante evolução das ciberameaças exige atualizações frequentes dos métodos de defesa, o que pode tornar certas medidas rapidamente obsoletas.

Para pesquisas futuras, recomenda-se a análise de ciberataques mais recentes, a inclusão de entrevistas com especialistas em segurança e o aprofundamento sobre o papel da legislação nacional na prevenção e responsabilização de crimes virtuais. A construção de indicadores para mensurar as consequências sociais de tais eventos também pode ser uma valiosa linha de investigação.

Este trabalho reforça que investir em segurança da informação não é mais uma opção, mas uma necessidade estratégica e contínua, fundamental para garantir a tenacidade organizacional e preservar os ativos mais valiosos de uma instituição: seus dados e sua reputação.