INTELIGÊNCIA ARTIFICIAL, PROTEÇÃO DE DADOS E RESPONSABILIDADE CIVIL DIGITAL NA CIBERSEGURANÇA DE APLICAÇÕES WEB

Resumo

O presente estudo analisa a segurança da informação em aplicações web no contexto da crescente dependência social, econômica e institucional das tecnologias digitais. Parte-se da constatação de que a expansão da conectividade ampliou a superfície de ataque e intensificou riscos relacionados a invasões, vazamentos de dados, indisponibilidade de serviços e uso malicioso de Inteligência Artificial. O objetivo da pesquisa consiste em examinar a evolução das ameaças cibernéticas entre 2016 e 2026, articulando fundamentos da Engenharia de Software, governança da informação, proteção de dados e educação digital de usuários. Metodologicamente, adota-se abordagem qualitativa e analítica, estruturada em revisão bibliográfica e documental, com base em literatura especializada, relatórios técnicos e normas internacionais de segurança, além da análise descritiva de dois cenários de incidentes: um caso corporativo fictício e o episódio Facebook-Cambridge Analytica. Os resultados indicam que respostas meramente reativas são insuficientes diante da sofisticação dos ataques contemporâneos, sendo necessária a adoção de estratégias preventivas, multicamadas e juridicamente orientadas. Conclui-se que a construção de ambientes web resilientes demanda integração entre codificação segura, controle de acesso, criptografia, conformidade normativa e capacitação permanente do fator humano, de modo a fortalecer a confiança digital e a proteção dos direitos fundamentais na sociedade informacional.

Palavras-chave: Segurança da informação; Aplicações web; Cibersegurança; Proteção de dados; Engenharia de *Software*.

1 INTRODUÇÃO

Com o avanço e a consolidação das tecnologias digitais, as aplicações web passaram a desempenhar um papel estrutural e indispensável na sociedade moderna. Setores essenciais como o sistema bancário, o comércio eletrônico, as instituições de ensino, os serviços de saúde e os canais de interação social operam de forma dependente da internet para o tráfego regular e a comunicação de dados corporativos e pessoais. Essa conectividade massiva, contudo, expandiu a superfície de ataque e multiplicou os riscos associados à integridade dos ativos digitais, transformando invasões de sistemas, vazamentos de dados e infecções por códigos maliciosos em ameaças corporativas perenes.

Como conceitua Stallings (2018, p. 12), "a segurança computacional envolve a proteção dos sistemas de informação contra acessos não autorizados, destruição e alteração de dados". No ambiente de aplicações web, essa premissa exige o desdobramento de arquiteturas

de defesa multicamadas capazes de salvaguardar simultaneamente a tríade conhecida como princípio CID: *confidencialidade* (garantia de acesso restrito a usuários autorizados), *integridade* (preservação contra modificações não autorizadas) e *disponibilidade* (continuidade e permanência do acesso aos serviços).

A presente pesquisa caracteriza-se como um estudo qualitativo e analítico, cujo escopo está estruturado em duas etapas metodológicas complementares. A primeira consiste em uma ampla revisão da literatura científica e documental baseada em livros de referência, artigos indexados e relatórios técnicos emitidos por agências internacionais de cibersegurança e institutos de pesquisa de mercado (como IBM Security, CrowdStrike, OWASP Foundation, Gartner e Cybersecurity Ventures) cobrindo a evolução cronológica das ameaças digitais no decênio 2016–2026. O levantamento bibliográfico foi conduzido em bases acadêmicas consagradas, incluindo Google Acadêmico, SciELO, IEEE Xplore e ScienceDirect, tomando como parâmetros de conformidade as normas reguladoras internacionais de governança da informação, notadamente a ISO/IEC 27001.

A segunda etapa metodológica apoia-se na aplicação prática dos conceitos revisados por meio da análise descritiva de dois cenários de incidentes de segurança. O primeiro constitui um estudo de caso focado em um ambiente corporativo fictício a plataforma de gestão educacional *EduTech Solutions*, desenhado para evidenciar o impacto do fator humano combinado a falhas básicas de autenticação. O segundo revisita o escândalo real e histórico envolvendo as corporações *Facebook e Cambridge Analytica* (2018), avaliando as falhas de controle de acesso a APIs e as repercussões ético-jurídicas que impulsionaram a criação de legislações globais de privacidade, a exemplo da Lei Geral de Proteção de Dados (LGPD) no Brasil.

A justificativa deste estudo reside na velocidade e na gravidade com que o cibercrime tem se reestruturado. Entre os anos de 2016 e 2026, observou-se uma transição drástica de ataques manuais e isolados para ofensivas automatizadas, ágeis e potencializadas pelo uso malicioso de ferramentas de Inteligência Artificial, reduzindo o tempo de invasão e elevando os prejuízos globais a patamares trilionários. Diante desse cenário, compreender a segurança da informação sob uma ótica integrada unindo a Engenharia de Software, as ciências jurídicas e a educação digital de usuários revela-se uma necessidade estratégica urgente para organizações públicas e privadas.

2 FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO E VULNERABILIDADES EM APLICAÇÕES WEB

A segurança da informação é definida como o conjunto estratégico de práticas, controles de engenharia, políticas institucionais e tecnologias empregadas com o propósito de blindar os ativos de dados contra ameaças multifacetadas. Segundo Palma (2020, p. 35), "a segurança da informação busca assegurar que os ativos de informação sejam acessados apenas por pessoas autorizadas". No âmbito das aplicações web sistemas hospedados em servidores remotos e acessados de forma descentralizada por navegadores via protocolo HTTP/HTTPS, essa proteção torna-se complexa devido à exposição contínua na rede pública.

A OWASP Foundation (2021, p. 7) adverte que "as vulnerabilidades em aplicações web representam uma das principais causas de comprometimento de dados na internet". De acordo com os relatórios consolidados da comunidade técnica, o espectro de ataques cibernéticos mapeia um conjunto de falhas de desenvolvimento recorrentes. Dentre as principais ameaças tecnológicas e metodológicas que comprometem esses sistemas, destacam-se:

2.1. SQL Injection (Injeção de SQL)

O ataque de *SQL Injection* manifesta-se quando a aplicação web falha na sanitização, filtragem e validação dos dados inseridos pelo usuário em campos de entrada de formulários ou parâmetros de URL. Essa lacuna permite que atacantes injetem comandos SQL maliciosos que são repassados e executados diretamente no interpretador do banco de dados relacional. Como esclarece Duckett (2014, p. 488), "falhas de validação de entrada permitem que invasores manipulem consultas SQL". Como consequência direta, o invasor pode burlar mecanismos tradicionais de autenticação, ler informações confidenciais armazenadas, modificar ou excluir registros de tabelas inteiras e, em cenários severos, obter privilégios de administrador sobre o sistema de arquivos do servidor de banco de dados.

2.2. Cross-Site Scripting (XSS)

O *Cross-Site Scripting* (XSS) configura uma vulnerabilidade de injeção na qual scripts maliciosos (geralmente escritos em JavaScript) são introduzidos em páginas web confiáveis e, posteriormente, executados no navegador de outros usuários que acessam aquela aplicação.

A OWASP Foundation (2021, p. 14) ressalta que "o XSS explora a confiança que o usuário possui em uma aplicação web". Esse vetor de ataque subdivide-se em XSS Refletido, Armazenado ou baseado no DOM, e possui capacidade para capturar cookies de sessão ativa, sequestrar *tokens* de autenticação, realizar o redirecionamento arbitrário para páginas falsas e capturar dados sensíveis digitados pela vítima em tempo real.

2.3. Phishing e Engenharia Social

Diferente das falhas puramente de programação, a engenharia social concentra-se na exploração de vulnerabilidades psicológicas e comportamentais dos usuários que operam os sistemas. Nas palavras de Mitnick (2003, p. 5), "a engenharia social explora o elo mais fraco da segurança: o ser humano".

O *phishing* representa a principal técnica operacionais dessa categoria, valendo-se do envio de e-mails, mensagens ou páginas web fraudulentas que mimetizam com precisão a identidade visual de instituições legítimas (como bancos, universidades ou órgãos governamentais). O objetivo reside em induzir a vítima a erro, motivando-a a entregar voluntariamente credenciais de acesso, chaves criptográficas, senhas e informações de identificação pessoal.

2 MECANISMOS DE DEFESA E BOAS PRÁTICAS DE PROTEÇÃO

Para conter a proliferação dessas ameaças, a Engenharia de *Software* e a Segurança da Informação estruturam um conjunto de barreiras tecnológicas e de processos fundamentais:

- **Criptografia de Dados:** Consiste na aplicação de funções matemáticas que transformam dados legíveis em texto cifrado, ilegível para terceiros desprovidos da chave secreta de decodificação. Stallings (2018, p. 203) afirma que "a criptografia é um dos mecanismos mais importantes para proteção da confidencialidade dos dados". Na camada de transporte web, a implementação obrigatória do protocolo HTTPS (*Hypertext Transfer Protocol Secure*), amparado pelos padrões TLS/SSL, garante o sigilo e a integridade do tráfego entre o cliente e o servidor.
- **Autenticação Robusta e Controle de Acesso:** Mecanismos destinados a auditar e validar a real identidade dos usuários antes de conceder acesso aos recursos internos.

Anderson (2020, p. 91) postula que "o controle de acesso é essencial para limitar privilégios e reduzir riscos de invasão". As boas práticas exigem a adoção de políticas de senhas complexas, gerenciamento rigoroso de sessões e a obrigatoriedade de Autenticação Multifator (MFA), combinando fatores de conhecimento (senhas), posse (*tokens*, aplicativos autenticadores) ou inerência (biometria).

- **Gerenciamento de Patches e Atualizações:** Manutenção preventiva contínua voltada à correção de vulnerabilidades conhecidas em bibliotecas de terceiros, frameworks, sistemas operacionais e servidores web. Hardwares e softwares desatualizados tornam-se alvos fáceis para códigos maliciosos (*malwares*) e ferramentas de exploração automatizadas (*exploits*).
- **Segurança no Ciclo de Vida do Desenvolvimento (*Secure SDLC*):** Integração do paradigma *Security by Design*, preconizando que a segurança não deve ser um adendo corretivo aplicado após a conclusão do software, mas sim um requisito estrutural incorporado desde as fases de concepção, modelagem de ameaças e codificação inicial do projeto.

4 O PANORAMA REGULATÓRIO INTERNACIONAL DA PROTEÇÃO DE DADOS

O avanço exponencial das ameaças cibernéticas e os impactos gerados por vazamentos em massa impulsionaram o desenvolvimento de marcos regulatório global voltado à privacidade digital e ao tratamento ético de dados pessoais. No Brasil, a Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece que os agentes de tratamento possuem a obrigação legal de adotar medidas administrativas e técnicas aptas a salvaguardar os dados contra acessos não autorizados e incidentes destrutivos (Brasil, 2018). A fiscalização destas obrigações cabe à Autoridade Nacional de Proteção de Dados (ANPD).

Para compreender as convergências e as particularidades do ecossistema legal internacional de proteção à privacidade, estruturam-se os Quadros 1 e 2:

Quadro 1: Lei, país e característica

País/Região	Legislação	Ano	Objetivo Principal	Principais Características	Órgão Responsável
Brasil	LGPD (Lei Geral de Proteção de	2018	Proteger dados pessoais e privacidade	Consentimento do usuário, proteção de dados,	Autoridade Nacional de Proteção de

	Dados)			penalidades por vazamento	Dados
Brasil	Marco Civil da Internet	2014	Regulamentar uso da internet	Privacidade, neutralidade da rede, direitos digitais	Governo Federal
União Europeia	GDPR (General Data Protection Regulation)	2018	Garantir proteção de dados pessoais	Direito ao esquecimento, consentimento explícito, alta fiscalização	Comissão Europeia
Estados Unidos	CCPA (California Consumer Privacy Act)	2020	Garantir controle dos dados ao consumidor	Direito de acesso e exclusão de dados	Estado da Califórnia
Canadá	PIPEDA	2000	Regular uso de dados pessoais por empresas	Consentimento e transparência no tratamento de dados	Governo Canadense
China	PIPL (Personal Information Protection Law)	2021	Fortalecer proteção de dados digitais	Controle rigoroso de dados e transferência internacional	Governo Chinês
Reino Unido	UK GDPR	2021	Proteção de dados após Brexit	Regras semelhantes ao GDPR europeu	Information Commissioner's Office
Estados Unidos	HIPAA	1996	Proteger dados médicos e hospitalares	Segurança de informações de saúde	Departamento de Saúde dos EUA

Fonte: Adaptado OWASP Foundation,2021.

Quadro 2: Comparação Geral

Aspecto	LGPD (Brasil)	GDPR (Europa)	CCPA (EUA)	PIPL (China)
Consentimento do usuário	Sim	Sim	Parcial	Sim
Direito à exclusão de dados	Sim	Sim	Sim	Sim
Aplicação internacional	Sim	Sim	Limitada	Parcial
Penalidades financeiras	Sim	Muito altas	Sim	Sim
Proteção de crianças	Sim	Sim	Parcial	Sim
Fiscalização específica	Sim	Sim	Sim	Sim

Fonte: Adaptado OWASP Foundation,2021

Embora existam distinções operacionais e geográficas entre as leis com a GDPR europeia ostentando um caráter mais rigoroso e punitivo e a CCPA estadunidense adotando uma ótica voltada às relações de consumo de caráter regional —, todas convergem para a premissa de que a segurança digital é indissociável da regulação adequada (Anderson, 2020). A tendência global caminha para o endurecimento normativo, impondo pesados encargos de governança digital para prevenir vazamentos ilícitos.

5 A EVOLUÇÃO CRONOLÓGICA DAS AMEAÇAS E IMPACTOS ECONÔMICOS (2016–2026)

O decênio compreendido entre os anos de 2016 e 2026 marcou uma transformação profunda na sofisticação dos ataques virtuais. Os relatórios históricos indicam que as táticas baseadas em invasões genéricas cederam espaço a infiltrações velozes, automatizadas e impulsionadas por inteligência artificial generativa de caráter malicioso. Para mapear essa evolução técnico-cronológica e mensurar os impactos financeiros gerados pelo cibercrime, consolidam-se os dados no Quadro 3 e no Quadro 4:

Quadro 3: Cronológico de Dados sobre Ataques Cibernéticos

Ano	Dados sobre invasões de sistemas	Fonte
2016	Crescimento dos ataques relacionados à computação em nuvem e edge computing, destacando novos riscos de segurança digital.	
2017	Estudos apontaram crescimento contínuo de eventos de malware detectados em redes governamentais e corporativas.	
2018	Caso Facebook/Cambridge Analytica expôs dados de aproximadamente 87 milhões de usuários.	Investigações internacionais e Congresso dos EUA
2019	Crescimento global de ataques ransomware contra empresas e instituições públicas.	Relatórios IBM e Verizon
2020	Ataques durante a pandemia aumentaram significativamente devido ao trabalho remoto.	Relatórios Microsoft Security
2021	O relatório OWASP destacou vulnerabilidades críticas em aplicações web como principal vetor de invasão.	OWASP Foundation
2022	Crescimento expressivo de ataques contra infraestruturas críticas e serviços em nuvem.	Relatórios CrowdStrike
2023	O tempo médio de movimentação lateral de invasores caiu para cerca de 84 minutos.	Crowd Strike Global Threat Report
2024	O custo médio global de vazamento de dados ultrapassou US$ 4 milhões.	IBM Cost of a Data Breach Report
2025	IBM registrou aumento de 49% nos grupos ativos de ransomware.	
2025	Mais de 300 mil credenciais de contas ChatGPT foram expostas por malwares do tipo infostealer.	
2025	O número de ataques iniciados pela exploração de aplicações públicas aumentou 44%.	
2026	83% das violações de segurança envolveram uso de inteligência artificial por atacantes.	
2026	Ataques passaram a ocorrer até quatro vezes mais rápido que em anos anteriores.	
2026	O tempo de invasão e movimentação lateral caiu para apenas 29 minutos em alguns casos.	

Fonte: Adaptado do Relatório da IBM Security, 2025/2026.

Quadro 4: Prejuízo Global Estimado (2016-2026)

Ano	Prejuízo Estimado Global	Fonte
2016	Aproximadamente US$ 450 bilhões	Fórum Econômico Mundial
2017	Cerca de US$ 600 bilhões	McAfee
2018	Mais de US$ 1 trilhão em perdas relacionadas a vazamentos e fraudes digitais	Relatórios internacionais
2019	Crescimento global do ransomware gerando bilhões em perdas corporativas	IBM
2020	Mais de US$ 1 trilhão durante a pandemia	Interpol
2021	Aproximadamente US$ 6 trilhões globalmente	Cybersecurity Ventures

2022	Mais de US$ 7 trilhões	Relatórios globais de cibersegurança
2023	Cerca de US$ 8 trilhões	Statista
2024	Aproximadamente US$ 9,5 trilhões	IBM
2025	Estimativa superior a US$ 10 trilhões	Cybersecurity Ventures
2026	Previsão próxima de US$ 12 trilhões anuais	Relatórios internacionais de segurança digital

Fonte: Adaptado do Relatório da IBM Security, 2025/2026.

A análise dos dados denota o caráter hiperbólico do crescimento do prejuízo econômico, projetado para atingir patamares próximos a US$ 12 trilhões anuais (BRASIL, 2014). De acordo com os relatórios analíticos do *IBM Cost of a Data Breach Report* (2024), a média geral do impacto financeiro direto de um único incidente de vazamento estrutural estabilizou-se em US$ 4,45 milhões (BRASIL, 2014). A severidade desses custos é diretamente influenciada pelo setor corporativo afetado, conforme demonstrado no Quadro abaixo:

Quadro 5: Setores mais afetados

Setor	Prejuízo Médio
Saúde	Mais de US$ 10 milhões
Financeiro	Aproximadamente US$ 6 milhões
Tecnologia	Cerca de US$ 5 milhões
Educação	Milhões em paralisações e recuperação

Fonte: Adaptado do Relatório da IBM Security, 2025/2026

O setor de saúde encabeça os prejuízos devido à natureza crítica de seus dados (prontuários médicos possuem alta valoração comercial no mercado ilegal da *dark web*) e à urgência operacional de reaver o controle dos sistemas em cenários de ransomware(BRASIL, 2014). Eventos históricos emblemáticos atestam essa destrutividade: o ataque massivo do ransomware *WannaCry* (2017) infligiu prejuízos estimados entre US$ 4 e 8 bilhões ao redor do globo, impactando severamente a rede de hospitais públicos do Reino Unido (NHS)(BRASIL, 2014). Em 2021, a paralisão cibernética da infraestrutura de oleodutos da *Colonial Pipeline*, nos Estados Unidos, forçou o pagamento emergencial de resgate na ordem de US$ 4,4 milhões para evitar o colapso logístico de combustíveis na costa leste norte-americana(BRASIL, 2014).

6 MAPEAMENTO DE INTERESSES E ALVOS PRIORITÁRIOS DA ATIVIDADE HACKER

A motivação do cibercrime contemporâneo é multifacetada, distribuindo-se entre a obtenção de lucros financeiros diretos, espionagem geopolítica, interrupção de serviços estratégicos e ativismo político (*hacktivismo*)(BRASIL, 2014). De acordo com os indicadores do *World Cybercrime Index* (WCI) compilados nos relatórios analíticos de 2026, os polos de origem das ameaças e os interesses prioritários mapeiam dinâmicas específicas(BRASIL, 2014). O Quadro 4 detalha a distribuição das maiores atividades cibernéticas por nações, enquanto o Quadro 6 esquematiza o foco de interesse por alvo:

Quadro 6: Principal interesse dos hackers

Alvo	***Principal Interesse dos Hackers***
Bancos	Dinheiro e dados financeiros
Hospitais	Dados médicos
Governos	Informações estratégicas
Empresas de tecnologia	Dados e sistemas
Escolas e universidades	Dados acadêmicos
Infraestruturas críticas	Controle de serviços essenciais
Usuários comuns	Senhas e fraudes
E-commerce	Cartões e pagamentos
Sistemas em nuvem	Dados corporativos
Criptomoedas	Roubo financeiro digital

Fonte: autoral, 2026.

Paralelamente, a dinâmica de vulnerabilidade indica que os países detentores de estruturas econômicas amplamente digitalizadas tornam-se os alvos preferenciais devido ao volume de dados expostos e à dependência crítica de sistemas virtuais(BRASIL, 2014). Conforme relatórios emitidos pela *Microsoft Security* e pela *CloudSEK* (2025), o ranking de nações mais atacadas destaca os Estados Unidos (devido à sua massiva infraestrutura digital), o Reino Unido (setor financeiro centralizado), a Alemanha (indústria tecnológica avançada), Israel (conflitos geopolíticos persistentes) e a Polônia (alvo frequente de hacktivismo decorrente de tensões regionais na Europa Oriental)(BRASIL, 2014).

7 A ATUAÇÃO DA ENGENHARIA DE SOFTWARE NA MITIGAÇÃO DE RISCOS DIGITAIS

Diante da hostilidade do ecossistema cibernético contemporâneo, a atuação do engenheiro de software transcende a mera escrita de códigos lógicos para consolidar-se como elemento estratégico fundamental de defesa organizacional(BRASIL, 2014). Como postula

Pressman (2016, p. 32), "a qualidade do software depende diretamente dos processos adotados durante seu desenvolvimento"(BRASIL, 2014). A engenharia contemporânea atua de forma estruturada em múltiplas frentes de segurança, conforme resumido no Quadro 7:

Quadro 7: Resumido da Atuação do Engenheiro de Software

Área	Atuação
Desenvolvimento seguro	Criação de sistemas protegidos
Testes de segurança	Identificação de vulnerabilidades
Proteção de dados	Implementação da LGPD e criptografia
Autenticação	Controle seguro de acesso
Monitoramento	Detecção de ataques
Inteligência artificial	Automação da segurança
Educação digital	Conscientização de usuários
Arquitetura segura	Infraestrutura resiliente

Fonte: autoral, 2026.

A aplicação de modelos preditivos baseados em IA pelo engenheiro de software (Russell, 2021) permite rastrear atividades em frações de segundo, identificando invasões de forma precoce (BRASIL, 2014). Adicionalmente, amparado por diretrizes éticas internacionais de computação, como o *ACM Code of Ethics* (2018), o profissional assume o compromisso deontológico de priorizar a privacidade e a segurança digital como garantias indissociáveis do bem-estar social (BRASIL, 2014).

8 ANÁLISE DE CENÁRIOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.1. Estudo de Caso: O Incidente na *EduTech Solutions* (Cenário Corporativo Fictício)

A empresa fictícia denominada *EduTech Solutions* atuava no mercado de desenvolvimento e hospedagem de plataformas web voltadas à gestão educacional integrada, atendendo a uma vasta carteira de escolas, professores, alunos e responsáveis legítimos (BRASIL, 2014). A aplicação concentrava um banco de dados sensível composto por registros cadastrais, documentos financeiros de mensalidades, notas estudantis e históricos acadêmicos confidenciais (BRASIL, 2014). Devido ao crescimento acelerado da demanda comercial, a diretoria expandiu a infraestrutura lógica do sistema sem promover investimentos proporcionais em governança de cibersegurança e auditoria de sistemas (BRASIL, 2014).

O incidente de segurança materializou-se quando um colaborador lotado no setor administrativo foi alvo de uma manobra de engenharia social baseada em *spear phishing*(BRASIL, 2014). O funcionário recebeu um e-mail com identidade visual idêntica à do departamento de tecnologia interno, alegando a necessidade urgente de recadastramento de senhas devido a uma suposta manutenção corretiva do sistema (BRASIL, 2014). Induzido a erro, o colaborador acessou o link malicioso contido na mensagem e digitou suas credenciais corporativas no formulário clonado (BRASIL, 2014).

A análise pericial realizada após o ataque descortinou uma série de falhas na arquitetura da empresa, caracterizadas nos seguintes pontos:

1. **Frabilidade na Autenticação:** A aplicação web requeria unicamente o uso de senhas estáticas convencionais para a concessão de acessos administrativos, inexistindo qualquer camada de autenticação em dois fatores (MFA) que pudesse invalidar o uso das credenciais capturadas pelos criminosos (Anderson, 2020).
2. **Defasagem em Educação Digital:** A organização omitia a realização de programas de conscientização periódica de seus recursos humanos sobre técnicas de phishing, tornando a manipulação psicológica o vetor mais eficaz para a intrusão (Mitnick, 2003).
3. **Ausência de Segmentação de Privilégios:** O perfil do usuário comprometido detinha permissões irrestritas no banco de dados. Diante disso, após realizarem o login ilícito, os invasores moveram-se lateralmente pelas tabelas, realizando a exfiltração em massa de dados acadêmicos e pessoais de milhares de alunos e aplicando travas criptográficas (ransomware) na plataforma(BRASIL, 2014).

Os impactos para a *EduTech Solutions* incluíram a interrupção completa das atividades escolares por dias, perda de contratos comerciais por quebra de reputação, custos elevados com equipes forenses de resposta a incidentes e a abertura de processos administrativos sancionatórios junto à ANPD por violação direta aos preceitos protetivos da LGPD (Brasil, 2018; BRASIL, 2014). Posteriormente, a empresa reestruturou seu parque tecnológico, adotando criptografia integral em repouso e em trânsito (Stallings, 2018), MFA mandatório para todos os funcionários e auditorias contínuas de logs (BRASIL, 2014).

8.2. Caso Real Paradigmático: O Escândalo *Facebook / Cambridge Analytica* (2018)

No cenário internacional histórico, o episódio envolvendo a Meta Platforms (à época, Facebook Inc.) e a consultoria política britânica *Cambridge Analytica* (2018) figura como o principal marco de vulnerabilidade nas políticas de controle de acesso de dados e privacidade da história moderna(BRASIL, 2014). O escândalo revelou que a rede social permitia que desenvolvedores terceiros extraíssem de forma automatizada perfis de usuários por meio de APIs sob o pretexto de pesquisas acadêmicas(BRASIL, 2014). Através de um aplicativo de teste de personalidade, dados de aproximadamente 87 milhões de indivíduos foram coletados sem o devido consentimento e utilizados para traçar perfis psicográficos direcionados a campanhas de marketing político manipulativo (BRASIL, 2014).

Como denunciou o cientista de dados e *whistleblower* Christopher Wylie (2019, p. 1), "nós exploramos o Facebook para coletar milhões de perfis de pessoas"(BRASIL, 2014). O incidente forçou o pronunciamento do CEO da Meta, Mark Zuckerberg (2018, p. 2), admitindo a falha ética e institucional: "temos a responsabilidade de proteger seus dados, e se não pudermos, não merecemos servi-los" (BRASIL, 2014).

O episódio evidenciou que a ausência de mecanismos rigorosos de monitoramento pós-coleta e a excessiva permissividade na concessão de privilégios a aplicações de terceiros constituem vetores críticos de vulnerabilidade sistêmica, violando as premissas essenciais de controle preconizadas pela OWASP Foundation (2021). Esse marco histórico funcionou como o catalisador definitivo para a aceleração de leis globais severas, impulsionando a vigência imediata da GDPR no continente europeu e servindo de espinha dorsal doutrinária para a positivação da LGPD no território brasileiro (BRASIL, 2014).

9 DISCUSSÃO

A convergência dos dados evolutivos levantados entre 2016 e 2026 expõe uma realidade indiscutível: a segurança da informação desvinculou-se definitivamente de uma abordagem puramente operacional para consolidar-se como elemento de governança corporativa e soberania digital (BRASIL, 2014). A aceleração exponencial dos prejuízos econômicos saltando de bilhões para a projeção trilionária de US$ 12 trilhões reflete a mudança no perfil do cibercriminoso, que hoje atua amparado por ecossistemas altamente capitalizados na *dark web* e armados com automação por inteligência artificial (BRASIL, 2014).

O confronto analítico entre o estudo de caso fictício da *EduTech Solutions* e o evento real do *Facebook/Cambridge Analytica* demonstra que, independentemente do porte da

corporação, as maiores brechas raramente derivam de falhas isoladas de hardware. Elas ocorrem devido a falhas de processos e pelo menosprezo ao fator humano. O ataque à plataforma educacional evidencia que a ausência de controles básicos de engenharia (como a ausência de MFA) anula qualquer investimento em servidores modernos caso o usuário administrativo continue vulnerável à engenharia social (BRASIL, 2014).

Portanto, a discussão contemporânea exige que a Engenharia de Software adote metodologias de proteção que assumam o comprometimento do perímetro tradicional (filosofia *Zero Trust*). O desenvolvimento baseado no *Security by Design* (OWASP, 2021) e a validação contínua de conformidade jurídica com legislações como a LGPD e a GDPR não devem ser encarados pelas empresas como custos burocráticos restritivos, mas sim como mecanismos de sobrevivência mercadológica e salvaguarda da dignidade e privacidade de seus usuários (BRASIL, 2014).

CONSIDERAÇÕES FINAIS

A segurança da informação em aplicações web consolidou-se como um dos desafios mais complexos, dinâmicos e vitais na era da economia digitalizada. O mapeamento evolutivo demonstra que, à medida que os sistemas web aumentaram sua capilaridade e dependência social, a sofisticação do cibercrime expandiu-se na mesma proporção, incorporando ferramentas de inteligência artificial automatizadas capazes de desestabilizar corporações e governos em poucos minutos.

As evidências empíricas coletadas nos estudos de caso e nos relatórios econômicos internacionais reiteram que respostas puramente reativas e pós-incidentes geram prejuízos financeiros severos e danos reputacionais irreversíveis. O enfrentamento eficaz das ameaças cibernéticas contemporâneas demanda uma postura proativa e integrada, na qual o rigor técnico da Engenharia de Software (codificação segura, controle estrito de privilégios de APIs e criptografia robusta) atue em perfeita harmonia com as diretrizes normativas das leis de proteção de dados e com programas permanentes de treinamento do fator humano. Somente através dessa abordagem equilibrada entre tecnologia, direito e educação digital será possível construir ambientes virtuais resilientes, éticos e confiáveis para a sociedade contemporânea.

REFERÊNCIAS

ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT. **Association for Computing Machinery**. New York: ACM, 2018. Disponível em: https://www.acm.org/code-of-ethics. Acesso em: 26 mai. 2026(BRASIL, 2014).

ANDERSON, Ross. **Security Engineering**: a guide to building dependable distributed systems. 3. ed. Indianapolis: Wiley, 2020(BRASIL, 2014).

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 mai. 2026(BRASIL, 2014).

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 mai. 2026(BRASIL, 2014).

CALIFORNIA (State). **California Consumer Privacy Act of 2018** (CCPA). California: California Legislative Information, 2020. Disponível em: https://leginfo.legislature.ca.gov. Acesso em: 25 mai. 2026(BRASIL, 2014).

CROWDSTRIKE. **CrowdStrike Global Threat Report 2023**: Adversary velocity increases. Austin: CrowdStrike, 2023(BRASIL, 2014).

CROWDSTRIKE. **CrowdStrike Global Threat Report 2026**. Austin: CrowdStrike, 2026(BRASIL, 2014).

CYBERSECURITY VENTURES. **Official Cybercrime Report 2025/2026**. Sausalito: Cybersecurity Ventures, 2025(BRASIL, 2014).

DUCKETT, Jon. **PHP & MySQL**: server-side web development. Indianapolis: Wiley, 2014(BRASIL, 2014).

EUROPEAN UNION. **General Data Protection Regulation** (GDPR). Regulation (EU) 2016/679. Bruxelas: European Parliament, 2018. Disponível em: https://gdpr-info.eu. Acesso em: 27 mai. 2026(BRASIL, 2014).

IBM SECURITY. **Cost of a Data Breach Report 2024**. Cambridge: IBM Corporation, 2024(BRASIL, 2014).

IBM SECURITY. **X-Force Threat Intelligence Index 2026**. Cambridge: IBM Corporation, 2026(BRASIL, 2014).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Genebra: ISO, 2022.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: ataques de hackers a humanos. São Paulo: Pearson, 2003(BRASIL, 2014).

OWASP FOUNDATION. **OWASP Top Ten 2021**: the ten most critical web application security risks. Estados Unidos: OWASP, 2021. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 24 mai. 2026(BRASIL, 2014).

PALMA, André de. **Segurança da Informação**. São Paulo: Atlas, 2020(BRASIL, 2014).

PRESSMAN, Roger S.; MAXIM, Bruce R. **Engenharia de Software**: uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2016(BRASIL, 2014).

RUSSELL, Stuart. **Inteligência Artificial**: a que ponto chegamos? Rio de Janeiro: Companhia das Letras, 2021(BRASIL, 2014).

STALLINGS, William. **Computer Security**: principles and practice. 4. ed. Boston: Pearson, 2018(BRASIL, 2014).

WYLIE, Christopher. **Mindfck**: Cambridge Analytica and the plot to break America. New York: Random House, 2019(BRASIL, 2014).

ZUCKERBERG, Mark. **Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook**. Washington, DC: United States Senate Committee on the Judiciary, 2018(BRASIL, 2014)