Fundação Universidade Federal do ABC
Pró reitoria de pesquisa
Av. dos Estados, 5001, Santa Terezinha, Santo André/SP CEP: 09210-580
Bloco L, 3º Andar, Fone (11) 3356-7617
iniciacao@ufabc.edu.br

Santo André, 21 de abril de 2026.

À Pró-Reitoria de Pesquisa (PROPES)

Prezados(as) Senhores(as),

Apresentamos o relatório das atividades desenvolvidas no período de 01/04/2025 a 21/04/2026, referentes ao estágio pós-doutoral do pesquisador **Fretz Sievers Junior**, vinculado ao Programa de Pesquisador Colaborador (PC/UFABC), projeto **PIE1458-2025 (CECS)**, sob supervisão do **Prof. Dr. Mario Alexandre Gazziro**.

É com satisfação que destacamos as realizações do **Laboratório de Computação Forense da UFABC**, o qual tem oferecido contribuições significativas à sociedade e à academia. Destacam-se, no âmbito da Computação Forense, as atuações em casos jurídicos de relevância e repercussão nacional.

Atenciosamente,

_____	_____
Dr. Fretz Sievers Junior	Dr. Mário Alexandre Gazziro
Pesquisador Colaborador	Supervisor do Estágio Pós Doutoral
Docente Externo	Laboratório de Computação Forense

UFABC	UFABC – UNIVERSIDADE FEDERAL DO ABC

RELATÓRIO CONSOLIDADO DE ATIVIDADES

PIE1458-2025

FRETZ SIEVERS JUNIOR

Programa de Pós-Doutorado em Computação Forense

Linha de Pesquisa: Computação Forense.

Supervisor: Prof. Dr. Mario Alexandre Gazziro

Endereço Eletrônico do Curriculum Lattes:

http://lattes.cnpq.br/8821398582307961

TÍTULO: O ESTADO DA ARTE DAS FERRAMENTAS UTILIZADAS PARA COMPUTAÇÃO FORENSE E OS TIPOS DE ATAQUES EM SISTEMAS DIGITAIS

TITLE: THE STATE OF THE ART OF TOOLS USED FOR COMPUTER FORENSICS AND TYPES OF ATTACKS ON DIGITAL SYSTEMS

Relatório Final encaminhado à UFABC –como requisito parcial para obtenção do certificado de estágio Pós-Doutorado em Computação Forenses.

Versão 3.0

São Paulo

2026

RESUMO

A computação forense desempenha um papel crucial no combate aos crimes digitais, que se tornaram cada vez mais frequentes e sofisticados na Sociedade 4.0 utilizando cada vez mais as redes de computadores e sistemas de informação com o uso da Inteligência Artificial. Quando há indícios de crimes e fraudes, se faz necessário o levantamento de provas em sistemas digitais, visando elucidar os fatos para entender o que aconteceu para a instrução de procedimentos seja na esfera civil, administrativo ou criminal, possibilitando a produção de provas e a análise de evidências digitais de forma segura e legalmente admissível. Isso inclui a recuperação de dados excluídos, análise de logs de sistemas, rastreamento de atividades online e identificação de dispositivos utilizados em crimes. As pesquisas realizadas concentram em ferramentas específicas o que traz uma lacuna referente a qualidade das ferramentas comparadas a outras e para que casos uma determinada ferramenta e mais eficiente que a outra, com essa lacuna identificada, falta na literatura uma análise quantitativa e qualitativa das ferramentas de computação forense e sua aplicabilidade, propiciando provas para o combate de crimes digitais o que apresentam uma ameaça para a sociedade moderna.

Palavras-chave: computação forense, perícia forense, produção de provas digitais, vulnerabilidades, crimes digitais, LGPD.

ABSTRACT

Forensic computing plays a crucial role in combating digital crimes, which have become increasingly frequent and sophisticated in Society 4.0, increasingly using computer networks and information systems with the use of Artificial Intelligence. When there are reports of crimes and fraud, it is necessary to collect evidence in digital systems. This elucidates the facts to understand what happened for the instruction of procedures, whether in the civil, administrative or criminal sphere, enabling the production of evidence and the analysis of digital evidence in a safe and legally admissible manner. This includes recovering deleted data, analyzing system logs, tracking online activities and identifying devices used in crimes. The research carried out has focused on specific tools, which creates a gap regarding the quality of the tools compared to others and in which cases a particular tool is more efficient than another. With this gap identified, the literature lacks a quantitative and qualitative analysis of forensic computing tools and their applicability, providing evidence for combating digital crimes, which pose a threat to modern society.

Keywords: Computer Forensics, Forensic Expertise, production of digital evidence, vulnerabilities

SUMÁRIO

Lista de Figuras

I. Identificação

a) Do pesquisador

As atividades de pesquisa foram conduzidas por Fretz Sievers Junior, cujo perfil acadêmico e profissional integra competências multidisciplinares fundamentais à computação forense contemporânea.

Qualificações: Doutor em Engenharia de Computação e Eletrônica, possui graduação em Engenharia (da Computação, Civil, de Produção e Elétrica), Engenharia de Segurança do Trabalho, Ciências Contábeis e Direito, além de ser Mestre em Direito. Sua atuação destaca-se pela convergência entre Engenharia, Ciência da Computação e Direito, com ênfase em Perícia Computacional Forense, Cibersegurança e Direito Digital. Instrutor da multinacional Cisco em tecnologia de Redes de Computadores.

Vínculo Profissional: Professor do Centro Paula Souza há aproximadamente 17 anos, ocupa atualmente dois cargos públicos de docente. Leciona nos cursos de:

- Informática para Negócios: Sistemas Operacionais, Redes de Computadores e Linguagem de Programação III.
- Logística: Simulação em Logística.
- Desenvolvimento de Software Multiplataforma: Sistemas Operacionais, Redes, Algoritmos, Estrutura de Dados e Técnicas de Programação I.
- Análise e Desenvolvimento de Sistemas: Engenharia de Software III e Estrutura de Dados.

Além da docência, atua em consultoria empresarial e treinamentos especializados.

Supervisão: O pesquisador desenvolveu suas atividades sob supervisão do Prof. Dr. Mário Alexandre Gazziro, junto ao Programa de Engenharia da Informação do Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas (CECS).

b) Do escopo do projeto de pesquisa (PIE1458-2025)

O estágio pós-doutorado está formalmente vinculado ao projeto de pesquisa cadastrado no SIGAA sob o código PIE 1458-2025 na PROPES.

Título: O ESTADO DA ARTE DAS FERRAMENTAS UTILIZADAS PARA COMPUTAÇÃO FORENSE E OS TIPOS DE ATAQUES EM SISTEMAS DIGITAIS.

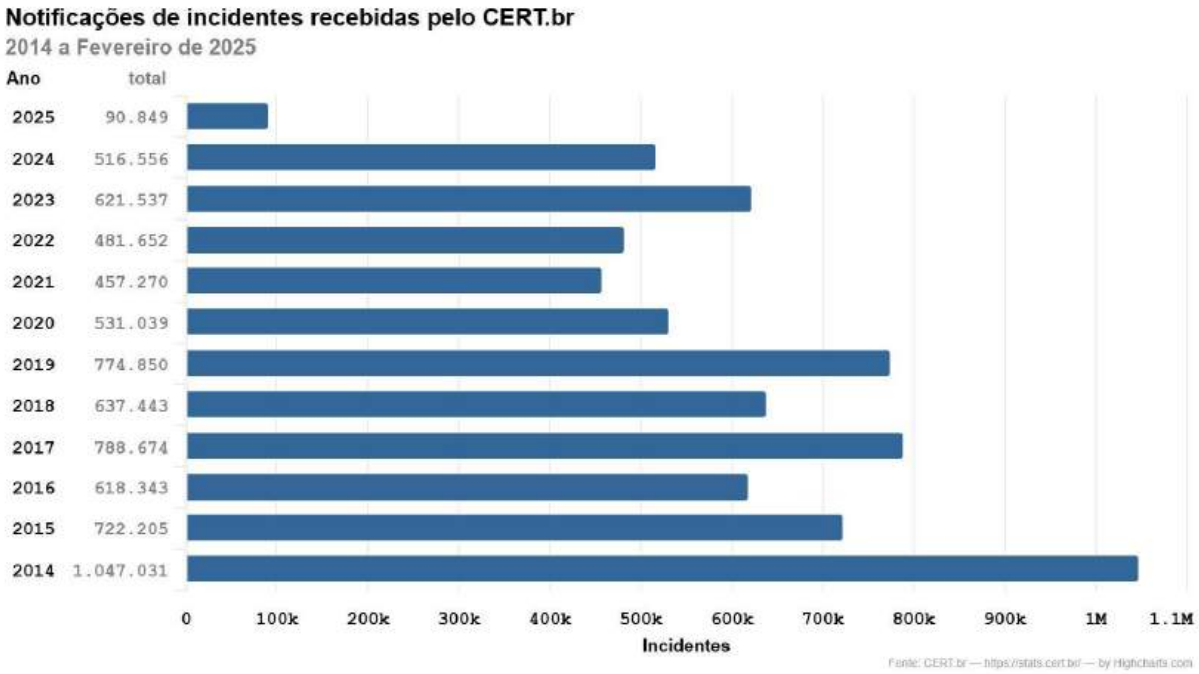
II. Introdução

Com as inovações tecnologias dos últimos anos, nasce a sociedade da informação com acesso à rede mundial de computadores, com diferentes tipos de sistemas de informação, oferecendo produtos e serviços diversificados nas mais diversas áreas tais como: saúde, educação, comércio eletrônico, negócios, bancos, dinheiro eletrônico, entre outras. Com a possibilidade de ganhar dinheiro fácil, pessoas más intencionadas, tentam práticas atos ilícitos visando conseguir vantagens financeiras explorando vulnerabilidades existentes nos sistemas e causando prejuízo tanto para pessoas físicas como jurídicas, através de furto de valores financeiros, ou mesmo sequestro de dados impossibilitando que as empresas executem sua atividade econômica gerando inúmeros prejuízos. A computação forense exige um estudo permanente e aprofundado de muitos aspectos da informática, sendo necessário um acompanhamento constante, tanto das tecnologias envolvidas quanto das técnicas mais utilizadas nos crimes eletrônicos e suas inovações tecnologias.

Segundo o CERT.br[1] (2025), a quantidade de incidentes reportados em 2014 foi de 1.014.031 contra 516.556 do ano de 2024, havendo uma queda de aproximadamente 50%, porém os números são altos e com o avanço da tecnologia novos crimes podem surgir. Na Figura 1 pode-se acompanhar a evolução dos incidentes ao longo dos anos, os quais demonstram que existem muitas ameaças relacionadas a problemas de segurança de informação estão a cada dia mais presentes, gerando demandas que precisam ser investigadas pela computação forense, possibilitando conhecer as sua origem e a motivação e como evitar os problemas investigados. O gráfico apresenta que os incidentes durante os 10 anos (2014 a 2024) houve uma variação, na quantidade de incidentes, com uma média de 654.236 incidentes, confirmando a quantidade alta de incidentes reportados.

[1] CERT – Centro de Estudo, Resposta a Tratamento de Incidentes de Segurança no Brasil, disponível em: https://stats.cert.br/incidentes/, acessado em 03/04/2025.

Figura 1 – Incidentes reportados



Fonte: (CERT,2025)

III. Descrição dos objetivos da pesquisa.

Abaixo são apresentados os objetivos gerais e específicos da pesquisa.

a) Objetivo Geral.

Realizar uma pesquisa sobre os tipos de ferramentas de computação forense estão sendo utilizadas e realizar uma classificação referente aos tipos de incidentes e quais ferramentas podem ser usadas para a produção de provas materiais.

b) Objetivos específicos.

Fazer uma análise quantitativa e qualitativa sobre as ferramentas utilizadas e quando uma ferramenta pode ser utilizada com uma outra para a produção de provas e verificar qual o nível de eficiência da ferramenta.

c) Enunciado do Problema

O problema considerado nesta pesquisa consiste em analisar um conjunto de ferramentas aplicada na computação forense, visando a produção de artefatos que possam ser utilizados como provas e seu nível de eficiência.

d) Hipótese da Solução Escolhida

Fazer um levantamento bibliográfico das principais ferramentas de software livre utilizadas e para quais casos são aplicados.

IV. Metodologia

A metodologia da pesquisa consiste em uma busca bibliográfica utilizando bases indexadas dos trabalhos publicados entre os anos de 2015 à 2025 com as seguintes palavras chaves: “Computação Forense”, “Perícia Forense”, “Provas digitais” e “*CyberSecurity*” e realizando uma revisão sistemática da literatura sobre computação forense, verificando quais são as ferramentas utilizadas para cada caso em específico.

V. Cronograma de atividades

Conforme detalhado no cronograma Figura 2, apresenta-se a seguir o cumprimento das atividades executadas:

1. **Análise de requisitos da pesquisa:** Com base na revisão bibliográfica e nas demandas do laboratório forense da UFABC, foram levantados os requisitos necessários para a elaboração do relatório final e das publicações acadêmicas, visando atender plenamente às necessidades da instituição.
2. **Levantamento de softwares de computação forense:** Por meio de pesquisa bibliográfica, foram catalogados os tipos de ataques recorrentes e os respectivos *softwares* utilizados para análise forense, subsidiando as demandas surgidas no laboratório e as lacunas identificadas na literatura.
3. **Análise comparativa qualitativa e quantitativa:** Após o mapeamento dos tipos de ataques, realizou-se uma análise comparativa (qualitativa e quantitativa) das ferramentas selecionadas, verificando sua eficácia e aplicabilidade técnica.
4. **Aplicação das ferramentas em demandas forenses laboratoriais:** Os casos encaminhados mensalmente pela imprensa foram analisados e discutidos junto ao grupo de pesquisa do laboratório, visando formular hipóteses e soluções técnicas para os incidentes em tela.
5. **Verificação e validação dos sistemas analisados:** Após a análise das necessidades investigativas de cada caso concreto, o pesquisador validou a eficácia dos métodos empregados, assegurando a robustez necessária para a produção de provas passíveis de utilização em demandas judiciais.
6. **Elaboração e submissão de produção acadêmica:** Foi publicado o artigo intitulado **“Responsabilidade Civil nas Instituições Financeiras na Sociedade 4.0 e a Gestão de Risco na era digital”** na *Revista de Direito Bancário e do Mercado de Capitais* (Apêndice I). Adicionalmente, o capítulo **“O**

(não) combate à falsificação na era digital no Brasil quanto à defesa das pessoas físicas na atualidade" foi aprovado para publicação nos anais do *I Simpósio do Conectajur* (Apêndice II).

7. **Escrita do relatório final:** Concluídas as atividades junto à supervisão e ao Laboratório Forense da UFABC, procedeu-se à redação do relatório final. O documento visa consolidar o cumprimento do plano de trabalho estabelecido na proposta inicial do estágio pós-doutoral.

Figura 2 – Cronograma das atividades executadas

Atividades serem executadas	abr/25	mai/25	jun/25	jul/25	ago/25	set/25	out/25	nov/25	dez/25	jan/26	fev/26	mar/26	abr/26
1. Análise dos requisitos da pesquisa	■												
2.Levantamento dos softwares de computação forense		■											
3. Realizar analise comparativa qualitativa e quantitativa dos softwares escolhidos referente a computação forense			■										
4.Uso e aplicação das ferramentas nos caso de demanda forenses do Laboratório (Recebidos mensalmente por demanda de imprensa)				■	■								
5. Validação dos sistemas analisados.						■	■	■					
6. Elaboração e submissão de artigos									■				
7. Escrita do relatório final										■	■	■	■

Fonte: (do Autor)

VI. Resultados e Discussão

Esta seção dedica-se à apresentação e à discussão dos resultados obtidos, estruturadas em subcapítulos que detalham os achados da pesquisa sob diferentes perspectivas técnicas.

a) Pesquisa de tipos de ataques durante o estágio de pós-doutoramento

A incidência de ataques digitais apresenta um crescimento contínuo, impulsionada tanto pela descoberta de novas vulnerabilidades em redes de computadores quanto pela desinformação dos usuários diante do célere avanço tecnológico e da Inteligência Artificial. Soma-se a esse cenário a limitação do Estado em manter um efetivo de investigação especializado que atue estritamente sob o rigor legal. A dificuldade em conciliar a celeridade investigativa com a garantia constitucional do contraditório e da ampla defesa, aliada à carência de recursos estatais, acaba por favorecer a impunidade e, consequentemente, o aumento exponencial do número de vítimas.

As soluções de segurança fundamentam-se no modelo OSI, uma arquitetura de referência que, conforme ensina Forouzan (2013), serviu de base para a implementação do modelo TCP/IP. A estruturação em camadas permite orientar

estrategicamente a aplicação de controles de segurança, possibilitando a visualização de um cenário complexo no qual cada nível apresenta vulnerabilidades específicas. É importante notar que o modelo TCP/IP, em sua concepção original, priorizou a comunicação e a interoperabilidade, relegando a segurança a um segundo plano, visto que a proteção de dados não era uma preocupação crítica na época. Com o passar do tempo, à medida que a informação se tornou um ativo estratégico, a implementação de sistemas de criptografia e outros mecanismos de proteção tornou-se essencial. A Figura 3 ilustra o modelo OSI, composto por sete camadas: Física (1), Enlace de Dados (2), Rede (3), Transporte (4), Sessão (5), Apresentação (6) e Aplicação (7). A figura apresenta, ainda, a correspondência com o modelo TCP/IP atualizado, estruturado em cinco camadas: Física (1), Enlace de Dados (2), Rede (3), Transporte (4) e Aplicação (5).

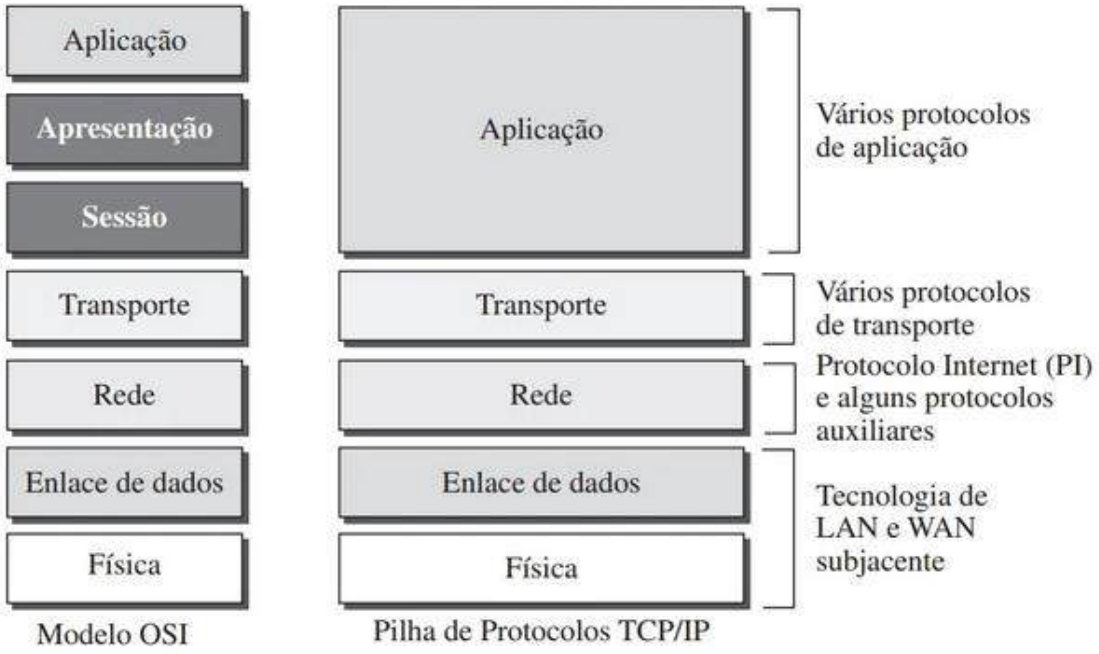
Diferente do modelo OSI, que é um padrão formal da ISO, o modelo TCP/IP evolui por meio de RFCs (*Request for Comments*). Não existe um único documento que decrete um "novo modelo", mas sim um consenso evolutivo baseado em registros fundamentais. A RFC 1122 (*Requirements for Internet Hosts -- Communication Layers*) [2] é a referência clássica que define as quatro camadas originais: Aplicação, Transporte, Internet e Link (Acesso à Rede). O modelo de cinco camadas, adotado atualmente como padrão didático e prático, não é definido por uma RFC que substitua a 1122, mas decorre da necessidade técnica de dissociar o hardware (Camada Física) do protocolo de controle de acesso (Camada de Enlace), como o Ethernet.

Quanto às atualizações mais recentes sobre o tráfego de dados nessas camadas, destacam-se a RFC 9293 (2022), considerada a mais relevante para a Camada de Transporte por consolidar e substituir a histórica RFC 793 do TCP, incorporando décadas de aprimoramentos. Complementarmente, a RFC 9110 (2022) estabelece a atualização fundamental para a Camada de Aplicação (HTTP). Em suma, enquanto a RFC 1122 estabelece a base histórica, a literatura moderna, como Forouzan (2013), adota o modelo de cinco camadas para fins de interoperabilidade com o modelo OSI, e a RFC 9293 representa a modernização definitiva do controle de transmissão nessas camadas. O modelo OSI é utilizado como a arquitetura

[2] INTERNET ENGINEERING TASK FORCE (IETF). **RFC 1122**: Requirements for Internet Hosts -- Communication Layers. Editado por Robert Braden. [S. l.]: IETF, out. 1989. Disponível em: https://datatracker.ietf.org/doc/html/rfc1122. Acesso em: 21 abr. 2026.

fundamental para referenciar a atuação dos dispositivos de segurança, sejam eles implementados em hardware ou software.

Figura 3 – Modelo OSI e TCP-IP



Fonte: Fourlan (2013)

Nesta seção, são apresentados os tipos de ataques mais comuns em golpes digitais. O gráfico da Figura 4, conforme dados do Cert.br (2025), destaca o elevado volume de incidentes do tipo scan que, segundo De Carvalho Bertoli (2020), consistem na identificação de serviços ativos e no mapeamento de vulnerabilidades em redes de computadores. Essa técnica é amplamente utilizada por permitir que o invasor descubra as aplicações em uso e identifique falhas exploráveis. Sob a ótica da computação forense, a investigação desses vetores fornece informações cruciais sobre a gênese e o comportamento de diversos incidentes de segurança. Dentre os ataques de reconhecimento, destacam-se o *Port Scanning*, utilizado para identificar portas e serviços abertos em um servidor, e o *Packet Sniffing*, que consiste na interceptação de pacotes em trânsito para capturar informações em texto claro, como credenciais não criptografadas. Scan é uma técnica na qual o hacker busca identificar computadores e aplicações disponibilizadas por eles. A ideia do scanning e identificar alvos e serviços vulneráveis que podem ser explorados.

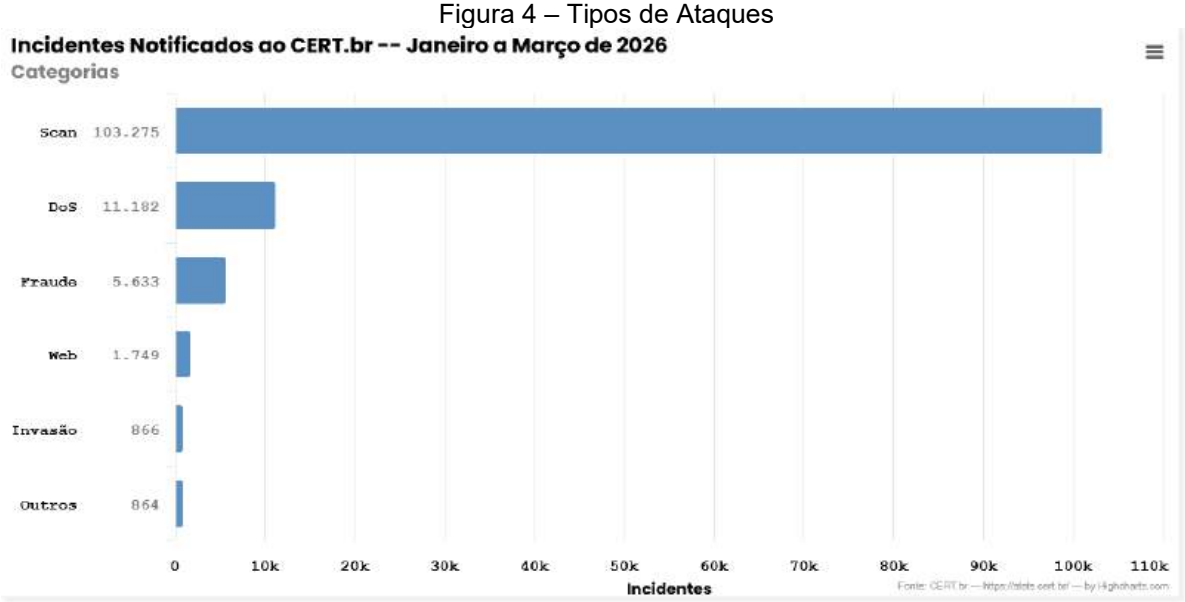
Uma das estratégias fundamentais para mitigar esses ataques é a atuação de um profissional que realize a análise contínua das portas ativas em *endpoints*

(estações de trabalho, servidores, dispositivos móveis e de IoT). Além do monitoramento da integridade dos softwares instalados — incluindo sistemas operacionais e *firmwares* de ativos de infraestrutura, como roteadores e *switches* —, é imprescindível a gestão diligente de vulnerabilidades e a aplicação sistemática de atualizações de segurança (*patch management*). Contudo, a eficácia dessas ações depende da implementação rigorosa de políticas de segurança da informação. Tais diretrizes permitem a redução progressiva das brechas de segurança, garantindo uma proteção mais robusta e efetiva dos ativos digitais ao longo do tempo.

Os ataques de reconhecimento ocupam o primeiro lugar na estatística de incidentes, visto que representam a fase inicial e obrigatória em que o invasor mapeia as tecnologias utilizadas no alvo. O objetivo é realizar um levantamento das vulnerabilidades passíveis de exploração, permitindo um planejamento estratégico que maximize as chances de sucesso da intrusão. Essa modalidade de ataque fornece informações críticas sobre a superfície de exposição da rede, servindo como base para a execução de procedimentos subsequentes de invasão e comprometimento de sistemas.

Os ataques de Negação de Serviço, ou DoS (*Denial of Service*), ocupam a segunda posição na lista de incidentes. O objetivo central dessa modalidade é interromper a disponibilidade de um recurso, impedindo o acesso de usuários legítimos. Machado (2023) ressalta a profunda dependência contemporânea de serviços conectados à internet, o que torna a garantia de disponibilidade um pilar essencial da segurança cibernética. Contudo, ativos expostos a usuários autênticos tornam-se, simultaneamente, alvos acessíveis a agentes maliciosos. Diante de ataques cada vez mais frequentes e sofisticados, este estudo demonstra a relativa simplicidade na execução de um DoS, evidenciando que mesmo *firewalls* com defesas ativas podem enfrentar dificuldades de mitigação, especialmente quando operam apenas com configurações padrão. Nesse sentido, faz-se necessária a realização de testes intrusivos, como o Pentest, que permite validar se os ativos de cibersegurança estão configurados para prover a proteção necessária. Somada à atualização constante e ao monitoramento, essa prática visa robustecer os sistemas de defesa, mitigando os riscos de indisponibilidade e os consequentes prejuízos financeiros e operacionais para a organização.

Figura 4 – Tipos de Ataques



Fonte: (Cert.br, 2026)

O ataque dos (*Denial of Service*), ou Negação de Serviço, tem como objetivo principal exaurir os recursos de um sistema para tornar seus serviços indisponíveis aos usuários legítimos. Quando essa ação é executada de forma coordenada por um conjunto de computadores distribuídos, geralmente infectados e controlados remotamente (botnets), o ataque é classificado como DDoS (*Distributed Denial of Service*). Em ambos os casos, a finalidade é interromper a continuidade operacional do alvo, sobrecarregando sua capacidade de processamento ou largura de banda.

Para mitigar ataques de DoS (*Denial of Service*) e sua variante distribuída (DDoS), é imperativo adotar uma estratégia de defesa em camadas, integrando hardware, software e serviços de rede. Entre as ferramentas fundamentais, destacam-se os Firewalls de Próxima Geração (NGFW - *Next-Generation Firewall*). Diferente das soluções tradicionais, os NGFWs realizam a inspeção profunda de pacotes (*Deep Packet Inspection*) até a Camada de Aplicação (Camada 7 do modelo OSI), o que lhes permite identificar padrões de tráfego anômalos e bloquear endereços IP que realizem requisições excessivas. Exemplos consolidados no mercado incluem as soluções Fortinet FortiGate[3] e Cisco Firepower[4], que são ferramentas pagas.

[3] ARMANI TECHNOLOGY. **Firewall FortiGate para Empresas**: conheça a solução Fortinet. [S. l.], 2026. Disponível em: https://armanitechnology.com.br/firewall-fortigate-para-empresas/. Acesso em: 21 abr. 2026.
[4] CISCO. **Cisco Firepower 1000 Series**: NGFW for small to medium-sized businesses. San Jose: Cisco Systems, 2026. Disponível em: https://www.cisco.com/site/us/en/products/security/firewalls/firepower-1000-series/index.html. Acesso em: 21 abr. 2026.

Considerando as ferramentas instaláveis, são ideais para o seu ambiente corporativo as seguintes soluções de software livre como o Snort (Suricata)[5], sendo considerado um sistema de prevenção de intrusão (IPS) de código aberto. Pode ser configurado por regras específicas para identificar e descartar pacotes que apresentem padrões de ataques dos (como o *SYN Flood*).

Conforme ensina Carvalho (2020), o ataque *SYN Flood* é uma das formas mais clássicas e eficazes de ataque de Negação de Serviço (*DoS*), que atua na Camada 4 (Transporte) do modelo OSI. Ele explora o funcionamento do protocolo TCP, especificamente a etapa de estabelecimento de conexão conhecida como *Three-Way Handshake* (Aperto de Mão de Três Vias), funcionando da seguinte forma:

1. SYN (Sincronizar): O cliente envia um pacote solicitando uma conexão.
2. SYN-ACK (Sincronizar-Agradecer): O servidor responde aceitando o pedido e reserva um espaço na memória para essa conexão.
3. ACK (Agradecer): O cliente confirma o recebimento e a conexão é estabelecida.

No mecanismo do Ataque SYN Flood, o ataque, o invasor subvertem esse processo:

1. O atacante envia uma rajada massiva de pacotes SYN para o alvo, muitas vezes utilizando endereços de IP falsificados (*spoofing*).
2. O servidor, agindo corretamente, responde a cada um com um SYN-ACK e deixa a conexão em estado "meio-aberto" (*half-open*), aguardando o último passo (ACK).
3. O atacante nunca envia o ACK final.
4. O servidor fica com sua "tabela de conexões" lotada, aguardando confirmações que nunca virão. Quando a memória ou os recursos destinados a essas conexões se esgotam, o servidor para de aceitar novas conexões de usuários legítimos, resultando na indisponibilidade do serviço.

Para evitar que um servidor caia devido a um SYN Flood, utilizam-se técnicas como: SYN Cookies**,** neste caso o servidor não reserva memória imediatamente. Ele envia o SYN-ACK com um "número de sequência" especial e só aloca recursos se receber o ACK de volta com esse número validado. Reciclagem de Conexões Meio-Abertas**:** Configurar o sistema operacional para descartar conexões pendentes em um

[5] SNORT. **Snort**: the world's foremost open source intrusion prevention system. [S. l.]: Snort, 2026. Disponível em: https://www.snort.org/. Acesso em: 21 abr. 2026.

curto espaço de tempo. O Firewalls e IPS são dispositivos que identificam o volume anormal de pacotes SYN de uma mesma origem e bloqueiam o tráfego antes que chegue ao servidor final. Embora eficazes, tais técnicas muitas vezes vêm desativadas ou mal configuradas nos sistemas operacionais convencionais, exigindo a intervenção de um especialista em segurança para sua correta implementação.

Em uma investigação forense, o ataque SYN Flood é identificado por meio da análise de *logs* ou do tráfego de rede capturado (arquivos PCAP). O perito observará um volume massivo de conexões com o status SYN_RECV (solicitação recebida e aguardando confirmação), indicando conexões incompletas que congestionam o sistema. Frequentemente, nota-se que os endereços IP de origem são aleatórios ou inexistentes — técnica conhecida como *IP Spoofing* —, o que evidencia o uso de métodos de ocultação pelo agressor. Esse cenário exemplifica porque as configurações padrão de fábrica são vulneráveis, uma vez que a maioria dos sistemas operacionais possui limites reduzidos para conexões simultâneas, tornando o esgotamento de recursos um processo célere e eficaz para o atacante.

O HAProxy[6] é um balanceador de carga de alta performance que possui recursos nativos para limitar a taxa de requisições (*rate limiting*) e bloquear IPs suspeitos, sendo uma defesa eficaz contra-ataques na camada de aplicação.

Zeebaree (2020), em seus experimentos, ensina que a alta disponibilidade de serviços de internet tornou-se a principal demanda da sociedade contemporânea. No entanto, esses serviços ocasionalmente tornam-se inacessíveis devido a diversas ameaças, sendo o ataque de Negação de Serviço Distribuído (DDoS) por inundação de sincronização (SYN Flood) o mais frequente, causando sérios impactos na infraestrutura de rede pública. O estudo ilustra sistematicamente o impacto desse ataque em servidores web baseados em *clusters*. Além disso, avalia-se o desempenho do *Internet Information Services 10.0* (IIS 10.0) no Windows Server 2016 e do Apache 2 no Ubuntu Linux 16.04. O processo de medição é realizado em ambientes de Balanceamento de Carga de Rede (NLB) e *Proxy* de Alta Disponibilidade (HAProxy). A estabilidade, a eficiência e a capacidade de resposta dos servidores são analisadas sob métricas como uso médio de CPU e taxa de transferência (*throughput*). Os resultados demonstram que os servidores baseados

[6] HAPROXY. **HAProxy**: the reliable, high performance TCP/HTTP load balancer. [S. l.]: HAProxy, 2026. Disponível em: https://www.haproxy.org/. Acesso em: 21 abr. 2026.

em *cluster* IIS 10.0 apresentam maior resiliência e desempenho superior ao Apache 2, tanto em condições normais quanto sob ataques DDoS de inundação SYN.

O FastNetMon[7] é uma ferramenta muito utilizada por provedores de internet (ISPs). Ela analisa o fluxo de rede (NetFlow/SFlow) e detecta ataques DDoS em milissegundos, podendo disparar scripts para bloquear o ataque automaticamente.

Outro tipo de firewall é o WAF (Web Application Firewall), um firewall que atua na camada de aplicação, enquanto o firewall de rede protege a infraestrutura, o WAF protege especificamente as aplicações web. Sua função é filtrar e monitora o tráfego HTTP/HTTPS, bloqueando ataques que tentam esgotar os recursos do servidor web por meio de requisições legítimas, mas em massa.

De acordo com o estudo de Scano (2024), embora o ModSecurity com o conjunto OWASP CRS (Core Rule Set - Conjunto de Regras Essenciais) seja o padrão global para proteção de aplicações web, sua dependência de pesos manuais e heurísticas estáticas limita sua eficácia contra ameaças personalizadas. Para mitigar essa deficiência, os autores introduzem o ModSec-Learn, uma abordagem baseada em inteligência artificial que transforma as regras do CRS em parâmetros de entrada para um modelo preditivo. Ao treinar o sistema com o tráfego real da aplicação, o modelo otimiza a importância de cada regra, reduzindo drasticamente os falsos positivos e aumentando a precisão da detecção. Adicionalmente, o uso de técnicas de regularização permitiu otimizar o desempenho do sistema, eliminando cerca de um terço das regras desnecessárias sem comprometer a segurança.

Outra solução fundamental reside no uso de sistemas IDS/IPS (*Intrusion Detection and Prevention Systems*). Enquanto o IDS monitora e alerta sobre atividades suspeitas, o IPS atua de forma proativa e em tempo real para interromper conexões que correspondam a assinaturas de ataques DoS conhecidos ou a comportamentos estatísticos anômalos. Um exemplo proeminente dessa tecnologia é o Snort, uma ferramenta de código aberto amplamente utilizada que realiza a inspeção profunda de pacotes para mitigar ameaças antes que estas comprometam a disponibilidade do servidor.

Segundo a análise de You (2020), a mitigação de ataques DDoS em larga escala pode ser otimizada através de um modelo de cooperação estratégica entre provedores de conectividade (ISPs) e de segurança (SSPs). O estudo utiliza a

[7] FASTNETMON. **FastNetMon**: DDoS detection toolkit with multiple packet capture engines. [S. l.]: FastNetMon, 2026. Disponível em: https://fastnetmon.com/. Acesso em: 21 abr. 2026.

metáfora dos *Scrubbing Centers* como centros de purificação de tráfego para justificar a terceirização desses serviços como uma forma de reduzir o ônus financeiro e técnico dos ISPs. O diferencial da pesquisa reside na criação de um sistema de leilão dinâmico que seleciona os melhores lances de mitigação em tempo real. Através de modelagem matemática complexa e algoritmos de otimização, o autor propõe um método que minimiza os custos de operação e de troca de provedor, mesmo sem conhecimento prévio de ataques futuros. Os resultados, validados com dados do mundo real, comprovam que essa abordagem automatizada é superior aos métodos tradicionais, oferecendo uma solução economicamente viável e tecnicamente robusta para a manutenção da disponibilidade de rede.

Conforme Albano (2023), a proliferação de dispositivos IoT vulneráveis intensificou a complexidade dos ataques DDoS, exigindo sistemas de detecção que suportem variações ruidosas no tráfego. A pesquisa propõe um método preditivo que utiliza a transformação ordinal para filtrar inconsistências nos dados de rede, aplicando o modelo One-Class SVM para identificar padrões anômalos sem a necessidade de treinamento prévio com dados rotulados. O grande diferencial desta abordagem é o seu caráter proativo: a capacidade de prever a iminência de um ataque com quase 45 minutos de antecedência e um índice de acerto de 89%, permitindo que as equipes de segurança implementem medidas de mitigação antes mesmo da interrupção dos serviços.

Os ataques de fraude fundamentam-se na atuação de má-fé com o propósito de obter vantagens indevidas sobre as vítimas. Conforme observado em atividades no Laboratório Forense, uma tendência recente é a sofisticação da Engenharia Social, exemplificada pelo golpe da "falsa central bancária". Nessas ocorrências, criminosos simulam o atendimento de uma agência legítima e estabelecem contato com o cliente, utilizando frequentemente ferramentas de Inteligência Artificial para mimetizar a voz de gerentes ou conhecidos. Além disso, o uso de tecnologias de *deepfake* permite que os atacantes personifiquem indivíduos de confiança da vítima, conferindo maior verossimilhança ao golpe e dificultando a identificação da fraude.

Embora a evolução tecnológica proporcione inúmeros benefícios à sociedade, ela também fomenta novas modalidades criminosas. Entre estas, destaca-se o desvio de ativos em sistemas bancários por meio do sequestro de sessão (*session hijacking*), técnica na qual o invasor assume a identidade digital da vítima para realizar transações ilícitas. No âmbito dos crimes cibernéticos, a determinação do *locus delicti*

e a localização do agente apresentam desafios complexos, visto que, em ambiente de rede, agressor e vítima não ocupam necessariamente o mesmo espaço geográfico. Diante dessa ubiquidade, torna-se imprescindível a aplicação de metodologias e ferramentas de computação forense para rastrear evidências digitais, identificar a origem das conexões e promover a autoria do delito.

Com o rápido desenvolvimento da tecnologia, a conexão à internet tornou-se um elemento indispensável da vida. Com a pandemia da Covid-19, o ensino online com computadores, tablets e celulares tornou-se obrigatório devido ao ensino remoto. A segurança dessas ferramentas de conectividade tornou-se crucial. Nesse processo, as compras online a partir de casa aumentaram consideravelmente. Devido ao uso inédito por parte dos usuários e à rapidez do serviço, as vulnerabilidades de segurança expõem os usuários a situações difíceis e ao cyberbullying. O fato de os dispositivos estarem conectados à internet, seja por cabo ou sem fio, torna-os vulneráveis. A exposição desses dispositivos a ataques cibernéticos em sua casa significa uma violação da sua privacidade, além da exposição de muitos dados pessoais. Atualmente, até mesmo os detalhes mais sutis dessas tecnologias são explorados para roubar dados pessoais, usando a necessidade de confiança, como em fraudes telefônicas ou propaganda enganosa de vacinas contra a pandemia. Torna-se cada vez mais importante informar os usuários finais sobre a tecnologia da internet e as vulnerabilidades de segurança nesse campo, além de conscientizá-los. Se essas ações forem intensificadas, o número de pessoas expostas a ataques cibernéticos diminuirá. O primeiro passo para isso é alcançar essas pessoas e educá-las.

Existem diversas metodologias para a intrusão em sistemas computacionais. Abaixo, detalham-se as técnicas e ferramentas mais utilizadas por criminosos digitais, cuja identificação e materialização de provas exigem o emprego de recursos avançados de computação forense conforme ensina BAŞESKIOĞLU(2021):

- **Chave Mestra (*Superzapping*):** Refere-se ao uso não autorizado de programas utilitários de sistema para modificar, destruir, copiar ou interceptar dados, ignorando os controles de segurança padrão.
- **Sniffers (Interceptadores):** Ferramentas que capturam e analisam o tráfego de dados em uma rede, permitindo a leitura de informações sensíveis que circulam sem criptografia.

- **Cavalo de Tróia (*Trojan Horse*):** Software que se disfarça de uma aplicação legítima para ocultar funcionalidades maliciosas, induzindo o usuário a permitir sua execução e o consequente comprometimento do sistema.
- **Vírus:** Fragmento de código capaz de se autorreplicar e infectar outros programas, alterando sua estrutura para destruir dados ou realizar ações nocivas com ou sem a ciência do usuário.
- **Satan (*Security Administrator Tool for Analyzing Networks*):** Ferramenta pioneira na análise de redes para detecção de vulnerabilidades. No contexto forense atual, representa a categoria de *Vulnerability Scanners* utilizados por invasores para mapear brechas de segurança.
- **Spyware:** Software projetado para monitorar as atividades do usuário e coletar informações pessoais ou hábitos de navegação, transmitindo-os a terceiros sem o devido consentimento.
- **Keylogger:** Tipo específico de *spyware* que registra as pulsações do teclado. É frequentemente utilizado para capturar credenciais de acesso, números de cartões e comunicações privadas.
- **Adware:** Programa que exibe anúncios publicitários de forma invasiva. Muitas vezes está acoplado a *spywares* para direcionar publicidade baseada no comportamento do usuário.
- **Cookies:** Pequenos arquivos de texto armazenados por websites. Embora sejam geralmente inofensivos e úteis para a personalização da navegação, *cookies* de rastreamento de terceiros podem ser utilizados para monitorar padrões comportamentais de forma invasiva.
- **Backdoor (Porta dos Fundos):** Vulnerabilidade ou método criado por invasores (muitas vezes via *Trojans*) para garantir o acesso persistente ao sistema, contornando os mecanismos de autenticação tradicionais.
- **EULA (End-User License Agreement):** Contrato de licença de uso. Frequentemente, usuários instalam adwares ou spywares inadvertidamente ao aceitarem termos de condições sem a devida leitura, especialmente em softwares gratuitos (sharewares).
- **Ransomware**: é uma modalidade de software malicioso (malware) projetada para bloquear o acesso a arquivos ou a sistemas inteiros, exigindo o pagamento de um resgate (normalmente em criptomoedas como o Bitcoin) para que o acesso seja restabelecido.

A Figura 5 ilustra uma arquitetura de rede contemporânea, projetada para mitigar ameaças sofisticadas e gerenciar as vulnerabilidades inerentes aos ambientes digitais atuais. A primeira camada, denominada Camada Externa / Internet, compreende o Provedor de Proteção Anti-DDoS (*Scrubbing Center*), que atua como a linha de frente contra-ataques volumétricos. Essa estrutura é essencial para impedir que ataques massivos de Negação de Serviço saturem o link de internet e paralisem a rede antes mesmo que os *firewalls* internos consigam processar o tráfego. O sistema opera filtrando o tráfego "espúrio" diretamente na nuvem e encaminhando apenas os dados legítimos para a infraestrutura interna.

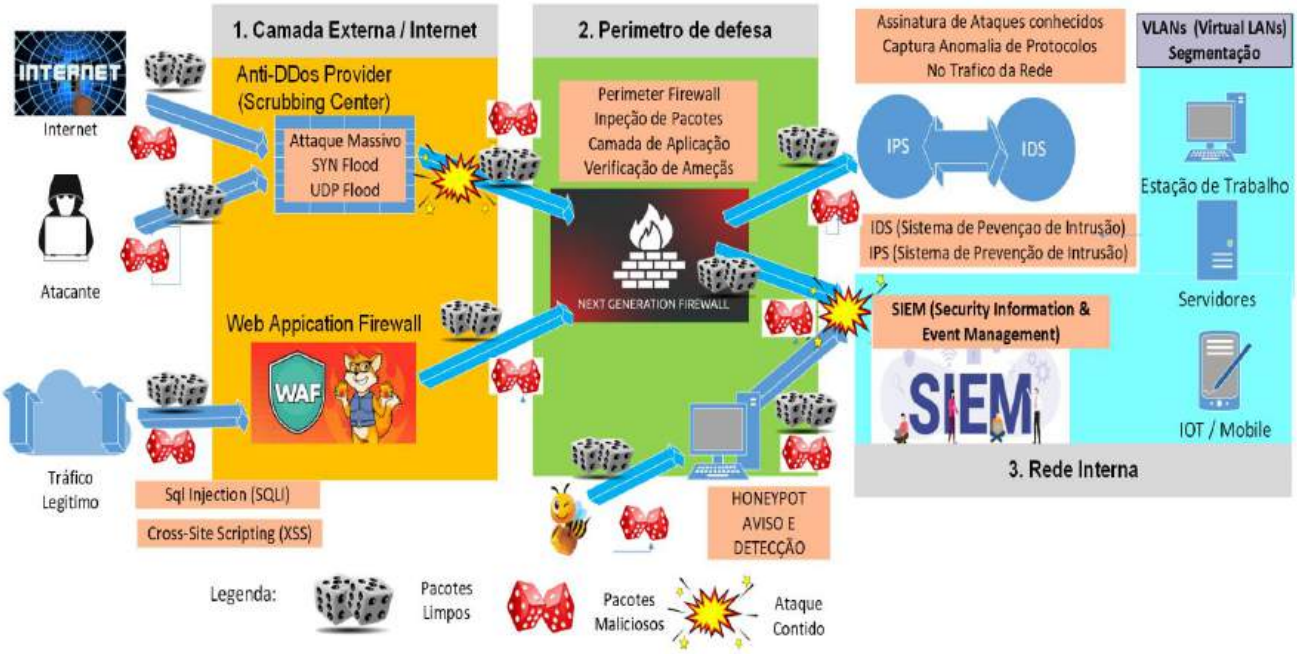
Ainda integrada à Camada 1, encontra-se o WAF (*Web Application Firewall*), projetado para a proteção específica de aplicações *web*, tais como sites institucionais, APIs e portais de alunos ou funcionários. Operando na Camada 7 (Aplicação) do modelo OSI, o WAF é capaz de mitigar ameaças como Injeção de SQL (SQLi) e *Cross-Site Scripting* (XSS), que buscam explorar vulnerabilidades de programação para o acesso indevido a bancos de dados. Diferente de um *firewall* de rede convencional, que analisa apenas portas e protocolos, o WAF realiza a inspeção profunda do conteúdo das requisições HTTP/HTTPS, identificando padrões maliciosos que passariam despercebidos por defesas perimetrais comuns.

Na Camada 2, estabelece-se o Perímetro de Defesa, onde opera o NGFW (*Next-Generation Firewall*), representando a evolução tecnológica dos *firewalls* convencionais. Além da filtragem básica de portas e endereços IP, o NGFW executa a Inspeção Profunda de Pacotes (*Deep Packet Inspection* — DPI), o que permite identificar com precisão a aplicação de origem do tráfego. Essa funcionalidade é vital para distinguir, por exemplo, consultas DNS legítimas de túneis de exfiltração de dados maliciosos. Adicionalmente, o NGFW realiza a inspeção de tráfego criptografado (SSL/TLS), uma capacidade crítica no cenário atual, dado que a maioria das ameaças utiliza protocolos cifrados para evadir sistemas de segurança tradicionais.

Ainda nesta camada, integram-se os sistemas IDS/IPS (*Intrusion Detection and Prevention Systems*), que atuam em tempo real para identificar e bloquear *exploits* e ataques conhecidos, baseados em assinaturas e anomalias de protocolo. Enquanto o foco do NGFW reside no controle e visibilidade das aplicações, o IPS concentra-se em mitigar a exploração de vulnerabilidades não corrigidas (*unpatched*) nos

servidores, servindo como uma camada de proteção ativa contra tentativas de intrusão.

Figura 5 – Arquitetura de Redes



Fonte: (do Autor)

Na Camada 3 (Rede Interna), estabelece-se a Segmentação de Rede, técnica fundamental para mitigar o movimento lateral de ameaças. Caso um dispositivo IoT ou uma estação de trabalho seja comprometida por um *ransomware*, a segmentação impede que o artefato malicioso se propague para segmentos críticos, como a rede de servidores ou o ambiente financeiro institucional.

O monitoramento e a visibilidade são geridos pelo SIEM (*Security Information and Event Management*), exemplificado por soluções como Splunk e QRadar. O SIEM atua como o "cérebro" da operação de segurança, centralizando os *logs* de diversos ativos (firewalls, servidores, WAFs e switches). Através da correlação de eventos e do uso de Inteligência Artificial, o sistema identifica padrões de ataque complexos que seriam imperceptíveis se analisados isoladamente em cada dispositivo.

Adicionalmente, utiliza-se o Honeypot (Pote de Mel), que opera como um sistema de alerta precoce (*early warning*). Trata-se de um servidor intencionalmente vulnerável projetado para atrair atacantes. Visto que não possui funções produtivas, qualquer acesso ao *honeypot* é, por definição, anômalo, permitindo que a equipe de segurança identifique intrusos e estude suas táticas de intrusão sem expor os sistemas reais.

Em síntese, essa arquitetura transcende a função preventiva. Cada dispositivo atua como uma fonte de evidências digitais cruciais para a reconstrução de incidentes. Enquanto o WAF registra tentativas de SQLi e o NGFW mapeia conexões com servidores de Comando e Controle (C&C), o SIEM correlaciona esses vestígios para comprovar a autoria, a cronologia e a extensão dos danos em uma investigação forense.

b) Atuação em grupo de pesquisa durante o estágio de pós-doutoramento

A atuação do laboratório pauta-se pela aplicação de tecnologias avançadas voltadas à perícia digital, visando à elucidação de evidências e ao estabelecimento da materialidade dos fatos por meio do confronto técnico-científico com as informações apresentadas.

- **Estudo de Caso 1 (Mel Maia):** Realizou-se perícia técnica em material videográfico para a identificação de *deepfake* de natureza íntima. A metodologia empregou ferramentas de análise de integridade de pixels e modelos de redes neurais para verificar a autenticidade do conteúdo e detectar possíveis manipulações sintéticas por inteligência artificial.
- **Estudo de Caso 2 (Ana Hickmann):** Atuação em perícia grafotécnica e documentoscopia, com foco na contraposição técnica entre os laudos "Del Picchia" (conclusivo pela autenticidade) e "Tirotti" (conclusivo pela falsidade). A inovação deste caso reside no desenvolvimento de animações 3D e no uso de *Chroma Key* para a criação de um "vídeo-laudo". Essa técnica visa traduzir a complexidade da prova pericial em uma linguagem visual inteligível para magistrados e para a opinião pública, conferindo maior transparência e clareza aos achados técnicos.
- **Estudo de Caso 3 Perícia Fonética (General Heleno):** O laboratório elaborou um laudo pericial de análise acústica e fonética sobre áudios que indicavam a articulação de um suposto golpe de Estado. O trabalho técnico consistiu na verificação de autenticidade e autoria das gravações, servindo como base científica para uma reportagem exclusiva da Revista Fórum. Este caso exemplifica a atuação do laboratório em demandas de alto interesse público e sua interface com o Direito e o Jornalismo Investigativo**.**

c) Utilização do Laboratório de Computação Forense da UFABC.

O laboratório está localizado no Bloco L, sala 403, no Campus Santo André, contando com localização estratégica e fácil acesso via Avenida do Estado ou pela estação de trem Prefeito Celso Daniel (Linha 10-Turquesa da CPTM).

A infraestrutura foi projetada para atender aos rigorosos critérios de perícia forense, destacando-se:

- **Segurança e Sigilo:** A sala é equipada com um cofre e sistema de fechadura eletrônica para garantir a custódia segura de evidências e o sigilo dos trabalhos realizados.
- **Acesso Controlado:** O ingresso ao recinto é restrito e autorizado exclusivamente pelo supervisor do estágio. Como protocolo de segurança, exige-se a assinatura do Termo de Responsabilidade e Confidencialidade antes da concessão de acesso.
- **Tecnologia e Colaboração:** O espaço dispõe de uma mesa de reuniões e uma tela de alta definição (85 polegadas) voltada para videoconferências e análises detalhadas de materiais audiovisuais.
- **Estações de Trabalho e Flexibilidade:** O laboratório conta com estações equipadas para a instalação de *softwares* específicos de pesquisa, além de bancadas preparadas para o uso de dispositivos pessoais (*notebooks*). Essa configuração permite a integração entre as atividades presenciais e o regime de trabalho remoto para tarefas que não envolvam dados de caráter sigiloso.

d) Demais demandas durante o estágio de pós-doutoramento.

O Laboratório de Computação Forense da UFABC integra Direito, Tecnologia e Inteligência Artificial para responder aos desafios da digitalização acelerada. Em um cenário onde a arquitetura cliente-servidor e a inovação tecnológica constante favorecem novos crimes digitais, o Laboratório oferece uma resposta multidisciplinar por meio de pesquisadores de todos os níveis acadêmicos. Inaugurado em 19 de março de 2025, o centro é considerado pelo supervisor de estágio, o Prof. Dr. Mario Alexandre Gazziro, como o primeiro laboratório brasileiro de análises forenses digitais. Abaixo, elenco as áreas de atuação do laboratório nas quais tive a oportunidade de participar:

- **Forense Multimídia:** Identificação de adulterações e *deepfakes* em áudio e vídeo para garantir a integridade de provas digitais.

- **Grafoscopia Digital e 3D:** Aplicação de técnicas avançadas, como a sobreposição de imagens em 3D utilizada no caso Ana Hickmann, permitindo uma visualização clara de divergências em assinaturas.
- **Análise Documental Crítica:** Identificação de anacronismos e fraudes históricas, como no caso Silvinei Vasques, onde o uso de nomenclaturas obsoletas revelou a invalidade de documentos oficiais.
- **Operações em Cibersegurança:** O laboratório conta com alunos que atuam na resolução de crimes cibernéticos, em parceria com advogados que buscam o suporte especializado da unidade. Entre as frentes de atuação, destacam-se a perícia em perfis falsos e a recuperação de ativos digitais. Um exemplo da eficácia da equipe foi a resolução célere de uma invasão de e-mail: utilizando engenharia social reversa, os pesquisadores enviaram um link de rastreamento ao criminoso, cujo clique resultou na identificação imediata do IP e da geolocalização do suspeito em São Caetano do Sul. Atualmente, o projeto expande suas fronteiras com o planejamento de workshops de conscientização e a realização de testes de intrusão (*Pentests*).
- **Biometria e Inteligência Artificial:** O laboratório atua no desenvolvimento de *hardware* e *software* voltados à biometria, utilizando tecnologias de reconhecimento de íris, face e impressão digital. Além da identificação convencional, as pesquisas abrangem a extração de características biométricas (como etnia, sexo e altura) e o estudo de padrões de biometria vascular, especificamente a partir das veias da palma da mão.
- **Deepfakes:** O laboratório dispõe de ferramentas avançadas para a geração e análise de *deepfakes*, permitindo demonstrar tecnicamente como ocorre a substituição de faces (*face swapping*) para a personificação de terceiros. O objetivo dessas simulações é capacitar pesquisadores na identificação de artefatos digitais manipulados e no desenvolvimento de contramedidas forenses.
- **Detecção de Adulteração de Imagens, Vídeos e Sons:** O laboratório utiliza algoritmos baseados na análise de artefatos de compressão para identificar edições e montagens em diferentes mídias. Essa técnica permite destacar áreas ou segmentos específicos onde a fraude foi cometida, revelando inconsistências no processamento digital que, embora imperceptíveis ao olho ou ouvido humano, tornam-se evidentes via análise forense especializada.

e) Organização de eventos acadêmicos durante o estágio de pós-doutoramento.

No âmbito das atividades deste estágio pós-doutoral, foi oferecido à comunidade acadêmica o curso "Introdução à Cibersegurança". A iniciativa faz parte da Maratona de Cibereducação promovida pela Cisco, em parceria com o Centro Paula Souza (CPS). Como Instrutor Cisco e responsável pela Academia Cisco na Fatec Itaquera, atuei como o docente encarregado pela condução do curso e pela respectiva emissão de certificados. O treinamento foi disponibilizado de forma gratuita e aberta tanto aos alunos da UFABC e da Fatec Itaquera quanto à comunidade externa, facilitando o acesso democrático a informações essenciais sobre segurança digital. O conteúdo programático foi integralmente disponibilizado online[8], alinhando-se diretamente aos objetivos de difusão de conhecimento e cidadania digital previstos nesta pesquisa.

Atuei como avaliador no evento Engineering Innovation da UFABC, por indicação do Prof. Dr. Mario Alexandre Gazziro, contribuindo na análise dos trabalhos discentes e no suporte às demandas organizacionais. Na ocasião, alunos das Fatec Mauá e Fatec Itaquera foram convidados a prestigiar o evento, o que proporcionou uma rica integração entre as instituições. Essa visita permitiu que os estudantes conhecessem os projetos desenvolvidos na UFABC, servindo como referencial e motivação para seus próprios Trabalhos de Conclusão de Curso (TCC) e Projetos Integradores. Além disso, o intercâmbio ofereceu a oportunidade de aproximação com o corpo discente e com a infraestrutura da universidade, visando estimular a continuidade de sua formação acadêmica por meio de futuros programas de Especialização, Mestrado e Doutorado.

VII. Produção Acadêmica e Técnica

As atividades que foram realizadas durante o estágio de pós-doutorado:

Foi publicado o artigo intitulado **“**Responsabilidade Civil nas Instituições Financeiras na Sociedade 4.0 e a Gestão de Risco na era digital**”** na *Revista de Direito Bancário e do Mercado de Capitais* (Apêndice I).

O capítulo de livro, intitulado **“**O (não) combate à falsificação na era digital no Brasil quanto à defesa das pessoas físicas na atualidade**”** foi aprovado para publicação nos anais do *I Simpósio do Conectajur* (Apêndice II).

[8] Introdução a CiberSegurança, disponível em: https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=pt-BR&instance_id=701aa02e-34be-4986-956f-f6c18f172e9f, acessado em 21/04/2026

VIII. Considerações Finais

O problema central desta pesquisa consiste na análise de um ecossistema de ferramentas aplicadas à computação forense, visando a produção de artefatos que sirvam como evidências materiais e a avaliação de seus respectivos níveis de eficiência.

O objetivo da pesquisa é fazer uma análise quantitativa e qualitativa sobre as ferramentas utilizadas e quando uma ferramenta pode ser utilizada com uma outra para a produção de provas e verificar qual o nível de eficiência da ferramenta. Sendo que a hipótese da solução escolhida foi fazer um levantamento bibliográfico das principais ferramentas de software livre utilizadas e para quais casos são aplicados.

As evidências discutidas ao longo desta pesquisa permitem concluir que os objetivos gerais e específicos foram plenamente cumpridos. A análise quantitativa e qualitativa das ferramentas selecionadas demonstrou que a eficácia da computação forense moderna não reside apenas na análise *post-mortem*, mas na capacidade de uma infraestrutura de rede gerar artefatos digitais íntegros e tempestivos.

A transição de sistemas de defesa meramente reativos para arquiteturas proativas, equipadas com Inteligência Artificial, mostrou-se imperativa diante da sofisticação de ameaças como o *Ransomware*. A integração entre diferentes camadas — como o uso conjunto de WAF, NGFW e SIEM — não apenas potencializou a capacidade de detecção, mas enriqueceu significativamente a base de provas materiais coletadas. Observou-se que a predição de incidentes oferece uma janela de oportunidade crítica para a mitigação de danos, permitindo que a resposta ocorra antes da efetivação do ataque.

A hipótese de solução baseada no levantamento bibliográfico de tecnologias de software livre provou-se correta, demonstrando ser uma alternativa viável e de alta eficiência para a construção de ambientes resilientes. A implementação estratégica de dispositivos como Honeypots e sistemas de correlação de eventos (SIEM) garantiu a manutenção da cadeia de custódia digital, fornecendo os subsídios técnicos indispensáveis para a elucidação de crimes cibernéticos. Em última análise, o estudo consolida um modelo de defesa em profundidade capaz de proteger os ativos organizacionais e fundamentar a responsabilidade civil na era digital.

Como resultado deste trabalho, propôs-se uma arquitetura de rede voltada à mitigação das principais ameaças digitais enfrentadas pelas organizações contemporâneas. Fundamentada nas tendências e estatísticas apresentadas pelo

Cert.br (2025), a estrutura foi desenhada não apenas para a defesa, mas para assegurar o fornecimento de artefatos digitais robustos, essenciais para os procedimentos de computação forense.

A pesquisa demonstra que a implementação de uma arquitetura resiliente vai além da proteção perimetral, estabelecendo a Prontidão Forense necessária para que a organização responda legalmente a incidentes com conformidade e integridade.

Por fim, este trabalho reforça o papel da Cibereducação no âmbito acadêmico e institucional. A convergência entre o Direito Digital e a Engenharia de Redes aqui explorada serve de base para a formação de profissionais mais resilientes e para o fortalecimento da cidadania digital nas instituições de ensino técnico superior, garantindo que o desenvolvimento tecnológico ocorra sob a égide da segurança e da ética.

IX. Agradecimentos

Gostaria de expressar minha profunda gratidão a todos que contribuíram para a realização deste estágio de pós-doutoramento:

- Ao Prof. Dr. Mario Alexandre Gazziro, pela supervisão e orientação sempre precisas. Sua expertise e confiança foram fundamentais para a condução desta pesquisa no Laboratório de Computação Forense, proporcionando um ambiente de aprendizado e inovação constante.
- Aos membros da Pró-Reitoria de Pesquisa (PROPES), pelo suporte institucional e pela viabilização dos trâmites administrativos necessários para o pleno desenvolvimento deste ciclo acadêmico.
- Ao colega Vitor da Silva Bittencourt, pela parceria nas atividades laboratoriais, pelas discussões técnicas e pelo apoio mútuo que tanto enriqueceram o cotidiano desta pesquisa.
- Aos membros do Laboratório de Computação Forense, pelo compartilhamento de conhecimentos e pela colaboração técnica, fundamentais para o sucesso dos experimentos realizados.
- Ao bibliotecário da instituição, pelo auxílio indispensável na busca por referências e pelo suporte na normalização e acesso às bases de dados científicas.
- Aos funcionários da UFABC, que, com seu trabalho e dedicação, garantem a infraestrutura e o suporte necessários para que a produção científica da universidade seja possível.

X. Referências Bibliográficas

ALBANO, Lucas et al. Predição de ataques ddos pela correlação de séries temporais via padrões ordinais. In: **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. SBC, 2023. p. 69-82.

ALFARSI, Ghaliya et al. Using Cisco Packet Tracer to simulate smart home. **International Journal of Engineering Research & Technology (IJERT)**, v. 8, n. 12, p. 670-674, 2019

ALMADA, María Luz; TALAY, Carlos Alberto. **Consideraciones al momento de evaluar la migración del simulador ns-2 al ns-3**. Informes Científicos Técnicos-UNPA, v. 12, n. 2, p. 63-83, 2020

ARMANI TECHNOLOGY. Firewall FortiGate para Empresas: conheça a solução Fortinet. [S. l.], 2026. Disponível em: https://armanitechnology.com.br/firewall-fortigate-para-empresas/. Acesso em: 21 abr. 2026.

BALYK, Anatoliy et al. Using graphic network simulator 3 for DDoS attacks simulation. **International Journal of Computing**, v. 16, n. 4, p. 219-225, 2017.

BAŞESKIOĞLU, Mehmet Özer; TEPECIK, Abdülkadir. Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews. In: **2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)**. IEEE, 2021. p. 1-5.

BRESSAN, Graça et al. Virtualização de experimentos do laboratório didático de redes de computadores para a flexibilidade, redução de custos e uso remoto: Virtualization of computer network educational laboratory experiments for flexibility, cost reduction and remote use. **Brazilian Journal of Development**, v. 8, n. 11, p. 74848-74863, 2022.

BRITO, Samuel Henrique Bucke. **Laboratórios de tecnologias Cisco em infraestrutura de redes**. Novatec Editora, 2019

CARVALHO, Ranyelson Neres. DoSSEC: proposta de detecçao e mitigaçao de ataques SYN Flood em redes SDN. 2020.

Cisco Packet Trace, Simulador de redes, disponível em https://www.netacad.com/pt-br/courses/packet-tracer, acessado em 09/04/2024.

CAGNANI, Caio; SANTOS, Valdecir de Deus dos; **Computação Forense: Fundamentos. Universidade do Vale do Rio dos Sinos**; UNISINOS; Disponível em: <http://pt.scribd.com/doc/47774532/computacao-forense-fundamentos>. Acesso em 03 abr. 2025.

CERT, **Centro de Estudos e Respostas de Tratamento de Incidentes no Brasil**, acessado em 21/04/2026

CISCO. Cisco Firepower 1000 Series: NGFW for small to medium-sized businesses. San Jose: Cisco Systems, 2026. Disponível em: https://www.cisco.com/site/us/en/products/security/firewalls/firepower-1000-series/index.html. Acesso em: 21 abr. 2026.

COMER, Douglas E. **Redes de computadores e internet**. 6th ed. Porto Alegre: Bookman, 2016. *E-book.* p.Capa. ISBN 9788582603734. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788582603734/. Acesso em: 24 nov. 2024.

CISCO, Curso CCNA 3, Comutação de Rede Local e Sem Fio, Curso Cisco On-line, disponível em www.netacad.com, acessado em 25/06/2014

DA SILVA, Lucas Ferreira; PARISOTO, Mara Fernanda; DO NASCIMENTO, William Junior. APRENDIZAGEM SIGNIFICATIVA EM CLUBES DE CIÊNCIAS: UMA

DE CARVALHO BERTOLI, Gustavo et al. Abordagem fim-a-fim para uso de aprendizado de máquina em IDS–Caso de detecção stateless para TCP Scan. In: **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. SBC, 2020. p. 271-284.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. São Paulo: Novatec Editora, 2010.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional: Teoria e Prática Aplicada**. São Paulo: Pearson Prentice Hall, 2007

FASTNETMON. **FastNetMon**: DDoS detection toolkit with multiple packet capture engines. [S. l.]: FastNetMon, 2026. Disponível em: https://fastnetmon.com/. Acesso em: 21 abr. 2026.

HAPROXY. **HAProxy**: the reliable, high performance TCP/HTTP load balancer. [S. l.]: HAProxy, 2026. Disponível em: https://www.haproxy.org/. Acesso em: 21 abr. 2026.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 1122**: Requirements for Internet Hosts -- Communication Layers. Editado por Robert Braden. [S. l.]: IETF, out. 1989. Disponível em: https://datatracker.ietf.org/doc/html/rfc1122. Acesso em: 21 abr. 2026.

REVISÃO SISTEMÁTICA DA LITERATURA. **REPPE-Revista de Produtos Educacionais e Pesquisas em Ensino**, v. 8, n. 2, p. 2801-2815, 2024.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de computadores**. Porto Alegre: AMGH, 2013. *E-book.* p.Capa. ISBN 9788580551693. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788580551693/. Acesso em: 24 nov. 2024.

GARCÍA NAVARRO, Gonzalo. Tsubame: simulador de redes informáticas basado en tecnologías web. 2023

KALI, Kali Linux site oficial, www.kali.org, acessado em 04/04/2025

HASSAN, Nihad A. **Perícia Forense Digital: Guia prático com uso do sistema operacional Windows**. Novatec Editora, 2019.

MACHADO, Fábio Guedes Labbate; HADAD, Renato Moreira. Análise de Desempenho de Firewall: Performance do PfSense em ataque DoS–Denial of Service, disponível em: https://bib.pucminas.br/pergamumweb/vinculos/000006/0000062c.pdf, acessado em 21/04/2026.

MORANDI, Maria Isabel W. Motta; CAMARGO, Luis F. Riehs. Revisão sistemática da literatura. In: DRESCH, Aline; LACERDA, Daniel P.; ANTUNES JR, José A. Valle. Design sciencie research: método e pesquisa para avanço da ciência e da tecnologia. Porto Alegre: Bookman, 2015.

MAIA, Luiz Paulo. **Arquitetura de redes de computadores** . Grupo Gen-LTC, 2000.

MORENO, Daniel. **Introdução ao PENTEST**. Novatec Editora, 2019.

OLIVEIRA, Valdinei Carlos. Simulador Eve-NG em projetos de redes heterogêneas: um estudo sobre a importância da simulação em redes de computadores. **Research, Society and Development**, v. 9, n. 11, p. 562-572, 2020

ROCHA, Lucio Agostinho et al. **WebLab SOA no domínio de redes de computadores para experimentos DiffServ**. 2009, disponível em: https://repositorio.ufu.br/handle/123456789/12472, acessado em 10/04/2024.

ROSSATO, Nelson Piletti, Solange M. **Psicologia da aprendizagem: da teoria do condicionamento ao construtivismo**. São Paulo: Editora Contexto, 2011. *E-book.* p.1. ISBN 9786555413106. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555413106/. Acesso em: 26 jan. 2025.

ROZI, Nurwan Reza Fachrur; NURHAYATI, Ade; ROZANO, Seandy Arandiant. Implementation OSPFv3 For Internet Protocol Verses 6 (IPv6) Based On Juniper Routers Use Emulator Virtual Engine–Next Generation (Eve-NG). **International Journal of Engineering Continuity**, v. 3, n. 1, p. 1-11, 2024

SCANO, Christian et al. Modsec-learn: Boosting modsecurity with machine learning. In: **International Symposium on Distributed Computing and Artificial Intelligence**. Cham: Springer Nature Switzerland, 2024. p. 23-33.

SNORT. **Snort**: the world's foremost open source intrusion prevention system. [S. l.]: Snort, 2026. Disponível em: https://www.snort.org/. Acesso em: 21 abr. 2026.

SUN, Shu; MACCARTNEY, George R.; RAPPAPORT, Theodore S. A novel millimeter-wave channel simulator and applications for 5G wireless communications. In: **2017 IEEE international conference on communications (ICC)**. IEEE, 2017. p. 1-7.

VISWANADH, K. S. et al. Engineering End-to-End Remote Labs using IoT-based Retrofitting. **arXiv preprint arXiv:2402.05466**, 2024, disponível em: https://arxiv.org/abs/2402.05466, acessado em 10/04/2024.

WHITE, Curt M. **Redes de computadores e comunicação de dados**. São Paulo: Cengage Learning Brasil, 2013. *E-book.* ISBN 9788522112944. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522112944/. Acesso em: 12 fev. 2024.

ZEEBAREE, Subhi Rafeeq; JACKSI, Karwan; ZEBARI, Rizgar R. Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers. **Indones. J. Electr. Eng. Comput. Sci**, v. 19, n. 1, p. 510-517, 2020.

YOU, Wencong et al. Scheduling DDoS cloud scrubbing in ISP networks via randomized online auctions. In: **IEEE INFOCOM 2020-IEEE Conference on Computer Communications**. IEEE, 2020. p. 1658-1667.

XI. Apêndice A - Artigo publicado na Revista dos Tribunais

Revista Direito Bancário e do Mercado de Capitais.

https://doi.org/10.5281/zenodo.19651684

Responsabilidade Civil nas Instituições Financeiras na Sociedade 4.0 e a Gestão de Risco na era digital

Alexandre Borges Leite

Mestre em Direito Comercial. Advogado.
a.leite@rochaleiteadvogados.com.br

Fretz Sievers Junior

Mestre em Direito Administrativo, Mestre e Doutor em engenharia de computação, Advogado.
fretz.sievers@gmail.com

Mario Alexandre Gazziro

Doutor em Física Computacional, professor de engenharia da informação na UFABC.

mario.gazziro@ufabc.edu.br

Resumo: A Responsabilidade Civil das Instituições Financeiras na Sociedade 4.0 é um tema complexo e cada vez mais relevante no cenário jurídico e tecnológico atual exigindo inovações constantes com as novas tecnologias. A crescente digitalização dos serviços bancários, embora traga inúmeros benefícios em termos de comodidade e eficiência, também acarreta novos riscos e desafios, especialmente no que diz respeito à segurança e à proteção dos dados dos clientes, sendo necessária uma análise sobre sua responsabilidade objetiva, como determina a Súmula 479 do STJ. Na sociedade há pessoas que têm facilidade por tecnologia de informação intituladas com tecnofilia e as que tem medo ou não gostam intituladas com tecnofobia, mas precisam dos serviços oferecidos que se encontram informatizados que muitas vezes não há outra forma de ter acesso, tendo a necessidade de ter um dispositivo móvel, para ter acesso aos serviços das instituições financeiras, e precisam de ajuda para conseguir acessar os recursos ou até mesmo benefícios do governo e podem estar sujeitos a golpes por falta de conhecimento.

Palavras-chave: Direito Comercial – Direito bancário – Inteligência artificial – Sistemas de informação.

Abstract: The Civil Liability of Financial Institutions in Society 4.0 is a complex and increasingly relevant topic in the current legal and technological landscape, bringing constant innovation with new technologies. The increasing digitalization of banking services, while bringing considerable benefits in terms of convenience and efficiency, also poses new risks and challenges, especially regarding the security and protection of customer data. Therefore, an objective analysis of their liability is required, as determined by Superior Court of Justice (STJ) Summary 479. In society, there are people who are comfortable with information technology advertised as technophilia, and those who are afraid or dislike it due to technophobia, but who need the services offered, which are computerized and often have no other way to access them. They require a mobile device to access financial institution services. They also need help accessing resources or even government benefits, and may be subject to scams due to a lack of knowledge.

Keywords: Commercial law – Banking law – Artificial intelligence – Information systems.

Para citar este artigo: LEITE, Alexandre Borges; SIEVERS JUNIOR, Fretz Responsabilidade Civil das Instituições Financeiras na Sociedade 4.0 e a gestão de risco na era digital. Revista de Direito Bancário e do Mercado de Capitais. vol. 110. ano 29. São Paulo: Ed. RT, jan./jun. 2026. Disponível em: [URL]. Acesso em: DD.MM.AAAA. Confira as informações gerais da Revista: [https://www.thomsonreuters.com.br/pt/juridico/webrevistas.html]

1. Introdução

Mudanças sociais estão acontecendo de forma constante e muitas vezes não são percebidas por todos através das inovações tecnológicas, seja cada vez mais pelo uso de telefones inteligentes, que antes na sua versão inicial, tinha somente a função de fazer e receber chamadas a distância, tendo um custo elevado na prestação de seus serviços. Atualmente surgem os telefones inteligentes intitulados *smartphones* que além das suas funções básicas de enviar e receber chamadas por voz, são computadores móveis que podem fazer inúmeras funções, inclusive transações bancárias, tendo terminais de pronto atendimento em qualquer lugar e a qualquer hora, sem a necessidade de ir a uma agência bancária.

Essas inovações tecnológicas trazem modificações na contratação de produtos e serviços como por exemplo os contratos eletrônicos, conforme ensina Rebouças (2016). A Sociedade 4.0, com ampla utilização de sistemas de informação, oferece diversos serviços através da utilização de software desktop e aplicativos móveis com a promessa de que cada vez menos, seja mais necessário o auxílio humano de um analista de suporte ou aquele que faça a sua vez. As aplicações oferecem de forma organizada opções de um catálogo de serviços, utilizando uma arquitetura de informação que permite disponibilizá-las de uma forma mais intuitiva, facilitando o seu acesso. Sendo que os contratos podem ser assinados de forma eletrônica conforme a MP 2200-2/2001, que institui a Infra-Estrutura de Chaves Públicas Brasileira e do Decreto 10.278/2020, sendo as assinaturas consideradas válidas, vinculantes e executáveis, desde que firmadas pelos representantes legais das partes.

A StatCounter[1], oferece estatísticas através de dados agregados coletados em uma amostra de mais de 5 bilhões de visualizações de página por mês, com mais de 1,5 milhão de sites que propicia estatísticas atualizadas e disponibilizadas, através do seu algoritmo, consegue informar a quantidade de dispositivos dos usuários no Brasil, afirma que entre os dispositivos utilizados, 64,48% são dispositivos móveis, 34,86% são computadores de mesa e somente 0,66% são *tablets*. A computação móvel já ultrapassou o uso dos computadores de mesa no Brasil permitindo que os sistemas de informação sejam acessados em diferentes lugares, verificando sua localização através dos sistemas de GPS – *Global Positioning System,* presentes nos smartphones, permitindo saber a localização do usuário, para ser um dado utilizado para validar sua segurança, através de um histórico de acessos de localidade costuma utilizar os serviços bancários, para compra ou pagamentos.

Com os avanços tecnológicos surge a tecnofilia que conforme AGUIAR (2025) e DE MENEZES (2025), é uma afinidade com um grande interesse pela tecnologia, em especial as novas tecnologias de informação tendo uma facilidade com sistemas de informação, facilitando suas tarefas no cotidiano, ajudando no acesso a informações, de produtos e serviços, facilitando o acesso aos serviços digitais tais como agências bancárias e acesso aos serviços do Governo Digital[2], que apresenta como dados oferecidos ao cidadão 4752 serviços digitais, 3100 sistemas integrados na conta, 285,6 milhões de assinaturas eletrônicas, 169 milhões de contas ativas, sendo serviços totalmente gratuitos.

Em contrapartida, conforme pesquisa recente realizada pelo INAF – Instituto Nacional de Analfabetismo Funcional[3], realizado uma pesquisa no ano de 2024, utilizando telefones inteligentes. Foi realizado uma pesquisa, visando avaliar as habilidades digitais, sendo proposta três tarefas: a primeira foi a realização de compra em um comércio eletrônico, segunda tarefa proposta foi escolher um filme em uma plataforma digital e a última o preenchimento de um formulário para um festival de música, avaliando os seguintes itens: habilidades operacionais em que consiste como saber utilizar a interação com o sistema de informação, o trato com a informação em entender o que está escrito e por fim a produção de conteúdo quando há necessidade de responder um questionamento realizado pelo sistema, realizando interação, comunicação e colaboração.

Entre os pesquisados 48% das pessoas entre 50 e 64 anos tiveram um baixo desempenho nos testes digitais, acertando entre zero e pelo menos uma das três tarefas propostas na avaliação. Outros 46% ficaram na média, acertaram acima de 1/3 e até 2/3 do teste, e apenas 6% obtiveram alto desempenho, ou seja, acima de 2/3 ou mais dos itens. Isso indica um baixo engajamento no uso de ferramentas digitais o que afeta diretamente aos brasileiros a terem

acesso ao governo eletrônico tais como os serviços oferecidos pelo E-Gov[4], que garante a identificação de cada cidadão aos serviços digitais do governo, como um importante recurso a assinatura digital que permite firmar negócios jurídicos, através da assinatura digital.

Para os serviços bancários se faz necessário a segurança digital conhecida como *cibersecurity*, em que consiste em utilizar tecnologias visando garantir os pilares da segurança da informação que confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, garantindo a proteção dos dados que trafegam nos meios digitais em conformidade com a Lei Geral de Proteção de Dados Lei 13.709 de 14 de agosto de 2018, alterada pela Lei 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais.

Em 2024, teve-se 412.528 ocorrências com celulares subtraídos no Estado de São Paulo, conforme apresentado na Secretaria de Segurança Pública[5]. Em 2025 temos 165.533, ocorrências com celulares, sendo um número bem menor considerando o ano passado, porém é um número considerável e se faz necessário cuidados e prevenção com os aparelhos, pois há inúmeras funcionalidades nos celulares como aplicações bancárias, acesso a cartões de crédito e débito, acesso a benefícios do INSS – Instituto Nacional de Seguridade Social, realização de empréstimos, pagamento de contas, transferência, gerando inúmeros problemas para os seus proprietários, além do prejuízos com o aparelho subtraído.

Neste cenário tem-se a tecnofobia, que é ao contrário da tecnofilia, em que consiste em dificuldades com este mundo digital, como um medo ou rejeição da tecnologia em especial a tecnologia da informação em que os serviços governamentais estão cada vez mais digitalizados e se faz necessário um conhecimento para ter acesso aos serviços, ficando a margem dos benefícios gerados pela tecnologia. E se faz necessário recursos do mundo digital tais como a cibersegurança que se trata de uma segurança lógica *security* e a segurança física *safety* pensando em possíveis roubos, furtos ou perdas e como proteger o acesso aos seus recursos, tão importantes na convivência no mundo moderno acessando os diferentes serviços oferecidos em uma sociedade cada vez mais conectada aos serviços digitais.

Outra questão são os dados que se encontram nos dispositivos móveis que possibilitam ter acesso aos seus dados, gerando problemas para seus usuários que tem seus aplicativos invadidos ou suas contas sequestradas que comprometem a sua identidade virtual, através de suas redes sociais, acesso a contas bancárias, seus cartões de crédito, passar pela pessoa através de assinaturas digitais ou mesmo ter acesso a informações sensíveis como dados de sua saúde e de sua intimidade. Neste artigo iremos focar nas aplicações bancárias e acesso a benefícios que seus usuários estão sujeitos e que através de golpes pode-se gerar fobia no uso desses dispositivos.

Este artigo trata sobre os serviços encontrados no governo eletrônico e que estão relacionados aos aplicativos bancários como o recebimento de benefícios do INSS ou mesmo para aumentar a confiabilidade de sua conta, tendo níveis de acesso como bronze, ouro ou prata para acessar novos serviços, atendendo o acesso aos diversos serviços oferecidos para a sociedade e o acesso aos seus benefícios através dos bancos.

2. Alguns serviços digitais governamentais relacionados às instituições financeiras oferecidas ao cidadão

O Governo Digital no Brasil tem trabalhado em conjunto com as instituições financeiras para aprimorar o atendimento aos cidadãos, tornando os serviços mais acessíveis, eficientes e seguros. Essa colaboração se manifesta em diversas frentes.

A Plataforma Gov.br[6] é o principal portal do governo brasileiro para acesso a serviços públicos digitais. A integração com as instituições financeiras é um pilar fundamental para o atendimento ao cidadão, oferecendo os níveis de conta com diferentes direitos, protegendo a conta do cidadão. Os cidadãos podem criar ou aumentar o nível de sua conta Gov.br (para Prata ou Ouro) utilizando o login de seus bancos credenciados. Isso facilita o acesso a serviços que exigem maior segurança e validação de identidade, sem a necessidade de validação facial em alguns casos. Bancos como Banco do Brasil, Caixa Econômica Federal, Itaú, Bradesco, Santander, BRB e Sicoob já estão integrados.

Através deste portal, é possível consultar e transferir "valores esquecidos" em bancos, como o Sistema Valores a Receber (SVR) do Banco Central conforme a Resolução BCB 98, de 1º de junho de 2021, que trata sobre a remessa ao Banco Central do Brasil de informações relativas a valores a devolver a pessoas naturais e jurídicas. Esse sistema pode ser utilizado na hipótese de uma pessoa falecida que ainda não foi feito o inventário e tenha herdeiros que querem saber os valores que se encontram na conta. Para isso, o sistema pede o número do CPF e a data de nascimento do falecido, sendo necessário ter uma conta ouro. Para ter acesso a essa informação, o solicitante deve ser herdeiro(a), testamentário(a), inventariante ou representante legal e, portanto, legitimamente autorizado(a) a acessar os dados da pessoa falecida. Em caso de paternidade ou união estável pós-morte, pode ser utilizado o sistema para verificar valores a receber do falecido. A opção de verificar Valores a Receber, referente a contas encerradas e em que ainda há algum valor existente, ou Contas de Empresas encerradas, sendo necessário entrar com o número de Cadastro Nacional de Pessoa Jurídica – CNPJ e a data de abertura da empresa.

O sistema Desenrola Brasil[7] é um programa de renegociação de dívidas criado pela Lei 14.690 de 2023; o objetivo é propiciar que pessoas que estão negativadas voltem a ter condições de adquirir novas operações de crédito, sendo uma maneira do cidadão conseguir pagar suas

dívidas. O programa destina-se a negociar as dívidas compreendidas no primeiro de janeiro de dois mil e vinte e um a trinta e um do mês de dezembro de dois mil e vinte e dois. O programa é dividido em duas faixas. A faixa I é destinada a pessoas físicas com renda bruta mensal de até dois salários-mínimos ou que estejam inscritos no Cadastro Único (CadÚnico), sendo um Programa Social do Governo Federal visando atender a população de baixa renda com benefícios sociais. A faixa II é destinada a pessoas físicas, com dívidas financeiras negativadas até trinta e um de dezembro de dois mil e vinte e dois, com renda de até vinte mil reais.

O programa "CRED+" e regulamentado pela Lei 13.999 de 18 de maio de 2020, institui que oferece crédito, para microempreendedores individuais (MEIs) e pequenas empresas, que pode ser acessado no portal Gov.br na seção Portal Empresas & Negócios, oferecendo acesso a serviços e produtos financeiros, conectando empreendedores a instituições financeiras habilitadas para análise de crédito. O empresário, através do seu computador ou *smartphone,* pode realizar solicitações com diversas instituições financeiras simultaneamente, verificando qual a melhor proposta que atenda às suas necessidades financeiras, para o seu negócio. Através do Portal do Empreendedor o Microempresário Individual – MEI ou Micro e Pequena Empresa e o Artesão, permitindo escolher um serviço financeiro para o seu negócio, sendo encaminho o pedido para a instituição financeira, caso seja aceita o empreendedor recebera orientações para assinatura do contrato, sendo um serviço gratuito oferecido pelo Governo Federal.

O Pix, é instituído pela Resolução BCB 1 de 12 de agosto de 2020, que institui o arranjo de pagamentos que aprova seu regulamento sendo o sistema de pagamentos instantâneos transformou a forma como os brasileiros realizam transações financeiras, promovendo agilidade, baixos custos e ampla inclusão, basta ter uma conta bancária para ter acesso a este recurso, muito utilizado no mercado nacional.

O Sistema Financeiro Aberto – *Open Finance****[8]***, instituído pela Resolução BCB 32, de 29.10.2020, estabelece requisitos técnicos e os procedimentos operacionais para a implementação no País permitindo o compartilhamento de dados financeiros dos clientes entre diferentes instituições (com o consentimento do cliente), possibilitando a oferta de produtos e serviços mais personalizados e vantajosos, além de facilitar a gestão financeira do cidadão em um único ambiente, propiciando taxas mais acessíveis para o seu negócio. As informações de uma instituição financeira poderão ser compartilhas com as demais visando oferecer a melhor proposta para o cliente permitindo a movimentação de suas contas bancárias em diferentes plataformas e não apenas pelo aplicativo ou site do banco que possui a conta.

O cliente poderá compartilhar seus dados com outras instituições financeiras, através de plataformas, e receber novas propostas sobre os produtos financeiros em que tem interesse,

analisando a menor taxa de juros e o tempo para quitar sua negociação, respeitando a Lei Geral de Proteção de Dados, podendo ser cancelado a qualquer momento. Referente aos produtos que podem ser negociados, são eles: contas bancárias, operações de crédito, investimentos, operações de câmbio. Há previsão de serem implantados seguros e previdência. O compartilhamento das informações do cliente propicia às instituições financeiras conhecerem o cliente e oferecer produtos de acordo com sua necessidade. Este serviço atende tanto pessoas físicas como pessoas jurídicas. Este recurso está disponível no aplicativo do banco; basta apenas o cliente realizar o seu pedido, após a validação dos dados do cliente. A transmissão dos dados poderá ser feita somente entre duas instituições por vez. O cliente pode fazer transações de Pix através do *Open Finance* para pagar uma loja virtual, preservando a sua conta principal. Este serviço permite a integração entre as instituições financeiras com lojas virtuais, permitindo que o cliente ao pagar uma conta, possa verificar o seu saldo e utilizar no próprio aplicativo do lojista sem a necessidade de alterar entre aplicações do lojista e do banco, trazendo mais comodidade ao cliente.

Alguns exemplos de uso dos dados compartilhados por meio do *Open Finance* são: oferta de produtos mais rentáveis e adequados ao perfil do cliente (crédito e investimento) com taxas melhores e tarifas mais baixas; maior agilidade nas contratações dos produtos e na abertura de contas; visão consolidada dos dados das contas, dos cartões ou dos investimentos; aconselhamento financeiro; simplificação da portabilidade de salário e de crédito; entre outros.

Para permitir o compartilhamento de dados, é necessário que o cliente acesse o ambiente (aplicativo ou internet banking) da instituição que ele deseja que receba seus dados (instituição recebedora dos dados), procure pela área do *Open Finance* ou pela funcionalidade “Trazer meus dados” e selecione a instituição de onde deseja trazer os dados (instituição transmissora dos dados). Cada consentimento é dado pelo cliente de forma direta e vale somente para duas instituições (recebedora e transmissora) por vez.

Os dados não são enviados para uma estrutura centralizada, como em alguns países. No Brasil apenas a instituição recebedora de dados acessa os dados. O consentimento pode ser cancelado a qualquer momento nos ambientes digitais de qualquer uma das duas instituições envolvidas no compartilhamento. É possível realizar pagamentos com Pix, possibilitando pagamento por meio de canais mais convenientes, preservando a segurança do processo, propiciando a utilização em lojas virtuais.

As instituições financeiras fazem muitos investimentos no atendimento digital, investindo em tecnologia para melhorar a experiência do cliente, impulsionados também pelas iniciativas do governo digital. A pandemia do COVID-19 incentivou uma aceleração nos serviços digitais

das instituições financeiras, oferecendo maior número de serviços digitais que propiciam realizar as transações e serviços bancários via internet banking e aplicativos móveis, permitindo que os cidadãos realizem operações (transferências, pagamentos, investimentos, contratação de crédito).

A utilização da Inteligência Artificial (IA) e Automação: Bancos e *Fintechs* utilizam IA e automação em seus canais de atendimento (*chatbots*, assistentes virtuais) para oferecer suporte rápido e personalizado, além de otimizar processos internos.

A Segurança e Privacidade com a digitalização crescente exigem um compromisso ainda maior com a segurança da informação. As instituições financeiras e o governo trabalham para garantir a proteção dos dados dos cidadãos, em conformidade com a LGPD e a Lei do Sigilo Bancário (Lei Complementar 105/2001), utilizando tecnologias como criptografia e autenticação multifatorial.

A convergência entre o governo digital e o setor financeiro é moldada por diversas leis e regulamentações, como a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018), sendo fundamental para a proteção de dados pessoais. A LGPD estabelece princípios, direitos dos titulares e obrigações para controladores e operadores, impactando diretamente como as instituições financeiras e o governo tratam as informações dos cidadãos. Isso é crucial para serviços financeiros digitais e plataformas governamentais que lidam com dados sensíveis.

O Marco Civil da Internet (Lei 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no país, incluindo a neutralidade de rede, a privacidade e a liberdade de expressão. Embora não seja exclusiva do setor financeiro, serve como base para o desenvolvimento de serviços digitais seguros, pois a internet é uma rede mundial de computadores interligando pessoas e instituições financeiras em qualquer parte do mundo, utilizados nos aplicativos móveis.

A**s** Leis e Resoluções do Banco Central do Brasil (BCB) e do Conselho Monetário Nacional (CMN) são os principais reguladores do sistema financeiro nacional. Diversas resoluções e circulares foram emitidas para regulamentar as *Fintechs* e o *Open Finance*, visando promover a competitividade, a eficiência e a inclusão financeira.

As Sociedades de Crédito Direto (SCDs) e as Sociedades de Empréstimos entre Pessoas (SEPs), regulamentadas pelo BCB (como na Resolução 4.656/2018), permitem que *Fintechs* ofereçam crédito diretamente aos clientes ou realizem empréstimos entre pessoas, sem a intermediação de bancos tradicionais, democratizando o acesso ao crédito.

A Lei do Arranjo de Pagamentos (Lei 12.865/2013) é essencial para o surgimento de novos modelos financeiros, como as *Fintechs* de pagamento, essa lei estabelece as diretrizes para instituições de pagamento e arranjos de pagamento.

A Legislação de Combate à Lavagem de Dinheiro (Lei 9.613/1998 e Circulares do BCB): as *Fintechs* e as instituições financeiras estão sujeitas a rigorosas obrigações de identificação de clientes (KYC – *Know Your Customer*), monitoramento de transações e relatórios de atividades suspeitas para prevenir crimes financeiros.

A Estratégia de Governo Digital (Decreto 10.332/2020 e Lei 14.129/2021) define diretrizes para a digitalização de serviços públicos federais, buscando simplificar processos, reduzir burocracia e melhorar a experiência do cidadão. Isso inclui a oferta de serviços públicos digitais, identidade digital e a promoção da interoperabilidade entre sistemas governamentais. A digitalização de processos governamentais para abertura de empresas, por exemplo, reduz custos e tempo, facilitando a entrada de novas *Fintechs* no mercado e, com o aumento das transações e serviços digitais, a segurança cibernética se torna uma prioridade. Novas políticas e regulamentações (como a Política Brasileira de Cibersegurança estabelecida em dezembro de 2023) são desenvolvidas para proteger os dados e o sistema financeiro contra ataques e fraudes. Com a digitalização, exige-se um foco maior na proteção dos consumidores, especialmente em relação à privacidade dos dados, à transparência nas ofertas de serviços e ao combate a fraudes online.

O ambiente regulatório no Brasil tem se adaptado para fomentar a inovação no setor financeiro, com o Banco Central atuando como um catalisador para tecnologias como o *Open Finance*, que promovem a competição e a criação de novos produtos e serviços. A interação entre o governo digital e as instituições financeiras no Brasil é dinâmica, com a legislação buscando criar um ambiente que favoreça a inovação, a segurança e a inclusão, ao mesmo tempo em que aborda os desafios inerentes à transformação digital.

Diante do exposto, pode-se verificar que os sistemas bancários trazem uma grande quantidade de serviços que se encontram nos dispositivos móveis, e por isso se faz necessária uma gestão de riscos para uma segurança lógica (*security*) e física (*safety*) dos dispositivos móveis.

3. Gestão de riscos e pilares da segurança digital

A experiência do roubo ou furto é muito desagradável e frustrante, pois a vítima tem um sentimento de vulnerabilidade, agradecendo por sair dessa experiência negativa guardando sua vida, sendo seu bem maior, e a saúde, segundo a definição da OMS em Malta (2013) "situação de perfeito bem-estar físico, mental e social", e não apenas como a ausência de doença ou

enfermidade. Na Sociedade 4.0, o roubo, furto ou perda de um smartphone, além do custo do aparelho, nos causa vários problemas para se viver na vida cotidiana. Agenda de compromisso, organização da vida diária, pagamento de contas, sair de um determinado lugar com o auxílio de um GPS. Além de termos um terminal bancário com cartões de crédito e muitos serviços de instituições bancárias que podem atrapalhar a nossa vida financeira e nossa saúde mental.

Se faz necessário, pensar em gestão de riscos, pois coisas ruins podem acontecer, e saber quais as atitudes deverão ser tomadas ajuda a resolver os problemas. Conforme Pereira (2025) e Beck (2011), o risco é a probabilidade de um evento indesejável ocorrer devido às suas circunstâncias, no caso de dispositivos móveis há um risco iminente, pois conforme mostram os dados de assaltos apresentados na introdução, há uma probabilidade de ficar sem seu dispositivo móvel e, com isso muitas coisas ruins podem acontecer, além do custo do aparelho, transações bancárias tais como pagamentos, transferências, empréstimos, compras, entre outros. Os dados são considerados o petróleo da sociedade moderna, sendo considerados como recursos valiosos (RAIS, 2020): contatos, contas em redes sociais, fotos, vídeos, sons e outros ativos digitais. Por alguns momentos, a pessoa se sente vulnerável e com medo do que pode acontecer sem estar mais na posse do seu dispositivo móvel.

Como pilares da segurança da informação, conforme ensina Barreto (2018) e Comer (2016), os principais são os quatro: confidencialidade, disponibilidade, autenticidade e não repúdio. A confidencialidade consiste em garantir que somente pessoas autorizadas (físicas ou jurídicas) tenham acesso à informação. No caso de transações bancárias entre cliente e a instituição financeira, os sistemas de criptografia devem garantir, através de protocolos de segurança da informação, que os dados fornecidos entre as duas entidades se comuniquem. Caso haja uma interceptação dos dados através dos meios de comunicação que estão sendo utilizados, como por exemplo cabos de cobre ou sem fio (1G, 2G, 3G, 4G, 5G, 802.11 da IEEE etc.), será muito difícil saber quais são os dados que estão trafegando.

A integridade consiste em garantir que os dados que são enviados do ponto de origem, chegarão íntegros ao seu destino. Em aplicações bancárias, a integridade consiste em garantir que os dados enviados, como uma transferência bancária ou o pagamento de um pix, não sejam alterados da sua origem, que é o aplicativo do usuário, até o seu destino, o servidor da agência bancária.

A disponibilidade consiste em que o sistema esteja disponível quando o cliente deseja utilizar. O acesso da agência e conta bancária em um sistema de informação em qualquer lugar e em qualquer hora deve estar disponível para a transação bancária.

A autenticidade é garantir que o cliente que está acessando o sistema seja o proprietário da conta, validando suas credenciais, como usuário e senha no aplicativo, e pode-se adotar a validação de dois ou mais fatores, que pode ser realizada através de uma verificação biométrica, ou um desafio através de um código enviado ao cliente via SMS – *Short Message Service*, ou validar um reconhecimento de imagem do usuário pedindo para que seja capturado uma foto do seu rosto validando a pessoa que está acessando o sistema.

O não repúdio consiste impedir que a pessoas que está fazendo a transação bancária negue sua ação, em um cenário normal, em que a pessoa não esteja sob uma forte coação irresistível. Com as ferramentas existentes hoje referentes a senha, validação de biometria e algo que o cliente saiba, tal como um apelido de infância ou o nome de um amigo mais próximo, fica muito difícil negar sua autoria em situações da vida cotidiana.

Além da segurança lógica, é necessário considerar a segurança física, quando o dispositivo móvel apresenta alguma falha, como uma quebra de tela, ou mesmo seja subtraído do seu proprietário. Neste caso, faz-se necessário pensar quais as ações que devem ser adotadas, visando a proteção dos dados e reduzir as perdas referentes ao acesso indevido de contas bancárias e empréstimos que podem ser realizados enquanto o dispositivo não se encontra mais no poder de seu proprietário.

Uma configuração e fazer o fechamento para pedir autenticação do celular a cada 10 ou 15 segundos, e ativar a validação por biometria da digital. Mas, caso esteja utilizando um software de navegação, essa tela não será ativada e, neste caso poderá ter acesso a outras aplicações do dispositivo.

A vítima do furto ou roubo de seu aparelho celular, dependendo da marca do seu dispositivo, deve-se cadastrar no site do fabricante, pois os dispositivos possuem um número identificador único, intitulado IMEI – *International Mobile Equipment Identity*, que se encontra na caixa do dispositivo, ou no site do fabricante, quando o usuário cadastra seus dados, fica gravado o IMEI no site do fabricante. Um exemplo é no caso dos sistemas operacionais Android, em que tem o Google, através de uma conta do *gmail*, permite localizar o dispositivo através do GPS e de forma remota propicia bloquear o dispositivo de forma remota e apagar seus dados de forma remota, impedindo que seus dados tenham acesso indevido. Para o proprietário restaurar os dados na compra de um novo aparelho, basta restaurar a cópia de segurança (*backup*), que deve ser realizada diariamente, reduzindo os impactos negativos que este evento pode ocasionar.

Uma das medidas é ter um segundo telefone inteligente, que, nesse caso, utiliza a redundância e, caso o dispositivo seja roubado ou furtado, pegar o segundo dispositivo, ir até a

prestadora de serviço do celular e comprar um novo chip e fazer a transferência do número para o novo chip e, desta forma, restaurar as contas do aplicativo de mensagem instantânea WhatsApp ou outros aplicativos de mensagem instantânea.

4. Responsabilidade civil

A Responsabilidade Civil é dividida em objetiva e subjetiva. Na responsabilidade subjetiva, a vítima deverá comprovar o ato, dano, nexo causal, culpa ou dolo da Instituição Financeira, sendo uma tarefa difícil, pois o cliente deverá produzir provas do ocorrido, supondo uma falha de segurança de dados sensíveis protegidos pela LGPD, o cliente deveria produzir provas do ocorrido, sendo que muitas vezes está numa condição de hipossuficiência, sem conhecimentos técnicos de saber como ocorreu a falha, mas somente sofrendo com o dano ocorrido.

Já a responsabilidade objetiva, não há necessidade de fazer a prova sobre o dano, mas sim ter mera relação causal entre o comportamento e o dano que o cliente sofreu.

A Súmula 479 do STJ, as Segunda Seção, julgada em 27.06.2012, *DJe* 01.08.2012, versa que: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

O Superior Tribunal de Justiça (STJ) pacificou o entendimento de que as instituições financeiras têm responsabilidade objetiva por danos causados por fraudes e delitos de terceiros, desde que ocorram dentro das operações bancárias.

As instituições financeiras são responsáveis pelos prejuízos que o cliente sofra, mesmo que a fraude tenha sido cometida por outra pessoa, se a falha aconteceu dentro dos seus próprios sistemas ou operações, isso se aplica aos aplicativos móveis. O chamado fortuito interno refere-se a eventos imprevisíveis, mas que estão diretamente ligados à atividade da empresa. Fraudes e golpes, como clonagem de cartão, por exemplo, são considerados riscos inerentes à operação bancária.

As instituições financeiras são responsabilizadas pelos danos, independentemente de terem agido com culpa (negligência, imprudência ou imperícia). Basta que o dano tenha ocorrido. Os danos por terceiros significam que os prejuízos podem ser causados por outras pessoas que não são o banco nem o cliente, como golpistas ou hackers. A responsabilidade do banco é limitada a eventos que ocorrem durante operações como transferências, saques, pagamentos e uso de cartões.

Essa súmula é frequentemente utilizada em ações judiciais para responsabilizar bancos por situações como fraudes no PIX, clonagem de cartões de crédito e movimentações não autorizadas na conta de clientes.

5. Conclusão

As mudanças na sociedade, através do advento dos novos recursos da tecnologia da informação, estão mudando a forma de as instituições financeiras se relacionarem com o cliente, sendo que antes era mais usual ir até as agências bancárias, mas, nos dias atuais, através da evolução da velocidade das redes de computadores com as redes de 5G, que permitem uma maior velocidade nas transferências de dados de forma móvel, sem a necessidade de estar em um escritório. A modernização dos *smartphones,* propiciou que os terminais bancários pudessem ser acessados através dos dispositivos móveis, mudando o comportamento dos clientes ao se relacionar com as instituições financeiras, e também que novos tipos de fraudes surgiram, sendo necessária a criação da Súmula 479 para indicar qual a responsabilidade das Instituições Financeiras perante as fraudes a que os clientes estão sujeitos na utilização de seus sistemas de informação, permitindo uma maior segurança de uso aos seus clientes.

A tecnofilia, consiste em usuários que gostam da tecnologia da informação e têm maior facilidade e, desta forma, serão mais aderentes à utilização dos aplicativos das instituições financeiras, porém há uma parcela da população, conforme apresentado na pesquisa INAF, que são analfabetos digitais, e se faz necessário, oferecer outros meios para que tenham acesso aos serviços bancários, que irão precisar com o passar do tempo, como é o caso do acesso aos benefícios da previdência, que são depositados através de contas bancárias, sendo necessário ter alguma familiaridade com os dispositivos móveis e a utilização de recursos digitais para o pagamento de contas, tais como transferências bancárias, PIX, cartões de créditos, pois cada vez mais as cédulas monetárias estão sendo menos utilizadas. Por esse motivo, faz-se necessário o atendimento humano nas agências bancárias, para oferecer um atendimento humanizado às pessoas que não têm tanta afinidade com tecnologia. Também se faz necessário investir na educação em tecnologia da informação, visando à redução do analfabetismo digital, para melhor convivência na sociedade moderna.

6. Referências bibliográficas

AGUIAR, Carlos Eduardo Souza; SILVA, Dayana K. Melo. Tecnologia e decolonialidade: arranjos insurgentes e a questão das cosmotécnicas. *Revista Tecnologia e Sociedade*, v. 20, n. 62, p. 111-124, 2025.

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; et al. *Fundamentos de segurança da informação*. Porto Alegre: SAGAH, 2018. E-book. ISBN 9788595025875. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/]. Acesso em: 01.08.2025. p. 13.

BECK, Ulrich. Sociedade de risco*: rumo a uma outra modernidade*. São Paulo: Editora 34, 2011.

COMER, Douglas E. *Redes de computadores e internet*. 6. ed. Porto Alegre: Bookman, 2016. E-book. ISBN 9788582603734. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788582603734/]. Acesso em: 01.08.2025.

MENEZES, Wladimir Jatobá de; CASTILHO, Goiara Mendonça de; SOUZA, Wânia Cristina de. Tecnologia, multitarefas e tecnoestresse: entre a hiperconectividade e os limites da atenção, memória de trabalho e saúde mental digital. *Caderno Pedagógico*, v. 22, n. 8, p. e17627-e17627, 2025.

BRASIL. *Desenrola Brasil: programa de renegociação de dívidas do Governo Federal*. Disponível em: [https://www.gov.br/pt-br/servicos/negociar-dividas-da-faixa-i-com-o-programa-desenrola-brasil]. Acesso em: 31.07.2025.

FOLLARI, Roberto. Por fuera de la tecnofilia y la tecnofobia. *Revista Ciencias Sociales*, v. 1, n. 44, p. 17-29, 2022.

BRASIL. *Governo Digital*. Disponível em: [https://www.gov.br/governodigital/pt-br]. Acesso em: 31.07.2025.

INAF. *Indicador de Analfabetismo Funcional*. Disponível em: [https://alfabetismofuncional.org.br/]. Acesso em: 30.07.2025.

MALTA, Deborah Carvalho; SILVA JR., Jarbas Barbosa da. O Plano de Ações Estratégicas para o Enfrentamento das Doenças Crônicas Não Transmissíveis no Brasil e a definição das metas globais para o enfrentamento dessas doenças até 2025: uma revisão. *Epidemiologia e Serviços de Saúde*, v. 22, n. 1, p. 151-164, 2013.

PEREIRA, Newton Narciso; et al. Gestão de risco em um terminal portuário brasileiro usando técnicas de avaliação de risco aprimoradas pela gestão do conhecimento distribuído. *Revista Brasileira de Transportes*, v. 5, n. 1, p. 22-69, 2025.

RAIS, Diogo; PRADO FILHO, Francisco Octavio de Almeida. *Direito público digital*. São Paulo: Thomson Reuters Brasil, 2020.

REBOUÇAS, Rodrigo F. *Contratos eletrônicos*. São Paulo: Almedina, 2016. E-book. ISBN 9788584931057. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788584931057/]. Acesso em: 31.07.2025. p. 1.

SÃO PAULO (Estado). Secretaria de Segurança Pública (SSP). *Celulares subtraídos 2024* (base de dados). Disponível em: [https://www.ssp.sp.gov.br/assets/estatistica/transparencia/baseDados/celularesSub/CelularesSubtraidos_2024.xlsx]. Acesso em: 28.07.2025.

STATCOUNTER. *Platform market share (Brazil): desktop, mobile, tablet*. Disponível em: [https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/brazil]. Acesso em: 28.07.2025.

[1] StatCounter, disponível em: [https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/brazil]. Acesso em: 28.07.2025.

[2] Governo Digital, disponível em: [https://www.gov.br/governodigital/pt-br]. Acesso em: 31.07.2025.

[3] INAF – Indicador de Analfabetismo Funcional, disponível em: [https://alfabetismofuncional.org.br/]. Acesso em: 30.07.2025.

[4]E-Gov, disponível em: [https://sso.acesso.gov.br/login?client_id=portal-logado.estaleiro.serpro.gov.br&authorization_id=1985b455a25]. Acesso em: 30.07.2025.

[5]SSP – Secretaria de Segurança Pública, disponível em: [https://www.ssp.sp.gov.br/assets/estatistica/transparencia/baseDados/celularesSub/CelularesSubtraidos_2024.xlsx]. Acesso em: 28.07.2025.

[6]Gov.br, Portal do Governo Digital, disponível em: [https://www.gov.br/pt-br]. Acesso em: 30.07.2025.

[7] Desenrola Brasil, Programa de renegociação de dívidas do Governo Federal, disponível em: [https://www.gov.br/pt-br/servicos/negociar-dividas-da-faixa-i-com-o-programa-desenrola-brasil]. Acesso em: 31.07.2025.

[8] Disponível em: [https://www.bcb.gov.br/estabilidadefinanceira/openfinance].

XII. Apêndice B - Capítulo de Livro

LIVRO I SIMPÓSIO DO CONECTAJUR

O (NÃO) COMBATE À FALSIFICAÇÃO NA ERA DIGITAL NO BRASIL, QUANTO À DEFESA DAS PESSOAS FÍSICAS NA ATUALIDADE

Mario Alexandre Gazziro[9], Alessandra Oliveira de Jesus[10], Vitor da Silva Bittencourt[11], Fretz Sievers Junior[12]

INTRODUÇÃO

O ano era 2004, ainda bem no início do ano, em janeiro, quando tivemos a notícia da primeira prisão de um *hacker* no Brasil (Folha de São Paulo, 2004), por roubos cibernéticos cometidos tanto contra pessoas jurídicas quanto pessoas físicas. Mal sabia o *hacker*, que se tivesse ele cometido seus crimes de forma única e exclusivamente contra pessoas físicas, talvez jamais tivesse sido preso até hoje, final de 2025, momento no qual esse capítulo de livro foi escrito.

Sim, mais de 20 anos se passaram no Brasil e até hoje ainda não tivemos nenhum caso de prisão de *hackers* que tivessem atacado única e exclusivamente pessoas físicas - de forma a obter vantagens pecuniárias indevidas - seja por subtração direta, roubo de carteiras e contas digitais ou mesmo estelionato simples praticado por meio digital. Tal prática foi alçada à categoria virtual de crime inimputável, para o qual nada pode ser feito (alegadamente) pelas autoridades, além da orientação para registro do fato em B.O.s (boletins de ocorrência) digitais, os quais jamais vão dar início a uma investigação real, e para as vítimas mais indignadas, fazem o convite para a efetivação de um B.O. real em delegacia mais próxima a sua escolha, em um ato tão ineficaz como o registro virtual.

Tampouco os bancos ou agências de crédito chegam a devolver o dinheiro da vítima, a menos que a ação tenha sido orquestrada diretamente contra a própria instituição financeira e o perpetrador tenha conseguido seus dados diretamente pela invasão da instituição, e que nessa situação as investigações realmente são acionadas, mas nunca motivadas pelo prejuízo de uma simples pessoa física ter sido lesada e sim devido a um grupo de pessoas físicas lesadas numa invasão contra uma pessoa jurídica, parte ativa do sistema financeiro.

---

[9] Doutor em Física Computacional pela USP, professor de engenharia da informação na UFABC
[10] Programadora e especialista em segurança da informação, especializada em simular ataques cibernéticos
[11] Doutor em Administração pela UNINOVE, professor na FATEC, perito Judicial TJSP, membro da comissão de direito digital e proteção de dados da OAB
[12] Doutor em Engenharia Eletrônica pelo ITA, professor de informática e engenharia na FATEC-Mogi

[4].

Devido justamente à ausência de referências bibliográficas nacionais nesse tema intrinsecamente brasileiro, não restou muita opção aos autores desse capítulo senão a realização de uma pesquisa de campo e coleta de informações sobre os golpes, visto que praticamente nada foi publicado até o momento, nem em artigos ou mesmo eventos científicos da área de computação forense, com foco nos ataques às pessoas físicas através de execução de golpes de estelionato digital.

Para atingir seus alvos, os golpistas usam as mais diversas formas, podendo fazer uso desde ligações telefônicas para contato inicial e "oferta" do serviço relacionado ao golpe, como injeção de *links* maliciosos em propagandas falsas em e-mails de *spam*, cartazes e cartões com códigos de barras QR (*quick response*) levando sites maliciosos (os quais podem ser colocados, por exemplo, sobre equipamentos diversos como parquímetros e máquinas de pagamento de tarifas de estacionamento), ou ainda, o que é bastante comum e mais abrangente: o impulsionamento por sites de busca e redes sociais ou de notícias usando empresas de fachada para custear o impulsionamento.

Nosso estudo de caso optou por adotar essa última forma de atingir as vítimas - 'impulsionamento por sites de busca' - por ser a mais perigosa na atualidade, pois além do grande alcance, as pessoas tendem a confiar nos anúncios divulgados nessas plataformas, criando então um vínculo inicial de confiança que é devidamente explorado pelos golpistas. A estrutura completa do golpe aqui apresentado segue o fluxograma da Figura 01 abaixo:

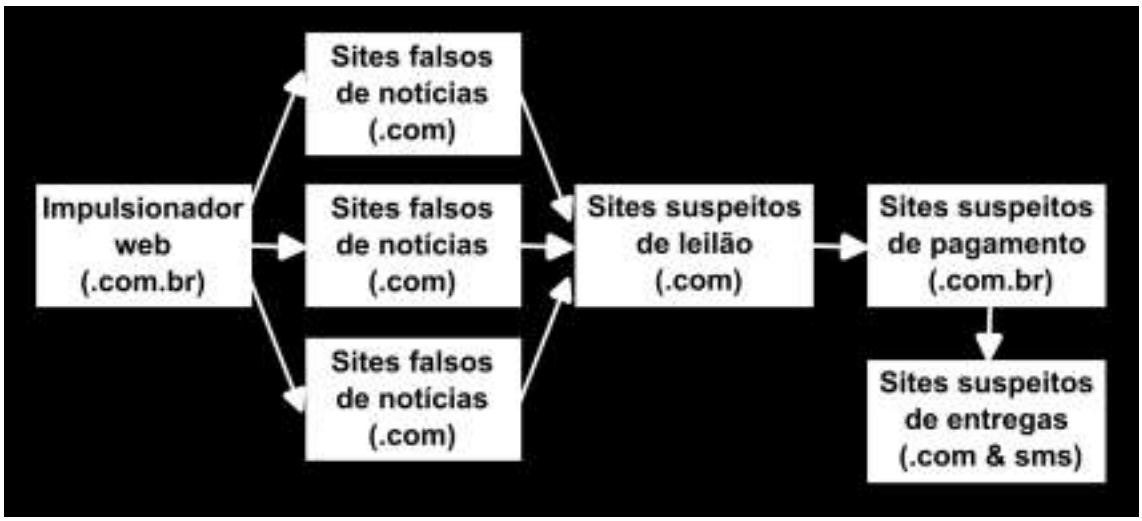


Figura 01: Fluxograma do encadeamento dos sistemas utilizados no golpe da venda falsa de aparelhos celulares provenientes de leilão (fonte da figura: autoria própria).

Destacamos ainda na Figura 01 o uso intercalado de sistemas nacionais (.com.br) e estrangeiros (.com), sendo que o uso de sistemas no exterior visa dificultar qualquer eventual ação da justiça brasileira por questões de foro internacional, sendo combinados com sistemas

nacionais apenas quando necessário para possibilitar pagamentos usando o sistema nacional **PIX** de pagamentos do banco central. Até mesmo o sistema de entregas utilizado não tem base nacional, como será devidamente apresentado ao longo do capítulo.

Na Figura 02 abaixo é possível visualizar 3 anúncios de impulsionamentos do mesmo referido golpe, todos apresentados no *feed* de notícias do Google (TM) dos autores, com chamadas que levam a diferentes *links* de notícias falsas sobre vendas de aparelhos de celulares adquiridos em 'leilões', frisando sempre que, embora se trate de leilão, não é necessário dar lances, e limitando ainda a venda a apenas um aparelho por CPF, configurando o *modus operandi* dos golpistas, que tentam dessa forma passar uma credibilidade à vítima, mas também têm o intuito de evitar que pessoas jurídicas caiam no golpe com a eventual compra no atacado, o que poderia atrair a investigação criminal devido a não lesar apenas pessoas físicas.

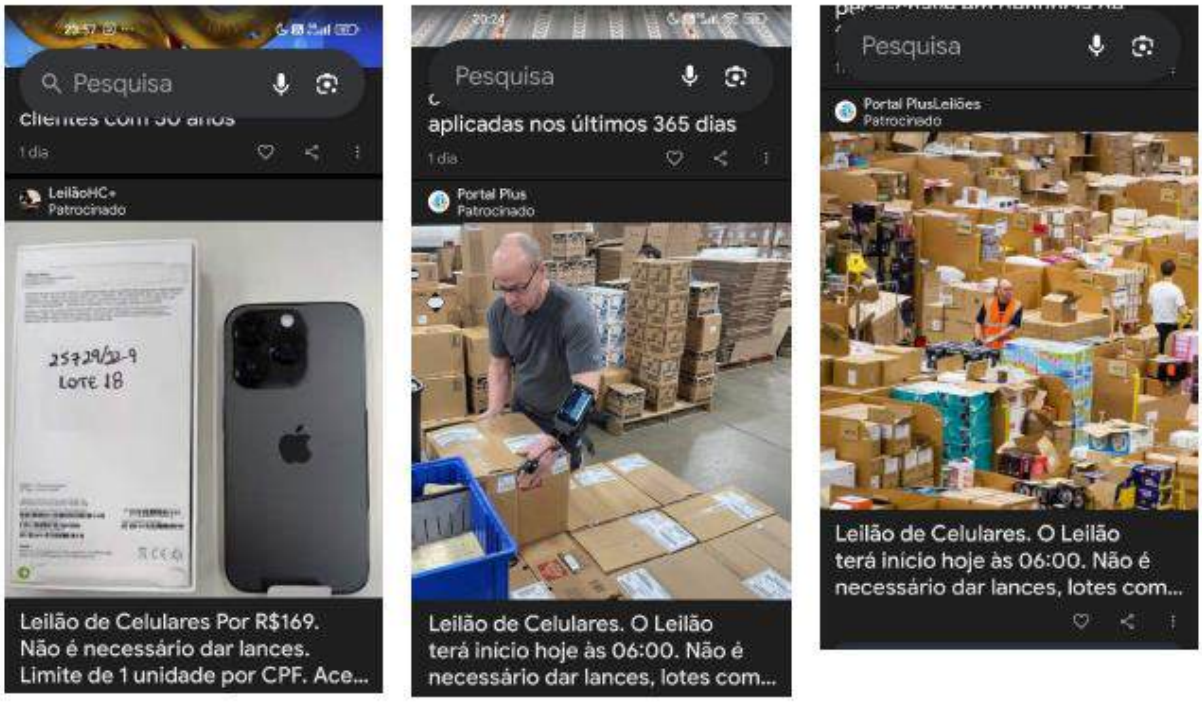


Figura 02: Notícias falsas patrocinadas impulsionadas pela plataforma Google (TM), sob responsabilidade de seus respectivos anunciantes (fonte da figura: autoria própria).

No entanto, sendo essa a primeira etapa do golpe ocorrendo em plataforma nacional, ela fica sujeita a responsabilidade dos patrocinadores do anúncio. Muitas vezes esses patrocinadores também se estabelecem no exterior, muito comumente em países como o Chipre, porém, nesse caso em particular do exemplo, encontramos um patrocinador nacional, a empresa TKG Engates, Carretas e Acessórios, como apresentado na Figura 03.

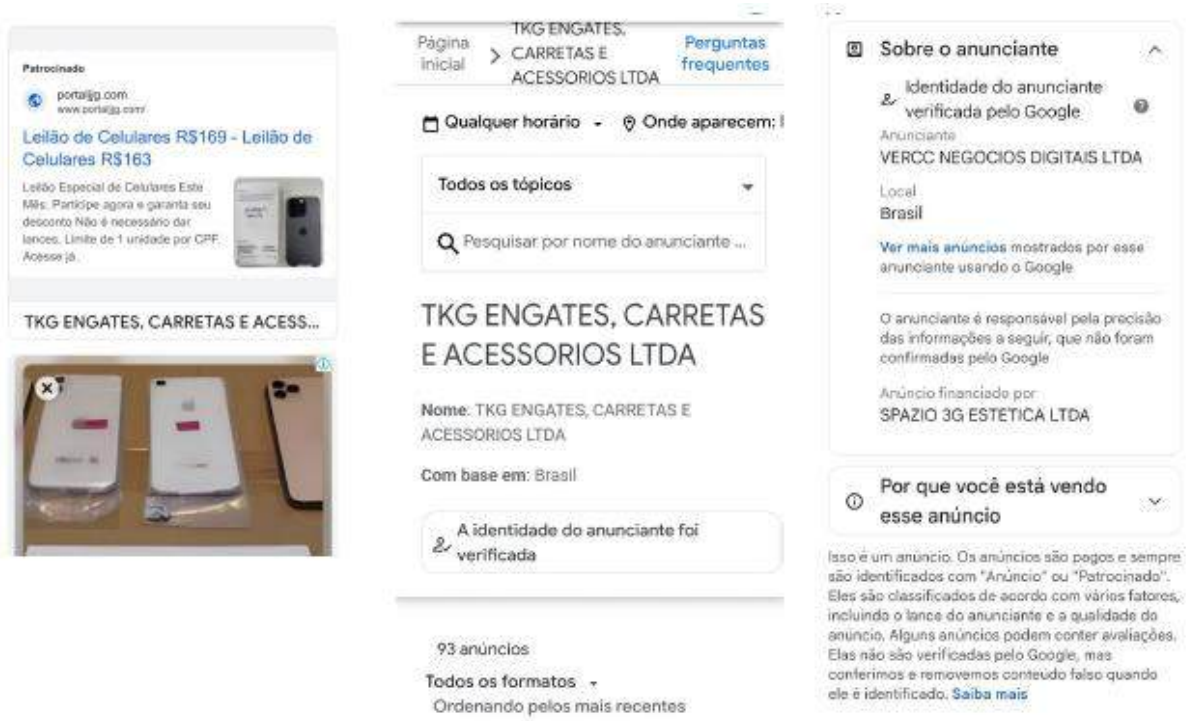


Figura 03: Indicação dos patrocinadores dos anúncios TKG Engates e Spazio 3G Estática, empresas que não são do ramo nem de tecnologia e nem mesmo de leilões (fonte da figura: autoria própria).

Muitas outras empresas que não atuam com leilão em seu ramo de atividades (tal como é o caso da TKG Engates, que opera com caminhões) aparecem como patrocinadores desses anúncios falsos, e se relacionam entre si, pois levam sempre até as mesmas notícias falsas, sendo que dos 93 anúncios recentes desse tipo de golpe, até mesmo empresas de estética foram listadas (Spazio 3G Estética), sendo provavelmente essas empresas também vítimas dos golpistas, que fazem uso não autorizado de seu CNPJ na contratação do serviço de patrocínio. Uma vez que não se tratam de empresas relacionadas à tecnologia, ficam inertes ao que acontece no mundo digital, sem imaginar que seus dados estão sendo utilizados para finalidades ilegais.

Vamos agora apresentar o próximo estágio do golpe, e talvez o mais convincente para as vítimas: as divulgações de notícias falsas, quase sempre mimetizando portais de notícia conhecidos ou empresas conhecidas de grande porte, mas todos FALSOS, hospedados em sites no exterior (meuportalofc.top e portaljjg.com), como mostra a Figura 04 a seguir.

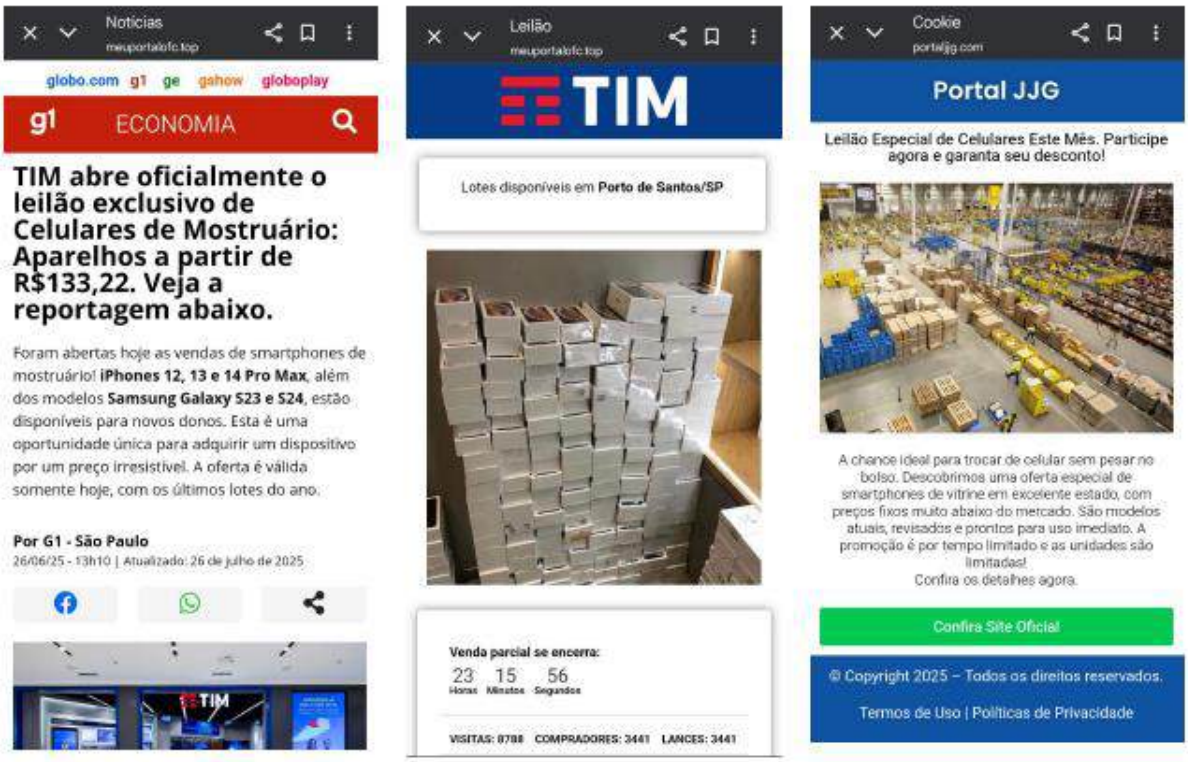


Figura 04: Sites de notícias falsas imitando empresas como G1 e TIM, ou meramente falsos como o Portal JJG, todos hospedados no exterior (fonte da figura: autoria própria).

Uma vez que o *link* para chegar nesses *sites* partiu de um buscador de notícias, seria suspeito se a primeira etapa efetiva do golpe não fosse justamente levar a vítima a um *site* de notícias falso, pois levar diretamente a um *site* de produto ou serviço, como leilão, iria causar desconfiança. Uma vez dentro do *site* falso de notícias, e já agora no domínio estrangeiro, as mentiras podem se consolidar além do escopo de atuação jurídico nacional (salvo nos casos de extradição de informações judiciais, mas escolhem países como Panamá, que estão fora desse tipo de acordo com o brasil para fazer o armazenamento dos sites falsos).

Uma vez que a vítima esteja convencida da veracidade da proposta, ela parte sem desconfiança então para a última etapa do golpe, justamente o tal portal de leilões.

Embora o domínio do *site* utilizado na compra se chame justamente pay.leilao-seguro.com (o qual de seguro não tem nada aliás, como mostra o aviso da Figura 05) e ele não seja a plataforma de propriedade dos golpistas, ele é utilizado por eles como ferramenta de prática do golpe, como apresentado na Figura 06.

Figura 05: Denúncias do portal ALEIBRAS e GOV.BR quanto ao grande risco de uso do portal de leilões chamado pay.leilao-seguro.com (fonte da figura: autoria própria).

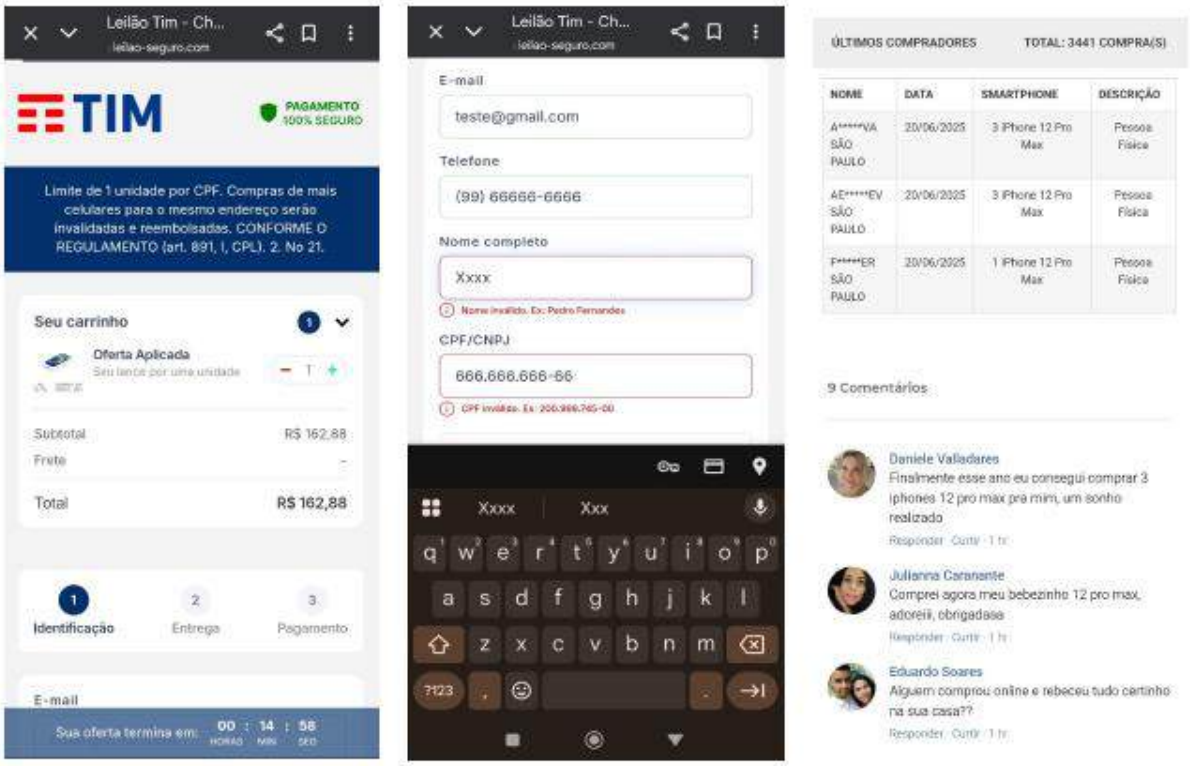


Figura 06: Site de leilão que executa a venda fraudulenta à vítima. Ele testa até mesmo o uso de CPFs fora de padrão. Notar inclusive que os portais de notícias do *link* anterior emulam opinião de falsos compradores (fonte da figura: autoria própria).

Chegando já ao final do golpe relatado, caso o pagamento da compra seja efetuado com cartão de crédito, se perde qualquer vínculo de prova com os golpistas, que farão uso de sistemas internacionais para retirada dos valores sem possibilidade de rastreio. No entanto, se o pagamento for realizado com meio de pagamento **PIX**, teremos um elo a mais na cadeia

investigativa, que é o CNPJ e/ou ou domínio da empresa recebedora ou sua chave **PIX**, necessariamente de origem nacional para uso do sistema do banco central.

E foi nessa linha que atuamos nesse estudo de caso, efetivando a compra real de um produto sabidamente falso, com o prejuízo financeiro dos autores investido em prol de levantar mais informações sobre o golpe, e também com o intuito de testar o estorno das instituições credoras e a atuação do sistema legal, conforme apresentado na Figura 07 abaixo.

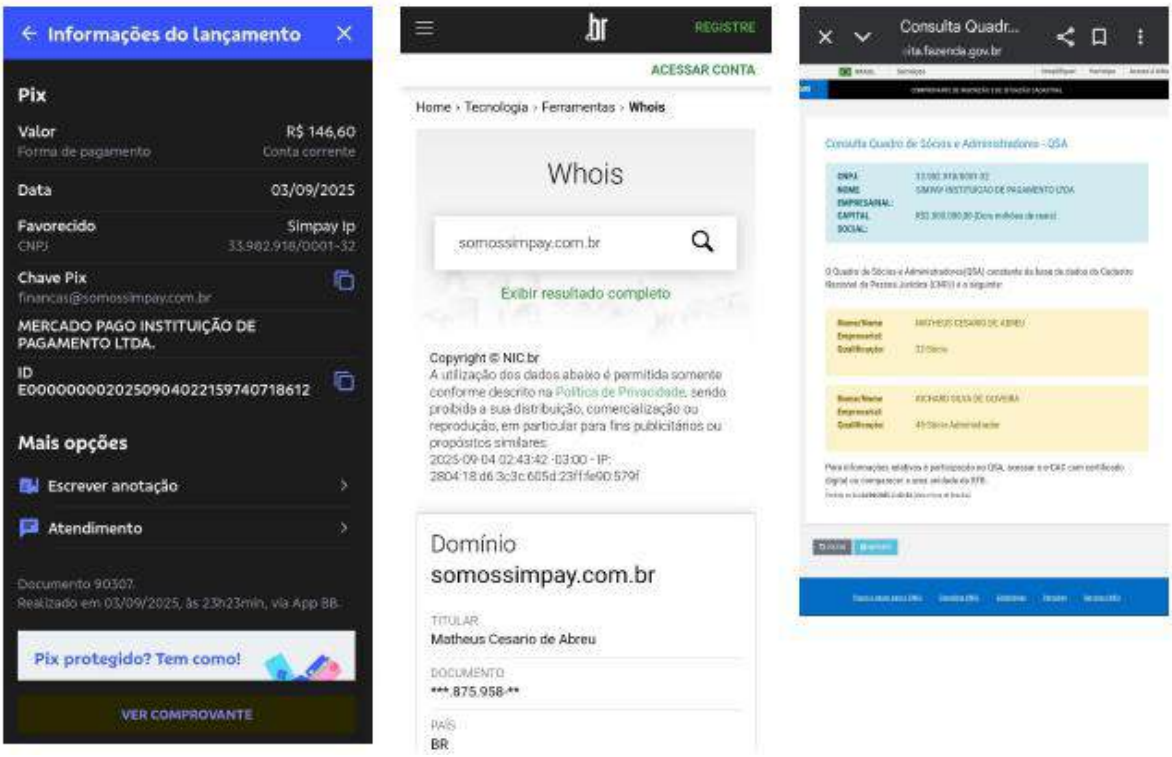


Figura 07: A chave **PIX** gerada para pagamento no site do www.leilao-seguro.com efetiva o pagamento para a empresa brasileira Simpay Ip, associada ao domínio nacional somossimpay.com.br, cujos sócios declararam capital social de 2 milhões de reais (fonte da figura: autoria própria).

No entanto, mesmo com o dinheiro sendo diretamente transferido para essa empresa, seus sócios alegam que são apenas um canal de pagamentos, e que no caso do não recebimento dos produtos ou serviços adquiridos, a vítima deve entrar em contato com o fornecedor desses produtos ou serviços para efetivação do estorno.

Figura 08: Esquema de atuação da empresa Simpay Ip para se manter longe dos holofotes dos *sites* de reclamação: devolvem dinheiro pontualmente aos poucos reclamantes. Ao final, e-mail de contato sem resposta (fonte da figura: autoria própria).

Porém, embora a reputação da tal empresa de destino dos pagamentos, a Simpay Ip, seja descrita como boa na internet, mesmo com centenas ou talvez milhares de brasileiros caindo nesse golpe todos os dias, uma busca online não retorna resultados negativos com relação a essa empresa, e nem mesmo a relaciona com os golpes.

Isso se deve pelo fato de que os proprietários monitoram os canais de reclamação, como ReclameAqui, que devolvem pontualmente os valores de pessoas que reclamam nesses canais, de forma a manter uma baixa exposição às denúncias, visto que devolver uma quantidade

pequena frente ao montante de pessoas que são vítimas do golpe os mantém fora do interesse dos investigadores corporativos, conforme apresentado na Figura 08.

Uma tentativa de contato com mensagem enviada para os e-mails informados no cadastro do domínio dessa empresa tampouco retornou alguma resposta, na qual os autores questionaram a relação deles com as vendas falsas de aparelhos de celular provenientes de leilões, ligadas a sites de notícia falsos associadas às empresas TIM e G1.

Outro aspecto importante do golpe é a falsa comunicação de envio do produto. O site de leilão utilizado para escolher o produto não gera nenhum código de rastreio para acompanhar o envio da suposta compra. Tampouco a empresa que recebe os pagamentos o faz. Porém, de forma totalmente desconectada da compra, um código de rastreio chega por mensagem de SMS no celular registrado no cadastro da compra no site de leilão, pouco tempo após a efetivação do pagamento, sem descrição da origem ou do produto rastreado, apenas uma mensagem genérica alegando que o produto foi enviado acompanhado de um código de rastreio na plataforma RotaSerena.com, conforme apresentado na Figura 09.

A plataforma RotaSerena.com, embora com site tendo nome em português e tendo sua interface inteiramente em língua portuguesa, não fica hospedada em domínio nacional, e conforme apresentado ao final da Figura 09, ela é amplamente uma plataforma reconhecida como sendo utilizada por golpistas, embora empresas idôneas façam uso dos serviços de rastreio deles também.

O rastreio então funciona por dias, inclusive apresentando trechos para a cidade correta de destino, porém, cessa o funcionamento após cerca de 1 mês e o produto nunca é entregue efetivamente. Dessa forma, acrescenta mais uma dúvida na vítima, a qual pensa que pode ter havido extravio ou furto do produto na entrega, ao passo que o sistema de rastreio era na verdade falso.

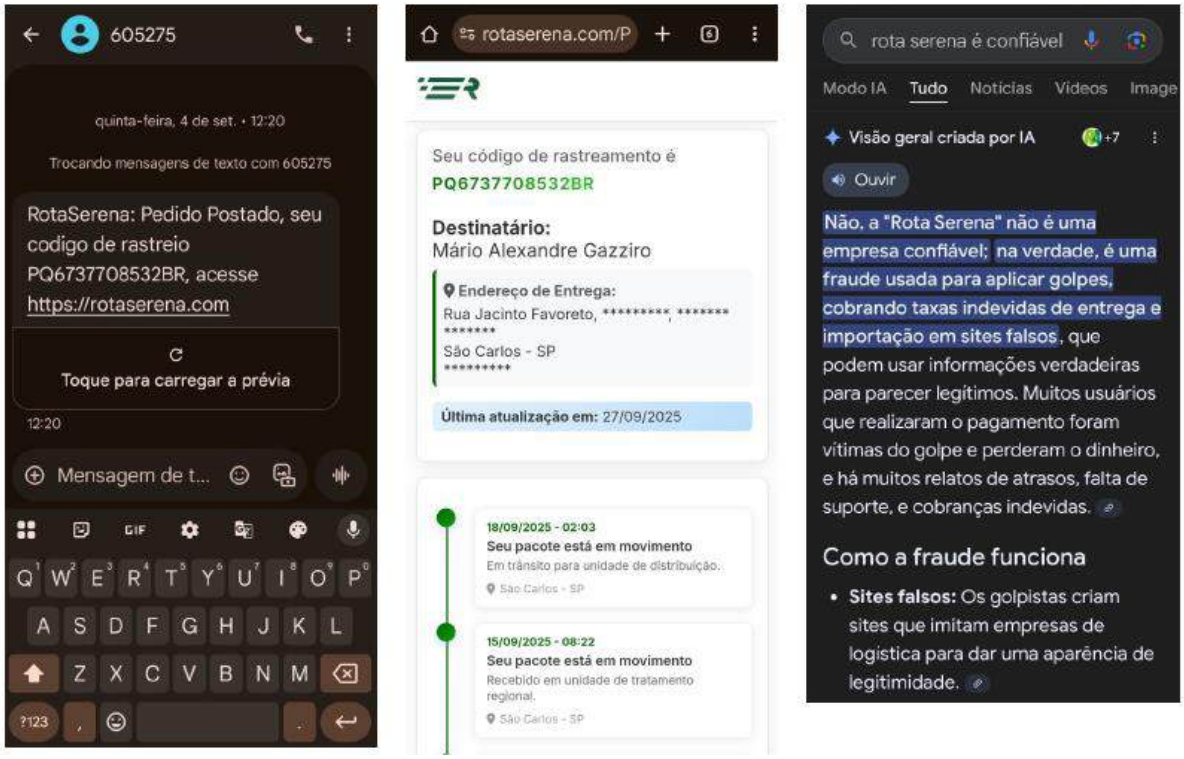


Figura 09: Falsificação do sistema de rastreio do produto usando o portal RotaSerena.com, fora do Brasil, com envio de código falso por mensagem de SMS para a vítima (fonte da figura: autoria própria).

Por fim, caminharemos para o encerramento deste capítulo mostrando os desdobramentos financeiros e criminais desse golpe. Após constatado o golpe efetivamente, vide a não entrega do produto, o término de funcionamento do código de rastreio e a ausência de resposta a todas as tentativas de comunicação, inclusive com a empresa do frete, demos início aos procedimentos para comunicação da fraude e tentativa de estorno do valor investido.

Para dar início ao procedimento de pedido de estorno bancário do valor pago usando a plataforma **PIX**, inicialmente o banco utilizado (banco do Brasil) requisitou o registro do boletim de ocorrência policial digital, conforme apresentado na Figura 10. Mesmo um relato quase tão completo do ocorrido como a própria descrição desse capítulo foi enviado ao banco, porém o pedido de estorno foi sumariamente indeferido (negado) em qualquer justificativa extra que não um aviso de ter sido negado, e sem qualquer indicação de eventual falha no relato ou documentação enviada. Simplesmente negaram o estorno de meros 146 reais num caso cristalino de golpe, algo que os autores imaginam ser relacionado ao grande número de vítimas e aos prejuízos ao banco caso seja aberta jurisprudência nesse tipo de caso.

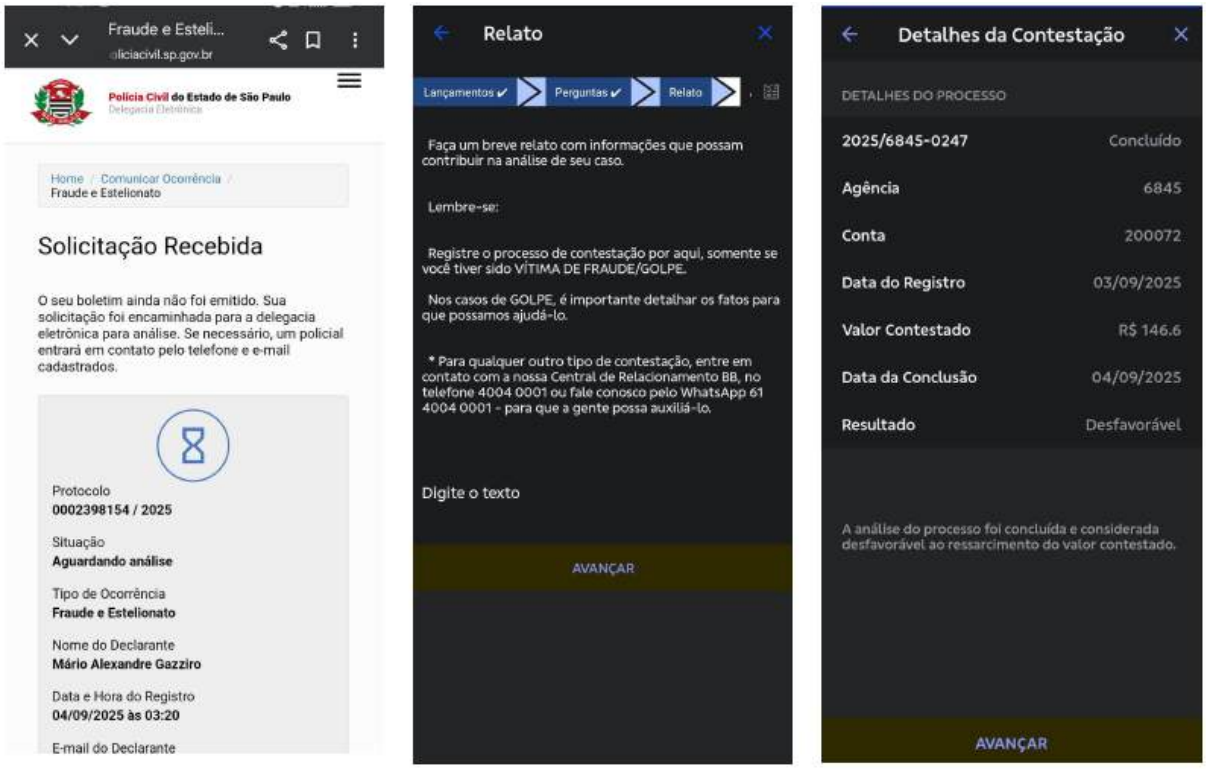


Figura 10: Elaboração do Boletim de Ocorrência digital e tentativa de estorno do valor utilizado no golpe, pedido indeferido (negado) pelo banco cerca de 24 horas após o relato e o envio do boletim de ocorrência (fonte da figura: autoria própria).

CONCLUSÃO

Apresentados todos os fatos anteriores, concluímos então que nossa hipótese inicial apresentada na introdução deste texto se faz verdadeira, visto que não há alusão ao apoio de pessoas físicas no Brasil que são vítimas de golpes de estelionato cibernético, restando as mesmas arcarem com seus prejuízos sem a chance de ressarcimento ou mesmo de aplicação da justiça aos culpados, que seguem proferindo o mesmo tipo de golpe vez sobre outra, sem risco de punição, e sem mesmo manchar a reputação de suas empresas nacionais, perfazendo um sistema de encadeamento complexo no qual as vítimas sequer conseguem inferir em qual ponto o golpe foi efetivado, sendo que na verdade todo sistema faz parte do golpe, inclusive as grandes empresas de anúncios, as quais se desoneram da responsabilidade, mesmo sendo elas que levam os golpistas até a porta de suas vítimas.

REFERÊNCIAS

EM MATO GROSSO DO SUL, ESTUDANTE DE 19 ANOS É O PRIMEIRO HACKER A SER CONDENADO À PRISÃO NO BRASIL. **Folha de São Paulo**, São Paulo, 6 de janeiro, 2004. Cotidiano. Disponível em: https://www1.folha.uol.com.br/fsp/cotidian/ff0601200415.htm. Acesso em: 22 set. 2025.

XIII. Anexo – Declaração que nada consta biblioteca

Bibliotecas UFABC (S.André)

CERTIDÃO NEGATIVA DE DÉBITOS

Sistema de Bibliotecas
Universidade Federal do ABC

Santo André,
25/03/2026

Atestamos que, na presente data, o usuário Fretz Sievers Junior, RA - SIAPE 16270, encontra-se

com a situação regular na Biblioteca podendo, por parte desta, desligar-se da Instituição sem pendências com

o SISTEMA DE BIBLIOTECAS DA UFABC.

Sem mais,

_____

Responsável - Biblioteca

COMPROVANTE USUÁRIO

Declaração gerada via internet em 25/03/26 às 17:56:00

Código de autenticidade

4327650818

Autenticidade da certidão pode ser validada em http://biblioteca.ufabc.edu.br/certidao

Bibliotecas UFABC (S.André)

CERTIDÃO NEGATIVA DE DÉBITOS

Atestamos que, na presente data, o usuário Fretz Sievers Junior, RA - SIAPE 16270, encontra-se com a situação regular na Biblioteca podendo, por parte desta, desligar-se da Instituição sem pendências com o SISTEMA DE BIBLIOTECAS DA UFABC.

Santo André, 25/03/2026

_____
Responsável - Biblioteca

Sistemas de Bibliotecas da UFABC - Vice-Reitoria - Bloco C
Av. Dos Estados nº 5001 - Bairro Bangu - Santo André - SP
CEP 09210-971 Tel.: (11) 4996-7933
E-mail: bibliotecasantoandre@ufabc.edu.br

Declaração gerada via internet em 25/03/26 às 17:56:00

Código de autenticidade

4327650818

Autenticidade da certidão pode ser validada em http://biblioteca.ufabc.edu.br/certidao