CIÊNCIA& TECNOLOGIA
ISSN: 2525-6599
unifev pesquisa
Coordenação de Pesquisa

CIBERSEGURANÇA: UMA ABORDAGEM CONTEMPORÂNEA NA PROTEÇÃO CONTRA AMEAÇAS

Fernando Tavares Pansani Filho[1]
Fernando Kendy Aoki Rizzatto[2]

Resumo:
A cibersegurança assumiu caráter estratégico no Brasil, especialmente diante do crescimento exponencial das ameaças digitais. Levantamento da Fortinet indica que o país registrou 103,16 bilhões de tentativas de ataques cibernéticos em 2022, figurando entre os mais visados da América Latina. Episódios emblemáticos — como o ataque de ransomware ao Superior Tribunal de Justiça (2020) e a invasão à nuvem do Ministério da Saúde (2021) — evidenciam a vulnerabilidade das infraestruturas digitais nacionais e reforçam a urgência de medidas de proteção mais robustas. Dessa forma, este estudo tem como objetivo analisar a cibersegurança no Brasil e avaliar sua relevância para a proteção de infraestruturas digitais frente ao aumento das ameaças cibernéticas, investigando riscos recorrentes, práticas de defesa, arcabouço legislativo e estratégias educacionais voltadas à mitigação desses desafios. A pesquisa adota abordagem dedutiva e qualitativa, fundamentada em revisão bibliográfica e análise documental. Os resultados apontam que a mitigação de riscos não depende apenas de soluções técnicas, exigindo também o fortalecimento da governança digital, a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a incorporação de tecnologias emergentes, como inteligência artificial, blockchain e criptografia avançada. Conclui-se que a combinação de investimentos contínuos em educação digital, políticas públicas de governança e inovação tecnológica é essencial para reduzir a vulnerabilidade das infraestruturas críticas brasileiras e ampliar a resiliência diante de ataques cibernéticos.

Palavras-chave: blockchain; cibersegurança; inteligência artificial; lgpd; resiliência digital.

Abstract:
Cybersecurity has become strategic in Brazil, particularly in light of the exponential growth of digital threats. A Fortinet report indicates that the country recorded 103.16 billion attempted cyberattacks in 2022, ranking among the most targeted in Latin America. Emblematic incidents—such as the ransomware attack on the Superior Court of Justice (2020) and the breach of the Ministry of Health cloud system (2021)—highlight the vulnerability of national digital infrastructures and underscore the urgency of stronger protective measures. This study aims to analyze cybersecurity in Brazil and assess its relevance for protecting digital infrastructures amid the rise of cyber threats, investigating recurring risks, defense practices, the legal framework, and educational strategies aimed at mitigating these challenges. The research adopts a deductive and qualitative approach, grounded in bibliographic review and documentary analysis. The findings indicate that risk mitigation depends not only on technical solutions but also on strengthening digital governance, ensuring compliance with the General Data Protection Law (LGPD), and incorporating emerging technologies such as artificial intelligence, blockchain, and advanced cryptography. It is concluded that the combination of continuous investment in digital education, public governance policies, and technological

[1] Unifev - Centro Universitário de Votuporanga. Votuporanga, São Paulo, Brasil. Graduando do curso de Engenharia da Computação. Email: fkendy86@gmail.comm.
[2] Unifev - Centro Universitário de Votuporanga. Votuporanga, São Paulo, Brasil. Graduanda do curso de Engenharia da Computação. Email: fkendy86@gmail.com

innovation is essential to reduce the vulnerability of Brazil's critical infrastructures and to enhance resilience against cyberattacks.

Keywords: blockchain; cybersecurity; artificial intelligence; lgpd; digital resilience.

INTRODUÇÃO

A transformação digital experimentada nas últimas décadas revolucionou profundamente a forma como a sociedade, as organizações e os governos operam. A crescente digitalização de serviços essenciais, a ampla conectividade proporcionada pela internet e a massificação do uso de dispositivos inteligentes criaram um ecossistema tecnológico complexo e interdependente (Gartner, 2023). Neste contexto, a cibersegurança emerge como elemento fundamental para garantir a integridade, confidencialidade e disponibilidade das informações que transitam no ambiente digital (Schneier, 2020).

O Brasil, como uma das maiores economias digitais do mundo, enfrenta desafios significativos no campo da cibersegurança. O país registrou números alarmantes de tentativas de ataques cibernéticos nos últimos anos, consolidando-se como um dos alvos preferenciais de cibercriminosos na América Latina. Esta vulnerabilidade não se restringe apenas ao setor privado, mas atinge também infraestruturas críticas governamentais, colocando em risco serviços essenciais à população e comprometendo a soberania digital nacional.

Os ataques ao Superior Tribunal de Justiça em 2020 e ao Ministério da Saúde em 2021 representam marcos que evidenciam a fragilidade das defesas cibernéticas brasileiras e a necessidade urgente de implementação de estratégias robustas de proteção. Estes incidentes não apenas causaram prejuízos financeiros e operacionais imediatos, mas também expuseram a carência de políticas integradas de segurança e a insuficiência de investimentos em tecnologias de proteção.

Diante deste panorama, torna-se imperativo compreender as múltiplas dimensões da cibersegurança no contexto brasileiro, abrangendo desde as características técnicas das ameaças até os aspectos regulatórios, educacionais e de governança que compõem um sistema efetivo de proteção digital. A abordagem contemporânea da cibersegurança transcende a mera implementação de soluções tecnológicas, exigindo uma visão holística que integre pessoas, processos e tecnologias.

Dessa maneira, o objetivo desta pesquisa foi analisar a cibersegurança no Brasil sob uma perspectiva contemporânea, avaliando sua importância estratégica para a proteção das infraestruturas digitais nacionais diante do crescimento exponencial das ameaças cibernéticas.

1 METODOLOGIA

Este trabalho adota uma abordagem dedutiva e qualitativa, fundamentada em revisão bibliográfica sistemática e análise documental de fontes primárias e secundárias. A escolha metodológica justifica-se pela natureza do objeto de estudo, que demanda a compreensão de fenômenos complexos e multidimensionais relacionados à cibersegurança no contexto brasileiro.

A revisão bibliográfica abrangeu publicações cientificas em periódicos especializados, livros técnicos, relatórios de organizações internacionais de referência na área de segurança cibernética, e documentos oficiais de órgãos governamentais brasileiros. Foram consultados bases de dados acadêmicos, repositórios institucionais e sites oficiais de entidades como Gabinete de Segurança Institucional (GSI), a Autoridade Nacional de Proteção de Dados (ANPD) e organismos institucionais como o National Institute of Standards and Technology (NIST) e a International Organization for Standardization (ISO).

A análise documental inclui legislações brasileiras pertinentes, como destaque para a Lei n° 13.709/2018 (LGPD), o Decreto n° 12.572/2025 (Política Nacional de Segurança da Informação) e o Decreto n° 12.573/2025 (Estratégia Nacional de Cibersegurança). Também foram examinados relatórios técnicos de empresas especializadas em cibersegurança, como Fotinet, Kaspersky, IBM e Checkpoint, que fornecem dados estatísticos e análise sobre tendências de ameaças.

A coleta de dados privilegiou informações atualizadas, com recorte temporal concentrado no período de 2020 a 2025, período marcado por transformações significativas no cenário de cibersegurança brasileiro, incluindo a implementação da LGPD e a ocorrência de ataques emblemáticos a instituições públicas. Este recorte temporal permite uma análise contemporânea e contextualizada das questões abordadas.

A análise dos dados foi realizada mediante triangulação de fontes, confrontando informações de diferentes origens para garantir a confiabilidade e validade dos achados. Os conceitos teóricos foram articulados com casos práticos documentados, permitindo uma compreensão integrada entre teoria e realidade empírica.

Quanto aos aspectos éticos, este estudo baseou-se exclusivamente em dados de domínio público, não envolvendo coleta de informações sensíveis ou identificação de indivíduos, respeitando assim os princípios de confidencialidade e privacidade estabelecidos pela legislação brasileira.

2 CONTEXTUALIZAÇÃO DA CIBERSEGURANÇA NO BRASIL

2.1 Panorama Histórico da Segurança Digital

Segundo a Estratégia Nacional de Cibersegurança (E-Ciber) A evolução da cibersegurança no Brasil acompanha a própria trajetória de digitalização da sociedade brasileira. Nas últimas três décadas, o país experimentou transformação significativa em sua infraestrutura tecnológica, transitando de uma realidade de conectividade limitada para um cenário de ampla penetração digital em todos os setores econômicos e sociais.

Conforme documentos institucionais do Governo Federal, os primeiros marcos regulatórios relacionados à segurança digital no Brasil remontam à Constituição Federal de 1988, que estabeleceu princípios fundamentais de acesso à informação, liberdade de expressão e proteção de dados, embora de forma ainda incipiente. Em 2003, a criação da Controladoria-Geral da União (CGU) representou avanço na governança de transparência e controle interno da administração pública federal.

Conforme documentos do Comitê Gestor da Internet no Brasil, o Decreto nº 4.829/2003 inaugurou a governança específica da internet no Brasil, estabelecendo diretrizes iniciais para a gestão da rede mundial de computadores no país. Este marco regulatório foi precursor de desenvolvimentos posteriores mais abrangentes na área de segurança cibernética.

Segundo o Ministério Público Federal, em 2018, a promulgação da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – representou mudança paradigmática na forma como o Brasil trata questões relacionadas à privacidade e segurança de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabeleceu princípios, direitos dos titulares e obrigações para controladores e operadores de dados, consolidando-se como pilar fundamental da governança digital brasileira.

A Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637/2018 e posteriormente atualizada pelo Decreto nº 12.572/2025, consolidou diretrizes estratégicas para a proteção de dados e sistemas na administração pública federal. Esta política

estabeleceu princípios de soberania nacional, garantia de direitos fundamentais, desenvolvimento de cultura de segurança e gestão de riscos informacionais.

Conforme estabelecido pela terceira geração da Política Nacional de Segurança da Informação e pela nova Estratégia Nacional de Cibersegurança (E-Ciber), a governança cibernética brasileira adota cinco pilares fundamentais: soberania e interesses nacionais, garantia de direitos fundamentais, defesa e segurança cibernética, cooperação e atuação internacional, e cultura e consciência em cibersegurança. Esta estratégia representa nível mais elevado de maturidade na governança cibernética nacional, promovendo abordagem integrada e colaborativa entre governo, setor privado e sociedade civil.

1.2 Cenário Atual das Ameaças Cibernéticas

Segundo dados da Fortinet e do Security Leaders, o cenário contemporâneo de ameaças cibernéticas no Brasil caracteriza-se por volume crescente, sofisticação técnica elevada e diversificação de vetores de ataque. Dados da fortinet revelam que o país registrou 103,16 bilhões de tentativas de ataques cibernéticos em 2022, consolidando-se como o segundo país mais atacado da América Latina. No primeiro semestre de 2025, este número alcançou 314,8 bilhões de tentativas, evidenciando aceleração preocupante do fenômeno.

De acordo com setoriais da Fortinet e da Checkpoint indicam que o setor financeiro brasileiro é particularmente visado por cibercriminosos, representando significativa parcela dos ataques direcionados. Infraestruturas críticas em áreas como saúde, energia, telecomunicações e governo também figuram entre os alvos preferenciais, devido ao potencial de causar impactos sistêmicos e ampliados.

Para Checkpoint, a tipologia das ameaças evoluiu substancialmente. O ransonware consolidou-se como uma das modalidades mais destrutivas e financeiramente impactantes, com grupos criminosos organizados operando modelos de Ransonware-as-a-Service (RaaS). Grupos como LockBit, RansomHub e Play destacaram-se em 2024 por atacarem centenas de organizações globalmente, incluindo alvos brasileiros.

Conforme relatórios da Fortinet, ataques de phishing e engenharia social permanecem entre os vetores mais utilizados, explorando vulnerabilidades humanas para obter acesso não autorizado a sistemas e dados. A sofisticação destas técnicas aumentou significativamente, com campanhas de spear phishing altamente personalizadas direcionadas a executivos e funcionários com acesso privilegiado.

Os relatórios da Fortinet, destacam que os Ataques de negação de serviço distribuído (DDoS) representam ameaça constante à disponibilidade de serviços digitais, sendo utilizados tanto como fim em si mesmo quanto como cortina de fumaça para ataques mais sofisticados. Em fevereiro de 2020, a Amazon Web Services (AWS) sofreu um dos maiores ataques DDoS já registrados, demonstrando a escala e capacidade destrutiva desta modalidade.

Dados da Fortinet e da Checkpoint demonstram que a exploração de vulnerabilidades em softwares e sistemas operacionais constitui vetor crítico de comprometimento. A velocidade com que novas vulnerabilidades são descobertas e exploradas, muitas vezes antes que patches de segurança sejam disponibilizados (vulnerabilidades zero-day), representa desafio significativo para equipes de segurança.

As ameaças internas (insider threats), sejam intencionais ou causadas por negligência, continuam representando um risco relevante para as organizações. Funcionários e ex-funcionários com conhecimento privilegiado sobre sistemas e acesso a informações sensíveis podem causar danos substanciais, seja por motivações maliciosas (espiões corporativos) ou por descuido no manuseio de credenciais e dados (CISA, 2022). O Verizon Data Breach Investigations Report (DBIR, 2024) aponta que, embora as ameaças externas dominem o volume de incidentes, os ataques internos, especialmente aqueles causados por erro humano, resultam em perdas financeiras significativas, reforçando a necessidade de políticas robustas de Zero Trust e de educação contínua.

1.3 Casos Emblemáticos de Ataques no Brasil

1.3.1 Ataque ao Superior Tribunal de Justiça (2020)

Em novembro de 2020, o Superior Tribunal de Justiça (STJ) foi alvo de um ataque cibernético de grande magnitude que resultou na suspensão completa de suas atividades por várias semanas. O ataque, identificado como ransomware, comprometeu servidores e sistemas críticos do tribunal, incluindo bases de dados processuais e sistemas de peticionamento eletrônico. Este incidente é frequentemente citado pela Agência Nacional de Proteção de Dados (ANPD, 2021) como um marco da escalada da ameaça de ransomware no Brasil, destacando a fragilidade da infraestrutura pública. A extensão do ataque ao STJ demonstrou a capacidade destrutiva desse tipo de malware, que, segundo a Kaspersky (2020), não visa apenas o roubo de dados, mas primariamente a interrupção da continuidade operacional e a extorsão financeira.

A investigação conduzida pela Polícia Federal identificou que os atacantes obtiveram acesso aos sistemas do STJ através de credenciais comprometidas, possivelmente obtidas por meio de phishing ou exploração de vulnerabilidades. Uma vez dentro da rede, os criminosos movimentaram-se lateralmente, criptografando dados e sistemas antes de serem detectados.

O incidente do STJ causou impactos operacionais severos, paralisando julgamentos e atrasando processos judiciais. Embora a corte não tenha confirmado pagamento de resgate, a recuperação dos sistemas demandou esforços técnicos intensivos e custosos, levando cerca de um mês para o restabelecimento total das operações. Este cenário é consistente com as descobertas da PwC (2023), que afirma que a principal despesa em casos de ransomware não é o pagamento do resgate, mas sim os custos de remediação, como o tempo de inatividade e a reconstrução de sistemas, que podem ultrapassar milhões de reais em grandes organizações. A Câmara de Comércio dos EUA (2022) aponta que a paralisação de atividades essenciais, como a justiça, gera um efeito cascata na economia e na sociedade, sublinhando a dimensão estratégica da resiliência cibernética.

Este caso evidenciou vulnerabilidades estruturais na segurança cibernética do Poder Judiciário brasileiro e impulsionou revisão abrangente das políticas e práticas de segurança em órgãos governamentais. O incidente também destacou a importância de backups seguros e planos de continuidade de negócios como medidas essenciais de resiliência.

1.3.2 Invasão ao Ministério da Saúde (2021)

Em dezembro de 2021, os sistemas do Ministério da Saúde foram alvo de um ataque cibernético sofisticado que comprometeu múltiplas plataformas, incluindo o site institucional, o aplicativo ConecteSUS e bases de dados relacionadas à vacinação contra COVID-19. O incidente, que ganhou ampla notoriedade nacional, ocorreu em um momento crítico da pandemia, quando estes sistemas eram essenciais para a gestão da resposta sanitária (Imprensa Nacional, 2021). A indisponibilidade do ConecteSUS e o risco de vazamento de dados de saúde sublinharam, conforme análise do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br, 2022), a alta dependência tecnológica do país em serviços críticos e a urgência em adotar estratégias de segurança mais robustas para proteger informações de interesse público e dados sensíveis dos cidadãos.

Investigações posteriores revelaram que os atacantes obtiveram acesso através de credenciais válidas, possivelmente roubadas ou obtidas mediante técnicas de engenharia social. Uma vez dentro dos sistemas, os criminosos excluíram dados, desfiguraram páginas web e

deixaram mensagens ameaçadoras. O uso de credenciais legítimas é uma tática cada vez mais comum, conforme observado pela Mandiant (2023), que destaca que a exploração da falha humana é, na maioria dos casos, o ponto de partida para ataques sofisticados a grandes infraestruturas. A exclusão de dados e a desfiguração de páginas, além do dano operacional, representam uma falha na Tríade CIA da Segurança (Confidencialidade, Integridade e Disponibilidade), com a Integridade sendo gravemente violada neste caso (Ross, 2020).

O impacto do ataque foi significativo, afetando a emissão de certificados digitais de vacinação, comprometendo a confiabilidade de dados epidemiológicos e gerando insegurança sobre a integridade das informações de saúde pública. A recuperação dos sistemas levou semanas e demandou esforços coordenados de múltiplas instituições.

Este incidente destacou a criticidade da proteção de infraestruturas de saúde digital e a necessidade de investimentos robustos em segurança cibernética para órgãos responsáveis por serviços essenciais. O caso também evidenciou lacunas em controles de acesso, monitoramento de sistemas e capacidade de resposta a incidentes.

Em resposta, o Ministério da Saúde implementou medidas de fortalecimento da segurança, incluindo revisão de controles de acesso, implementação de autenticação multifator e aprimoramento de capacidades de detecção e resposta a incidentes.

1.4 Impactos Econômicos e Sociais

A Deloitte (2024) corrobora que esses custos indiretos, conhecidos como custos ocultos, muitas vezes superam a perda inicial tendo os impactos dos ciberataques transcendem perdas financeiras diretas, gerando consequências amplas nas dimensões econômica, social, reputacional e de confiança institucional. No Brasil, estimativas do IDC Brasil (2023) apontam que o investimento em cibersegurança no Brasil deverá somar R$ 104 bilhões até 2028.

Na dimensão econômica, organizações afetadas por ataques de ransonware enfrentam dilemas complexos entre pagar resgates ou investir em recuperação técnica de sistemas. Dados globais indicam que resgates exigidos frequentemente excedem centenas de milhares ou milhões de dólares, valores que podem comprometer a sustentabilidade financeira de organizações de médio e pequeno porte.

Além dos custos diretos de resgate ou recuperação, incidentes de cibersegurança geram despesas significativas com investigações forenses, contratação de consultores especializados, implementação de medidas corretivas, atendimento a requisitos regulatórios e potenciais ações judiciais. A Deloitte (2024) corrobora que esses custos indiretos, conhecidos como custos

ocultos, muitas vezes superam a perda inicial, especialmente em multas regulatórias impostas pela LGPD no Brasil e por processos judiciais decorrentes do vazamento de dados.

Estimativas do IDC Brasil (2023) apontam que o investimento em cibersegurança no Brasil deverá somar R$ 104 bilhões até 2028, refletindo a crescente conscientização sobre a criticidade do tema e a necessidade de fortalecer as defesas preventivas e reativas.

No âmbito social, ataques a infraestruturas críticas podem comprometer serviços essenciais à população, como saúde, educação, energia e transporte. A interrupção destes serviços afeta diretamente a qualidade de vida dos cidadãos e pode gerar consequências graves, particularmente para populações vulneráveis.

O comprometimento de dados pessoais em violações de segurança expõe indivíduos a riscos de fraude, roubo de identidade e uso indevido de informações sensíveis. Em 2021, o Brasil figurou no topo do ranking mundial de vazamento de informações (Relatório Setorial, 2021), evidenciando a magnitude do problema.

Os danos reputacionais constituem impacto significativo para organizações afetadas. A perda de confiança de clientes, parceiros e investidores pode ter efeitos duradouros, comprometendo a posição competitiva e o valor de mercado das empresas. Para instituições governamentais, incidentes de cibersegurança minam a credibilidade e a confiança dos cidadãos na capacidade do Estado de proteger informações e garantir serviços públicos.

Na dimensão estratégica, a vulnerabilidade cibernética compromete a soberania digital e a segurança nacional, especialmente quando ataques se direcionam a infraestruturas críticas ou sistemas de defesa. A dependência de tecnologias estrangeiras e a insuficiência de capacidades técnicas nacionais amplificam estes riscos.

2 PRÁTICAS E TECNOLOGIAS DE DEFESA

2.1 Arquitetura de Segurança em Camadas

A defesa em profundidade (defense in depth) constitui princípio fundamental da cibersegurança contemporânea, baseando-se na implementação de múltiplas camadas de controles de segurança sobrepostos. Esta abordagem reconhece que nenhum controle individual é infalível, e que a combinação estratificada de mecanismos defensivos aumenta significativamente a resiliência organizacional contra ameaças diversificadas.

A arquitetura em camadas, conhecida como Defesa em Profundidade, abrange controles físicos, técnicos e administrativos, operando desde o perímetro externo até os núcleos mais

sensíveis da infraestrutura. Segundo Whitman e Mattord (2021), essa abordagem holística assegura que a falha de um controle não resulte no comprometimento total do sistema. Cada camada constitui uma barreira adicional que atacantes devem ultrapassar, aumentando exponencialmente a dificuldade, o tempo e os recursos necessários para um comprometimento bem-sucedido. A SANS Institute (2023) reforça que o objetivo estratégico não é a impenetrabilidade absoluta, mas sim elevar o 'custo do ataque' a um ponto em que ele se torne inviável para o adversário.

No nível físico, a segurança abrange controles de acesso a instalações, proteção de datacenters, gerenciamento de hardware e prevenção de acesso não autorizado a componentes críticos. No nível de rede, firewalls, sistemas de detecção e prevenção de intrusão, segmentação de rede e criptografia de comunicações constituem controles essenciais.

Na camada de sistemas e aplicações, controles incluem gestão de vulnerabilidades, hardening de sistemas operacionais, proteção de endpoints, controle de aplicações e monitoramento de integridade. No nível de dados, criptografia em repouso e em trânsito, classificação de informações, controle de acesso granular e prevenção de perda de dados são elementos crítico.

Controles administrativos, incluindo políticas de segurança, procedimentos operacionais, programas de conscientização, gestão de identidades e acessos, e governança de terceiros, permeiam todas as camadas técnicas, estabelecendo fundações organizacionais para segurança efetiva.

2.2 Firewall e Controle de Acesso

Firewalls constituem componentes fundamentais da primeira linha de defesa, funcionando como barreiras entre redes confiáveis e não confiáveis, filtrando tráfego com base em regras predefinidas. A evolução tecnológica transformou firewalls de simples filtros de pacotes baseados em endereços IP e portas em sistemas sofisticados capazes de inspeção profunda de pacotes, análise de estado de conexão e filtragem baseada em aplicações.

2.2.1 Segmentação de Rede

A segmentação de rede divide infraestruturas em zonas de segurança distintas, cada uma com controles de acesso e políticas específicas adequadas à sensibilidade dos recursos contidos.

Esta prática limita significativamente o potencial de movimentação lateral de atacantes que conseguem comprometer segmentos específicos, contendo brechas e minimizando impactos. Implementações efetivas empregam VLANs, sub-redes isoladas e firewalls internos para segregar diferentes departamentos, funções de negócio, níveis de confiança e criticidade. Zonas desmilitarizadas (DMZs) isolam sistemas expostos à internet, como servidores web e de e-mail, protegendo recursos internos mais sensíveis.

Microsegmentação representa evolução deste conceito, implementando controles granulares ao nível de carga de trabalho individual, particularmente em ambientes virtualizados e de nuvem. Esta abordagem permite políticas de segurança altamente específicas, reduzindo drasticamente a superfície de ataque.

2.2.2 Regras de Acesso e Monitoramento

A efetividade de firewalls depende criticamente da qualidade e manutenção de suas regras de configuração. Segundo as diretrizes do NIST (2009), uma política de regras mal definida ou desatualizada pode tornar o dispositivo ineficaz, criando uma falsa sensação de segurança enquanto mantém portas críticas abertas. O impacto da má gestão é corroborado pelo Gartner (2022), que estima que até 99% das falhas de segurança de firewall são causadas por erros de configuração humana, e não por falhas no software ou hardware do equipamento.

Melhores práticas estabelecem que regras devem seguir o princípio do privilégio mínimo, permitindo apenas tráfego explicitamente necessário e bloqueando todo o restante por padrão. Segundo o NIST (2009), esta abordagem, conhecida como Default Deny, é a base para uma configuração de firewall segura, pois assume que todo tráfego é hostil até prova em contrário. A SANS Institute (2022) reforça que essa prática reduz drasticamente a superfície de ataque, evitando que serviços esquecidos ou mal configurados fiquem expostos inadvertidamente à internet.

A organização lógica de regras por prioridade, agrupamento por funções ou serviços, e documentação detalhada facilitam gestão, auditoria e identificação de redundâncias ou inconsistências. Revisões periódicas são essenciais para remover regras obsoletas, corrigir configurações inadequadas e adaptar políticas a mudanças nos ambientes de negócio e ameaças.

Monitoramento contínuo e análise de logs de firewall constituem práticas indispensáveis para detecção de tentativas de acesso não autorizado, padrões anômalos e potenciais indicadores de comprometimento. Segundo o NIST (2020), a estratégia de monitoramento contínuo de segurança da informação (ISCM) é vital para manter a consciência situacional das

vulnerabilidades e ameaças em tempo real. Sistemas de Informação e Gerenciamento de Eventos de Segurança (SIEM) correlacionam eventos de múltiplas fontes, identificando padrões complexos que poderiam escapar à análise individual. A IBM Security (2023) destaca que a correlação automatizada é crucial para combater a 'fadiga de alertas', permitindo que analistas foquem em incidentes reais em vez de ruído, reduzindo significativamente o tempo de resposta a invasões.

Web Application Firewalls (WAFs) fornecem proteção especializada para aplicações web, inspecionando tráfego HTTP/HTTPS e bloqueando tentativas de exploração de vulnerabilidades comuns como SQL injection, cross-site scripting e inclusão de arquivos remotos.

2.3 Autenticação e Controle de Identidade

Gestão robusta de identidades e acessos (IAM – Identity and Access Management) constitui pilar fundamental da segurança cibernética, assegurando que apenas usuários autorizados possam acessar recursos específicos.

2.3.1 Autenticação Multifator

Autenticação multifator (MFA) adiciona camadas de verificação além de simples combinações de usuário e senha, exigindo que usuários apresentem múltiplos fatores de autenticação de categorias distintas. As categorias típicas incluem algo que o usuário sabe (senha, PIN), algo que o usuário possui (token físico, smartphone, smartcard) e algo que o usuário é (biometria).

A implementação de MFA reduz drasticamente o risco de comprometimento de contas mesmo quando credenciais são roubadas, phished ou obtidas por outros meios. Modalidades incluem tokens de hardware, aplicativos geradores de códigos temporários (TOTP), notificações push, biometria e autenticação baseada em certificados.

Protocolos modernos como OAuth e OpenID Connect facilitam implementação de MFA mantendo experiência de usuário aceitável e interoperabilidade entre sistemas . A adoção de MFA é mandatória em regulamentações de conformidade e representa prática básica essencial.

2.3.2 Princípio do Privilégio Mínimo

O princípio do privilégio mínimo estabelece que usuários, processos e sistemas devem receber apenas o nível de acesso estritamente necessário para desempenhar suas funções legítimas, e nada além. Esta abordagem limita significativamente a superfície de ataque e o potencial de dano em caso de comprometimento.

A implementação efetiva requer análise detalhada de funções e responsabilidades, mapeamento de requisitos reais de acesso e implementação de controles técnicos que façam cumprir estas restrições. Segundo o NIST (2021), essa granularidade é vital para garantir que o acesso lógico seja restrito apenas às funções necessárias para a execução de tarefas autorizadas (Need-to-Know). Revisões periódicas de privilégios, processos de aprovação formal para concessões excepcionais e auditoria contínua de uso de privilégios são componentes essenciais. A norma ISO/IEC 27002 (2022) enfatiza que a revisão regular dos direitos de acesso é mandatória para evitar o fenômeno do 'acúmulo de privilégios' (privilege creep), onde usuários mantêm acessos antigos e desnecessários ao mudarem de função dentro da organização.

Conceitos relacionados incluem acesso just-in-time (JIT), no qual privilégios elevados são concedidos temporariamente apenas quando necessário, e acesso suficiente (JEA), que fornece o mínimo absolutamente necessário para tarefas específicas. Estas técnicas reduzem janelas de exposição e oportunidades para abuso de privilégios.

Gestão de acessos privilegiados (PAM) emprega soluções especializadas para controlar, monitorar e auditar contas com privilégios elevados, como administradores de sistemas, evitando uso indiscriminado e facilitando detecção de atividades anômalas ou maliciosas.

2.4 Modelo Zero Trust

Zero Trust representa uma mudança paradigmática na arquitetura de segurança, abandonando o modelo tradicional de 'castelo e fosso' baseado em perímetros confiáveis. Conceituado originalmente por Kindervag (2010) na Forrester Research, este modelo assume que ameaças podem estar presentes tanto fora quanto dentro da rede, tornando o perímetro obsoleto. O princípio fundamental é 'nunca confie, sempre verifique' (never trust, always verify), tratando cada requisição de acesso como potencialmente maliciosa independentemente de sua origem, uma definição formalizada tecnicamente pelo NIST (2020) em seu padrão SP 800-207, que elimina o conceito de confiança implícita baseada em localização de rede.

A arquitetura Zero Trust opera sob a premissa de que atacantes podem já estar dentro do ambiente, eliminando distinções entre redes internas "confiáveis" e externas "não confiáveis". Cada usuário, dispositivo e carga de trabalho deve ser continuamente autenticado, autorizado e validado antes de receber acesso a recursos.

Princípios fundamentais incluem verificação contínua, aplicação de privilégio mínimo, e presunção de violação.

Decisões de acesso são baseadas em múltiplos fatores contextuais: identidade do usuário, postura de segurança do dispositivo, localização, padrões de comportamento, sensibilidade do recurso solicitado e nível de risco da requisição.

Implementação de Zero Trust requer eliminação de confiança implícita em qualquer parte da infraestrutura. Redes são microsegmentadas, cada sessão é independentemente autenticada, todo tráfego é inspecionado e criptografado, e acesso é concedido de forma granular e contextual.

Benefícios documentados incluem redução significativa da superfície de ataque, prevenção de movimentação lateral de atacantes, contenção efetiva de violações, e suporte a ambientes distribuídos modernos com usuários remotos, múltiplas nuvens e dispositivos diversos. O modelo alinha-se naturalmente com realidades contemporâneas de trabalho remoto e infraestruturas híbridas.

Tecnologias habilitadoras incluem gestão de identidades e acessos, autenticação multifator, microsegmentação de rede, gateways de acesso seguro, inspeção de tráfego criptografado, monitoramento comportamental e análise de riscos em tempo real.

2.5 Criptografia Avançada

Criptografia constitui tecnologia fundamental para proteção de confidencialidade e integridade de dados, tanto em trânsito quanto em repouso. Algoritmos criptográficos modernos, como AES-256 para criptografia simétrica e RSA, ECC para criptografia assimétrica, fornecem proteção robusta quando implementados corretamente.

A crescente capacidade computacional e, particularmente, o desenvolvimento de computadores quânticos, representa uma ameaça potencial para algoritmos criptográficos atualmente considerados seguros, como RSA e Criptografia de Curva Elíptica (ECC). Segundo o NIST (2024), a capacidade destrutiva do algoritmo de Shor tornará obsoleta a criptografia de chave pública atual, exigindo uma migração urgente. Criptografia pós-quântica (Post-Quantum Cryptography – PQC) emerge como área crítica de pesquisa, desenvolvendo algoritmos

resistentes a ataques por computadores quânticos. O NIST (2025) lidera o esforço global, tendo finalizado seus primeiros três padrões PQC (ML-KEM, ML-DSA e SLH-DSA) em 2024 e estabelecendo uma cronologia de transição que visa descontinuar algoritmos vulneráveis até 2035.

Implementação efetiva de criptografia demanda gestão robusta de chaves criptográficas, incluindo geração segura, armazenamento protegido, rotação periódica e destruição segura quando apropriado. Hardware Security Modules (HSMs) fornecem proteção especializada para operações e armazenamento de chaves críticas.

Criptografia de comunicações através de protocolos como TLS 1.3 protege dados em trânsito contra interceptação e manipulação. VPNs estabelecem túneis criptografados para acesso remoto seguro. Criptografia de disco completo e de arquivos protege dados em repouso contra acesso físico não autorizado.

Blockchain emprega criptografia avançada para garantir integridade, autenticidade e não repúdio de transações em ambientes distribuídos. Funções de hash criptográficas criam "impressões digitais" únicas de dados, permitindo verificação de integridade[11] [12] .

2.6 Inteligência Artificial na Detecção de Ameaças

Inteligência Artificial (IA) e Machine Learning (ML) revolucionaram as capacidades de detecção e resposta a ameaças, processando volumes massivos de dados, identificando padrões complexos e detectando anomalias com velocidade e precisão superiores a métodos tradicionais. Segundo o Capgemini Research Institute (2020), a IA tornou-se fundamental para responder a ataques automatizados que ocorrem em 'velocidade de máquina', impossíveis de serem contidos apenas por analistas humanos. A IBM Security (2024) quantifica esse impacto, demonstrando que organizações que utilizam IA e automação extensiva em segurança detectam e contêm brechas, em média, 100 dias mais rápido do que aquelas que não utilizam essas tecnologias.

Sistemas baseados em IA analisam comportamento de usuários, tráfego de rede, execução de processos e outras atividades, estabelecendo linhas de base de normalidade e identificando desvios indicativos de atividade maliciosa. Esta abordagem é particularmente efetiva contra ameaças sofisticadas que poderiam escapar a regras estáticas e assinaturas de malware conhecidas.

Aplicações incluem detecção de phishing através de análise de conteúdo e contexto de mensagens, identificação de malware por análise comportamental em sandbox, detecção de

anomalias em logs de sistemas, correlação de eventos de segurança em SIEMs, e resposta automatizada a incidentes.

IA também potencializa threat intelligence, agregando informações de múltiplas fontes, identificando indicadores de comprometimento, correlacionando campanhas de ataque e antecipando táticas, técnicas e procedimentos (TTPs) de adversários. Sistemas de User and Entity Behavior Analytics (UEBA) empregam ML para detectar ameaças internas e contas comprometidas através de análise de comportamento.

Desafios incluem necessidade de dados de treinamento de alta qualidade, risco de falsos positivos e negativos, complexidade de explicabilidade de decisões algorítmicas, e potencial uso adversarial de IA por atacantes para automatizar e aprimorar campanhas maliciosas. O desenvolvimento responsável e ético de IA para cibersegurança constitui imperativo crescente.

2.7 Blockchain para Segurança de Dados

Blockchain, tecnologia subjacente a criptomoedas, oferece propriedades únicas relevantes para aplicações de cibersegurança, particularmente integridade de dados, autenticidade, não repúdio e descentralização.

A estrutura de blocos encadeados criptograficamente torna registros imutáveis após validação, impedindo adulterações retroativas. Esta propriedade é valiosa para auditoria, logging de segurança, gestão de identidades digitais e cadeias de custódia de evidências.
Aplicações em cibersegurança incluem autenticação descentralizada eliminando pontos únicos de falha, gestão distribuída de identidades e credenciais, proteção de integridade de logs de auditoria, verificação de autenticidade de software e atualizações, e estabelecimento de confiança em ambientes sem autoridades centralizadas.

Smart contracts – programas autoexecutáveis em blockchains – podem automatizar políticas de segurança, controle de acesso e resposta a incidentes de forma transparente e verificável. Blockchain também habilita compartilhamento seguro de threat intelligence entre organizações mantendo privacidade e controle.

Desafios incluem escalabilidade limitada de *blockchains* públicas e consumo energético significativo de mecanismos de consenso Proof of Work, limitações técnicas amplamente documentadas pelo NIST (2018) em sua visão geral da tecnologia. A complexidade de implementação e integração com sistemas legados permanece alta. Além disso, surgem questões regulatórias críticas, especificamente a tensão entre a característica de imutabilidade do registro e requisitos de privacidade como o 'direito ao esquecimento' (previsto na LGPD e

GDPR). Segundo a ENISA (2019), este é um paradoxo jurídico fundamental, pois apagar dados pessoais de uma cadeia imutável é tecnicamente contraditório à própria natureza da tecnologia.

3 GOVERNANÇA DIGITAL E MARCO REGULATÓRIO

3.1 Política Nacional de Segurança da Informação (PNSI)

A Política Nacional de Segurança da Informação (PNSI), instituída originalmente pelo Decreto nº 9.637/2018 e atualizada pelo Decreto nº 12.572/2025, estabelece diretrizes estratégicas para a proteção de dados e sistemas de informação na administração pública federal brasileira. Esta política representa marco fundamental na governança de segurança cibernética do país, consolidando princípios, objetivos e estruturas de coordenação para enfrentamento de ameaças digitais.

A terceira geração da PNSI, publicada em agosto de 2025, surge como resposta à crescente sofisticação das ameaças cibernéticas, à rápida evolução tecnológica e à necessidade de fortalecer a resiliência do Estado diante de riscos informacionais. O decreto define que a segurança da informação abrange não apenas dados e ativos digitais, mas também ambientes físicos que contenham informações e pessoas envolvidas em seu ciclo de vida.

Entre os princípios fundamentais da PNSI destacam-se: soberania nacional e priorização dos interesses do país, garantia de direitos fundamentais como liberdade de expressão e privacidade, desenvolvimento de cultura de segurança através da educação, atuação colaborativa entre órgãos federais, e foco em gestão de riscos. Estes princípios orientam a implementação de práticas e controles em todos os níveis da administração pública.

A coordenação das ações está sob responsabilidade do Gabinete de Segurança Institucional (GSI) da Presidência da República, que atua na formulação de políticas públicas, elaboração de diretrizes e normativos técnicos, promoção de programas de formação e capacitação, acompanhamento da evolução tecnológica, e articulação de cooperação internacional.

Objetivos centrais incluem: proteger dados pessoais e informações sensíveis, salvaguardar infraestruturas críticas e serviços essenciais, incentivar pesquisa e inovação tecnológica, desenvolver cooperação internacional, e fortalecer ações de educação e conscientização. A política será operacionalizada através da Estratégia Nacional de Segurança da Informação, de planos nacionais específicos e de normativos do GSI.

Uma inovação significativa da PNSI 2025 é a obrigatoriedade de cada órgão e entidade federal instituir comitê interno de segurança, designar gestor responsável, planejar recursos

orçamentários específicos, e implementar programas de conscientização e capacitação. Este modelo de governança distribuída eleva o nível de accountability e integra a segurança da informação na agenda estratégica de toda a administração federal.

3.2 Estratégia Nacional de Cibersegurança (E-Ciber)

3.2.1 Pilares da E-Ciber 2025-2028

A Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo Decreto nº 12.573 de 4 de agosto de 2025, representa a segunda versão do documento estratégico brasileiro para cibersegurança, substituindo a versão de 2020. Esta atualização traz nível superior de maturidade e governança, refletindo aprendizados de incidentes recentes e alinhamento com melhores práticas internacionais.

O objetivo geral da E-Ciber 2025-2028 é fortalecer a cibersegurança do Brasil, promovendo proteção da soberania nacional, garantia de direitos fundamentais dos cidadãos, e resiliência de infraestruturas críticas e serviços essenciais, através de ações coordenadas envolvendo desenvolvimento tecnológico, formação profissional, pesquisa científica e cooperação internacional.

A estratégia de cibersegurança estrutura-se em cinco pilares fundamentais. O primeiro é a **Soberania e Interesses Nacionais**, que busca desenvolver capacidades tecnológicas e humanas nacionais para proteger a soberania do Brasil e avançar os interesses da sociedade no ciberespaço, reduzindo a dependência de tecnologias estrangeiras e fortalecendo a autonomia tecnológica. O segundo pilar, **Garantia de Direitos Fundamentais**, assegura que a cibersegurança esteja alinhada à preservação de direitos como liberdade de expressão, proteção de dados pessoais, privacidade e acesso à informação, garantindo que medidas de segurança não comprometam liberdades individuais essenciais.

O terceiro pilar, **Defesa e Segurança Cibernética**, promove a adoção de medidas e gestão de riscos para prevenir e mitigar vulnerabilidades, responder a ciberataques e desenvolver mecanismos de governança, regulação, fiscalização e controle que aprimorem a cibersegurança e a ciberresiliência. O quarto, **Cooperação e Atuação Internacional**, foca no fortalecimento da presença brasileira em fóruns e acordos internacionais, elevando o nível de cibersegurança, protegendo a soberania nacional e fomentando parcerias estratégicas e iniciativas multilaterais.

O pilar de **Cultura e Consciência em Cibersegurança**, por fim, busca desenvolver a conscientização e educação na sociedade, estimulando uma mentalidade proativa, especialmente entre gestores públicos e privados, e promovendo a cooperação na prevenção de cibercrimes. Juntos, esses pilares oferecem um arcabouço estratégico que integra proteção, desenvolvimento tecnológico, defesa de direitos e atuação internacional, consolidando a cibersegurança como prioridade nacional.

Diferentemente da versão anterior, a E-Ciber 2025-2028 não possui prazo de vigência fixo, operando de forma contínua com objetivos e ações de curto, médio e longo prazos, ajustáveis através de planos anuais. Esta flexibilidade permite adaptação dinâmica a evoluções tecnológicas e ameaças emergentes.

3.2.2 Governança e Coordenação Nacional

A E-Ciber estabelece governança centralizada promovendo desenvolvimento de mecanismos de regulação, fiscalização, coordenação e controle. O Comitê Nacional de Cibersegurança (CNCiber), criado em 2023, assume papel central na coordenação estratégica, reunindo 25 instituições entre órgãos governamentais, representantes da sociedade civil, instituições científicas e setor empresarial.

Esta composição plural assegura que a estratégia reflita perspectivas diversas e promova colaboração efetiva entre diferentes setores. O modelo de governança integrada estabelece rede de comunicação e coordenação entre instituições, permitindo respostas ágeis e compartilhamento de informações sobre ameaças e incidentes.

Cada órgão e entidade da administração pública federal deve instituir comitê interno de segurança articulado com o CNCiber, criando estrutura hierárquica de governança que permeia todo o governo federal. Esta arquitetura distribui responsabilidades mantendo alinhamento estratégico centralizado.

Inovação significativa é a exigência de que cada órgão reserve orçamento específico para ações de cibersegurança, criando disciplina orçamentária que trata segurança como prioridade estratégica e não custo acessório. Órgãos de controle interno poderão auditar alocação e execução destes recursos, fortalecendo accountability. A E-Ciber promove estruturação de maturidade cibernética, evoluindo estruturalmente a cibersegurança no Brasil através de padrões mínimos, certificação de produtos e serviços, e preparação e resiliência de serviços essenciais e infraestruturas críticas.

3.3 Lei Geral de Proteção de Dados (LGPD)

3.3.1 Princípios e Aplicabilidade

A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, em vigor desde 2020 – estabelece regras para o tratamento de dados pessoais no Brasil, aplicáveis a setores públicos e privados. Inspirada no GDPR europeu, baseia-se em princípios como finalidade, necessidade, transparência, segurança, prevenção de danos, não discriminação e responsabilização.

Ela se aplica a operações realizadas no Brasil, destinadas ao mercado brasileiro ou envolvendo dados de indivíduos localizados no país. Define bases legais para o tratamento de dados, incluindo consentimento, cumprimento de obrigação legal, execução de contratos, proteção da vida e legítimo interesse, exigindo cuidados especiais com dados sensíveis. Garante aos titulares direitos de acesso, correção, anonimização, portabilidade, bloqueio, eliminação e revogação de consentimento. A Autoridade Nacional de Proteção de Dados (ANPD) fiscaliza, orienta e aplica sanções, que incluem advertências, multas de até R$ 50 milhões, bloqueio ou eliminação de dados e suspensão de atividades.

3.3.2 Impactos na Cibersegurança Corporativa

A LGPD estabelece correlação intrínseca entre proteção de dados e cibersegurança, exigindo que organizações implementem medidas técnicas e administrativas adequadas para proteger dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão acidental ou ilícita.

Obrigações de segurança incluem implementação de controles de acesso, criptografia, anonimização e pseudonimização quando apropriado, gestão de vulnerabilidades, resposta a incidentes, testes de segurança, auditorias, e programas de treinamento. Estas exigências alinham-se com melhores práticas de cibersegurança e frameworks internacionais.

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, controladores devem comunicar à ANPD e aos titulares afetados em prazo razoável. Esta obrigatoriedade de notificação de breach cria incentivos para investimentos preventivos em segurança e resposta efetiva a incidentes.

Organizações devem designar encarregado (Data Protection Officer – DPO) responsável por atuar como canal de comunicação entre controlador, titulares e ANPD, orientar funcionários

sobre práticas de proteção de dados, e executar atividades de conformidade. Esta função fortalece governança de privacidade e segurança.

A LGPD exige demonstração de conformidade através de documentação de políticas, procedimentos, controles implementados e decisões tomadas. Relatórios de impacto à proteção de dados pessoais (RIPD) podem ser exigidos pela ANPD para tratamentos de alto risco. Esta ênfase em accountability demanda programas estruturados de governança de privacidade integrados à cibersegurança.

Impactos incluem necessidade de inventário abrangente de dados pessoais tratados, revisão de contratos com fornecedores e parceiros para assegurar conformidade, implementação de controles de privacidade by design e by default, estabelecimento de processos de gestão de direitos dos titulares, e criação de programas de conscientização sobre privacidade.

3.4 Frameworks Internacionais

3.4.1 NIST Cybersecurity Framework

O NIST Cybersecurity Framework (CSF), desenvolvido pelo National Institute of Standards and Technology dos Estados Unidos, constitui framework voluntário amplamente adotado globalmente para gestão de riscos de cibersegurança. Originalmente desenvolvido para infraestruturas críticas americanas, sua flexibilidade e aplicabilidade universal o tornaram referência para organizações de todos os portes e setores.

Ele é orientado a riscos, oferecendo linguagem comum e metodologia sistemática aplicável em vários níveis organizacionais, desde executivos até operações. Sua natureza não prescritiva permite adaptação a contextos específicos, integrando-se com outros frameworks e padrões.

3.4.2 ISO/IEC 27001

A ISO/IEC 27001 é norma internacional que especifica requisitos para estabelecer, implementar, manter e melhorar continuamente Sistema de Gestão de Segurança da Informação (SGSI). Fundamenta-se em ciclo PDCA (Plan-Do-Check-Act) de melhoria contínua aplicado à gestão de segurança.

A ISO/IEC 27001 define cláusulas obrigatórias e 93 controles de segurança em 14 domínios, aplicados conforme análise de riscos da organização. Os domínios abrangem desde

políticas de segurança e gestão de ativos até criptografia, continuidade e conformidade. O diferencial da norma é permitir certificação por organismos acreditados, garantindo reconhecimento internacional. A certificação exige auditorias rigorosas da implementação e efetividade dos controles.

A norma enfatiza abordagem baseada em processos, documentação de políticas e procedimentos, análise e tratamento de riscos, medição de desempenho e melhoria contínua. Esta ênfase em gestão estruturada promove sustentabilidade de longo prazo das práticas de segurança.

3.4.3 CIS Controls

Os Center for Internet Security (CIS) Controls são conjunto priorizado de ações defensivas desenvolvidas para mitigar ameaças cibernéticas mais prevalentes. Diferentemente de frameworks abrangentes, os CIS Controls focam em medidas específicas e acionáveis comprovadamente efetivas.

Atualmente na versão 8, os controles organizam-se em três grupos: **IG1**, essenciais para higiene cibernética básica em organizações com recursos limitados; **IG2**, adicionais para organizações com múltiplos departamentos e maior complexidade de TI; e **IG3**, completos para organizações com equipes de segurança dedicadas e infraestrutura complexa, garantindo proteção rigorosa.

Os 18 controles CIS cobrem áreas como inventário e controle de ativos, gestão de vulnerabilidades, proteção de dados, configuração segura, defesa contra malware, gestão de logs, defesa de e-mail e navegador, resposta e recuperação de incidentes, teste de penetração e exercícios red team.

A abordagem pragmática e priorizada dos CIS Controls torna-os particularmente úteis para organizações iniciando programas de segurança ou com recursos limitados. A especificidade das ações recomendadas facilita implementação e mensuração de progresso.

4 EDUCAÇÃO DIGITAL E CULTURA DE SEGURANÇA

4.1 Conscientização da Sociedade

A construção de uma sociedade digitalmente resiliente transcende a implementação de tecnologias de proteção, demandando o desenvolvimento de uma cultura de segurança

cibernética arraigada em todos os níveis sociais. Segundo a ENISA (2021), a tecnologia sozinha é insuficiente se o fator humano não for tratado como a primeira linha de defesa, exigindo uma mudança de mentalidade onde a segurança é vista como responsabilidade compartilhada. O SANS Institute (2023) reforça que uma cultura de segurança madura não se resume ao cumprimento de regras (compliance), mas à mudança comportamental intrínseca, onde cada indivíduo reconhece seu papel ativo na proteção do ecossistema digital.

Estudos demonstram que o fator humano constitui frequentemente o elo mais vulnerável nas cadeias de segurança, com engenharia social explorando cognição, emoções e comportamentos humanos para contornar controles técnicos.

Programas efetivos de conscientização devem alcançar diferentes públicos com abordagens adaptadas: crianças e adolescentes, população adulta geral, idosos, profissionais de diversos setores, e gestores públicos e privados. Cada grupo apresenta vulnerabilidades específicas, níveis variados de literacia digital, e papéis distintos no ecossistema de segurança.

Especialistas defendem que escolas devem incorporar educação cibernética em currículos, tratando temas como privacidade digital, identificação de ameaças, comportamento seguro online, ética digital e cidadania no ciberespaço. A formação desde a infância estabelece fundações para comportamentos seguros ao longo da vida.

Para população adulta, campanhas de conscientização devem abordar riscos cotidianos como phishing, golpes financeiros, proteção de senhas, configurações de privacidade em redes sociais, segurança de dispositivos móveis e Internet das Coisas, e proteção de informações pessoais e familiares. Linguagem acessível, exemplos práticos e canais diversos maximizam alcance e efetividade.

Idosos constituem grupo particularmente vulnerável a golpes digitais devido à menor familiaridade com tecnologias e à tendência de maior confiança em comunicações recebidas. Programas específicos devem fornecer orientações claras, simples e repetidas sobre identificação de fraudes, uso seguro de serviços bancários digitais, e proteção contra golpes direcionados a esta faixa etária.

Governo federal, através de órgãos como o Gabinete de Segurança Institucional, Ministério da Ciência, Tecnologia e Inovações, e Autoridade Nacional de Proteção de Dados, desenvolve iniciativas de conscientização incluindo cartilhas, vídeos educativos, webinars, e campanhas em mídias sociais. Parcerias com organizações da sociedade civil, setor privado e instituições de ensino amplificam o alcance destas ações.

Métricas de efetividade incluem redução de taxas de cliques em simulações de phishing, aumento de reportes de tentativas de ataque, melhoria em avaliações de conhecimento sobre

segurança, e mudanças mensuráveis em comportamentos de risco. Avaliações contínuas permitem refinamento de abordagens e focalização em áreas de maior necessidade.

4.2 Capacitação de Profissionais

O Brasil enfrenta um déficit significativo de profissionais qualificados em cibersegurança, com a demanda superando amplamente a oferta. Segundo o (ISC)² Cybersecurity Workforce Study (2023), o Brasil possui uma das maiores lacunas de força de trabalho da América Latina, contribuindo para um déficit global de quase 4 milhões de profissionais. Estimativas da Brasscom (2024) corroboram este cenário, indicando que o setor de tecnologia brasileiro demanda milhares de novos especialistas anualmente que o sistema educacional atual não consegue suprir. Este gap de talentos constitui uma limitação crítica para o fortalecimento da cibersegurança nacional, expondo organizações a riscos elevados devido à falta de pessoal para monitorar e defender sistemas.

Formação técnica abrange graduações em Ciência da Computação, Engenharia de Computação, Sistemas de Informação e cursos específicos de Segurança da Informação, além de pós-graduações especializadas em cibersegurança, perícia digital, gestão de riscos e áreas correlatas. Universidades públicas e privadas expandiram ofertas nestes campos, mas ainda insuficientes para preencher lacunas.

Certificações profissionais reconhecidas internacionalmente, como CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CISM (Certified Information Security Manager), CompTIA Security+, entre outras, complementam formação acadêmica e validam competências técnicas específicas.

Capacitação contínua é essencial dado o ritmo acelerado de evolução tecnológica e de ameaças. Programas de educação continuada, participação em conferências e eventos especializados, treinamentos em novas tecnologias e técnicas de ataque e defesa, e engajamento em comunidades de prática mantêm profissionais atualizados.

Iniciativas governamentais incluem programas de bolsas para formação em cibersegurança, apoio a centros de pesquisa e desenvolvimento, estímulo à criação de cursos técnicos e tecnológicos, e parcerias com instituições internacionais para transferência de conhecimento. A Estratégia Nacional de Cibersegurança estabelece meta explícita de desenvolver capital humano nacional.

Setor privado desempenha papel complementar através de programas de trainee, parcerias com instituições de ensino, patrocínio de certificações, estabelecimento de programas

de mentoria, e criação de ambientes propícios ao desenvolvimento profissional. Organizações líderes investem robustamente em desenvolvimento de equipes internas de segurança.

Competições de hacking ético (Capture the Flag), programas de bug bounty, hackathons focados em segurança, e iniciativas de inclusão de grupos sub-representados (mulheres, minorias étnicas) na área de cibersegurança contribuem para ampliação e diversificação do pipeline de talentos.

4.3 Programas Governamentais de Educação Digital

O governo brasileiro implementa programas multifacetados destinados a elevar o nível de literacia digital e conscientização sobre cibersegurança na população, ações estas coordenadas pelo Gabinete de Segurança Institucional (GSI, 2024) em parceria com o Comitê Gestor da Internet no Brasil. Estes programas alinham-se diretamente aos pilares da Estratégia Nacional de Cibersegurança (E-Ciber) relacionados a 'Educação' e 'Dimensão Humana', conforme estipulado no Decreto nº 12.573 (BRASIL, 2025), que reconhece a conscientização pública como um pré-requisito indispensável para a eficácia de qualquer defesa técnica nacional.

Iniciativas incluem desenvolvimento de materiais educativos adaptados a diferentes públicos e contextos, disponibilizados em formatos acessíveis através de portais governamentais e canais digitais. Cartilhas, vídeos explicativos, infográficos, podcasts e cursos online gratuitos abordam temas desde fundamentos de segurança até ameaças específicas e técnicas de proteção.

Campanhas de conscientização em datas específicas, como o Dia da Internet Segura e o Mês da Conscientização sobre Cibersegurança, concentram esforços de comunicação e engajamento público. Estas iniciativas utilizam mídias tradicionais, digitais e redes sociais para alcance amplo.

Programas em instituições de ensino públicas incluem formação de professores em educação digital e cibersegurança, disponibilização de recursos didáticos para incorporação de temas de segurança em disciplinas existentes, e apoio a projetos educacionais focados em segurança e ética digital.

Parcerias com entidades do setor privado, organizações não governamentais, academia e organismos internacionais ampliam alcance e recursos de programas governamentais. Colaborações multilaterais permitem compartilhamento de melhores práticas e adaptação de iniciativas bem-sucedidas de outros países.

O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), vinculado ao GSI, mantém canais de comunicação para reportes de incidentes, alertas sobre ameaças emergentes, e orientações técnicas para gestores de TI governamentais. Estes serviços constituem mecanismos práticos de suporte e educação continuada.

4.4 Responsabilidade Corporativa

Organizações privadas detêm responsabilidade significativa na promoção de cultura de segurança cibernética, tanto internamente quanto em suas cadeias de valor e comunidades de stakeholders. Investimentos em programas de conscientização e treinamento de funcionários representam medidas de segurança fundamentais com retornos mensuráveis na redução de incidentes.

Programas corporativos efetivos de conscientização em segurança incluem treinamentos obrigatórios periódicos para todos os funcionários, cobrindo fundamentos de segurança, políticas organizacionais, identificação de phishing e engenharia social, uso seguro de recursos corporativos, proteção de dados, e procedimentos de reporte de incidentes.

Simulações de phishing controladas permitem avaliação de vulnerabilidades comportamentais e identificação de necessidades específicas de treinamento. Feedback construtivo e oportunidades de aprendizado transformam falhas em simulações em experiências educativas valiosas, evitando penalizações contraproducentes que inibiriam reportes de incidentes reais.

Comunicações regulares de segurança através de newsletters, intranet, cartazes, screensavers e outros canais mantêm temas de segurança visíveis e reforçam mensagens-chave. Variação de formatos e criatividade nas comunicações aumentam engajamento e retenção de informações.

Estabelecimento de cultura de segurança positiva, na qual reporte de incidentes e identificação de vulnerabilidades são encorajados e reconhecidos, constitui elemento crítico. Funcionários devem sentir-se seguros ao relatar erros ou tentativas de ataque sem medo de repercussões negativas.

Incorporação de requisitos de segurança em processos de contratação, avaliações de desempenho e progressão de carreira sinaliza importância organizacional do tema. Responsabilidades específicas de segurança para diferentes funções devem ser claramente definidas e comunicadas.

Empresas líderes implementam programas de champions ou embaixadores de segurança, designando indivíduos em diferentes departamentos como pontos focais para disseminação de conhecimento, suporte a colegas e reforço de mensagens de segurança. Esta abordagem descentralizada amplifica alcance e adaptação de mensagens a contextos específicos.

Extensão de programas de conscientização a terceiros, fornecedores e parceiros de negócio fortalece segurança de cadeias de suprimento e ecossistemas corporativos. Requisitos contratuais relacionados à segurança, auditorias e treinamentos conjuntos promovem alinhamento de práticas.

5 RESILIÊNCIA DIGITAL E INFRAESTRUTURAS CRÍTICAS

5.1 Conceito de Resiliência Digital

A resiliência digital transcende a mera prevenção de incidentes, abrangendo a capacidade organizacional de antecipar, resistir, absorver, responder, adaptar-se e recuperar-se de adversidades cibernéticas mantendo operações críticas. Segundo o NIST (2021) em sua publicação SP 800-160 Vol. 2, a resiliência cibernética é definida pela capacidade de um sistema entregar o resultado pretendido continuamente, apesar de eventos adversos cibernéticos. Este conceito reconhece a impossibilidade de prevenção absoluta de todos os ataques, enfatizando preparação, adaptabilidade e recuperação como elementos essenciais, uma mudança de paradigma destacada pela Accenture (2023), que aponta que empresas resilientes focam não apenas na defesa do perímetro, mas na continuidade do negócio sob estresse.

A resiliência manifesta-se em múltiplas dimensões: tecnológica (redundância, backup, recuperação), organizacional (processos, governança, capacidades), humana (competências, conscientização, cultura), e ecossistêmica (parcerias, compartilhamento de informações, coordenação). Abordagens efetivas integram estas dimensões em estratégias coesas.

Princípios fundamentais incluem redundância e diversidade de sistemas críticos, segmentação para contenção de impactos, monitoramento contínuo para detecção precoce, capacidade de resposta rápida, planos testados de continuidade de negócios e recuperação de desastres, e aprendizado contínuo de incidentes. Investimentos em resiliência representam seguros contra impactos potencialmente catastróficos.

Métricas de resiliência incluem tempo médio entre falhas (MTBF), tempo médio para detecção (MTTD), tempo médio para resposta (MTTR), capacidade de manutenção de

operações críticas durante incidentes, efetividade de recuperação, e adaptabilidade a novas ameaças. Mensuração contínua permite identificação de lacunas e priorização de melhorias.

Resiliência digital tornou-se diferencial competitivo significativo, influenciando confiança de clientes, parceiros e investidores, além de impactar avaliações de risco e custos de seguros. Organizações resilientes recuperam-se mais rapidamente de incidentes, minimizam perdas financeiras e reputacionais, e mantêm vantagens competitivas.

5.2 Proteção de Infraestruturas Críticas

Infraestruturas críticas – sistemas e ativos essenciais cujo comprometimento teria impacto debilitante na segurança nacional, economia, saúde pública ou segurança – demandam atenção especial em cibersegurança. Setores incluem energia, telecomunicações, transporte, água e saneamento, saúde, serviços financeiros, governo, e tecnologia da informação.

A crescente digitalização e interconexão destas infraestruturas ampliaram significativamente superfícies de ataque e o potencial de impactos em cascata. Segundo a CISA (2023), a convergência entre TI e TO corroeu o isolamento físico (air gap) que historicamente protegia esses ativos, expondo sistemas legados vulneráveis à internet pública. Ataques a sistemas de controle industrial (ICS) e tecnologia operacional (OT) podem causar danos físicos, interrupções prolongadas de serviços essenciais e riscos à segurança pública. O relatório anual da Dragos (2024) confirma essa tendência, alertando que grupos adversários estão desenvolvendo capacidades específicas ("malware modular") para causar efeitos cinéticos destrutivos, cruzando a fronteira do digital para o mundo físico.

Desafios específicos incluem sistemas legados com vulnerabilidades conhecidas mas difíceis de remediar, convergência entre IT e OT introduzindo novos vetores de ataque, dependências complexas entre setores criando riscos sistêmicos, e tensões entre requisitos de disponibilidade operacional e necessidades de aplicação de atualizações de segurança.

Estratégias de proteção abrangem segmentação rigorosa entre redes corporativas e operacionais, implementação de zonas desmilitarizadas para conexões necessárias, controles de acesso físicos e lógicos robustos, monitoramento especializado de ambientes OT, planos de resposta específicos para ambientes industriais, e testes regulares sem comprometer operações.

Frameworks específicos para segurança de infraestruturas críticas incluem IEC 62443 para segurança de sistemas de automação e controle industrial, e orientações do NIST para infraestruturas críticas. Estes padrões fornecem diretrizes técnicas adaptadas às particularidades destes ambientes.

Colaboração público-privada é essencial dado que maioria das infraestruturas críticas são operadas pelo setor privado. Compartilhamento de informações sobre ameaças, exercícios conjuntos, desenvolvimento de padrões setoriais e coordenação de resposta a incidentes fortalecem resiliência coletiva.

A Estratégia Nacional de Cibersegurança estabelece proteção de infraestruturas críticas como pilar fundamental, promovendo padrões mínimos de segurança, certificação de produtos e serviços, e mecanismos de coordenação entre operadores de infraestruturas críticas e governo.

5.3 Planos de Continuidade de Negócios

Planos de Continuidade de Negócios (PCN) e Recuperação de Desastres (PRD) constituem elementos fundamentais de resiliência organizacional, estabelecendo estratégias e procedimentos para manutenção ou rápida restauração de operações críticas após incidentes disruptivos. Desenvolvimento efetivo destes planos demanda análise abrangente de riscos, identificação de processos críticos e suas interdependências, e estabelecimento de objetivos mensuráveis de recuperação.

Análise de Impacto nos Negócios (BIA – Business Impact Analysis) identifica processos, sistemas e recursos críticos, quantifica impactos potenciais de interrupções em diferentes períodos, e estabelece prioridades de recuperação.

Esta análise fundamenta decisões sobre investimentos em controles preventivos, capacidades de resposta e recursos de recuperação.

Objetivos de Tempo de Recuperação (RTO – Recovery Time Objective) definem tempo máximo aceitável para restauração de funções críticas. Objetivos de Ponto de Recuperação (RPO – Recovery Point Objective) estabelecem perda máxima aceitável de dados medida em tempo. RTOs e RPOs orientam arquiteturas de backup, replicação e redundância.

Estratégias de recuperação incluem sites alternativos (hot, warm ou cold sites), infraestrutura redundante geograficamente distribuída, capacidades de failover automático, backups regulares com testes de restauração, e procedimentos de operação manual para cenários de indisponibilidade prolongada de sistemas.

Planos devem documentar claramente papéis e responsabilidades de equipes de resposta, procedimentos detalhados passo-a-passo para diferentes cenários, informações de contato atualizadas, e dependências de recursos externos.

Acessibilidade destes planos mesmo durante incidentes que afetem sistemas primários é crítica.

Testes regulares através de exercícios de mesa, simulações técnicas e testes completos de failover validam efetividade de planos, identificam lacunas, treinam equipes e aumentam confiança em capacidades de recuperação.

Aprendizados de testes e incidentes reais devem alimentar atualizações contínuas dos planos.

5.4 Gestão de Incidentes e Resposta a Crises

Capacidades robustas de gestão de incidentes de segurança são essenciais para a resiliência organizacional, permitindo detecção rápida, análise eficaz, contenção de danos, erradicação de ameaças e recuperação ordenada de sistemas. Frameworks como o NIST SP 800-61 oferecem orientações estruturadas para a criação de processos de resposta a incidentes, definindo fases como preparação, detecção, análise, contenção, erradicação, recuperação e atividades pós-incidente.

A preparação envolve estabelecimento de equipes, ferramentas, procedimentos, treinamentos e playbooks para cenários comuns, além de infraestrutura técnica e canais de comunicação apropriados. Na detecção e análise, eventos de segurança são identificados via monitoramento, alertas automatizados ou notificações externas, permitindo avaliação de natureza, escopo e gravidade do incidente para priorização e acionamento de recursos.

As fases de contenção, erradicação e recuperação visam limitar impactos, eliminar ameaças e restaurar operações normais. Estratégias equilibram preservação de evidências forenses com proteção imediata de ativos críticos. Atividades pós-incidente incluem documentação detalhada, análise de causa raiz, lições aprendidas e implementação de melhorias preventivas e corretivas, promovendo aprendizado organizacional.

Equipes especializadas, como CSIRTs **e** CERTs, concentram expertise e autoridade para coordenar respostas. Organizações maiores mantêm equipes dedicadas, enquanto menores podem recorrer a serviços externos ou CSIRTs setoriais. A comunicação durante incidentes exige planejamento cuidadoso, com porta-vozes designados, mensagens pré-aprovadas e canais estabelecidos para reguladores, clientes, parceiros, mídia e público.

No Brasil, o CTIR Gov coordena respostas a incidentes na administração pública federal, fornecendo suporte técnico, compartilhamento de informações e integração com outros CSIRTs nacionais e internacionais. Outros CSIRTs setoriais atuam em setores como educação, pesquisa, financeiro e telecomunicações, fortalecendo a cooperação entre autoridades,

promovendo preservação de evidências e cumprimento de requisitos legais durante incidentes cibernéticos.

CONCLUSÃO

A cibersegurança no Brasil apresenta um cenário complexo, marcado por desafios expressivos, mas também por avanços relevantes em governança, regulação e conscientização. O país figura entre os mais atacados do mundo, com números alarmantes de tentativas de ataques digitais, o que evidencia a escalada das ameaças e a necessidade urgente de fortalecimento das defesas nacionais.

Incidentes graves envolvendo instituições públicas estratégicas, como o Superior Tribunal de Justiça e o Ministério da Saúde, expuseram vulnerabilidades críticas e demonstraram impactos sistêmicos possíveis. Esses episódios impulsionaram maior atenção governamental, investimentos e a atualização de políticas nacionais, culminando na nova Estratégia Nacional de Cibersegurança publicada em 2025.

As ameaças contemporâneas tornaram-se cada vez mais sofisticadas, incluindo ransomware industrializado, engenharia social avançada, exploração de vulnerabilidades inéditas e ações patrocinadas por estados. Paralelamente, soluções tecnológicas como Zero Trust, inteligência artificial, blockchain e criptografia pós-quântica vêm sendo incorporadas, embora sua efetividade dependa de implementação adequada e equipes qualificadas.

O marco regulatório brasileiro avançou significativamente, especialmente com a LGPD e o alinhamento a frameworks internacionais como NIST e ISO/IEC 27001. Contudo, permanece como desafio central o déficit de profissionais especializados e a necessidade de construir uma cultura de segurança abrangente na sociedade, com investimentos contínuos em educação, certificações e conscientização pública.

No futuro, tendências como IoT, cidades inteligentes, inteligência artificial e computação quântica ampliarão as superfícies de ataque e intensificarão dimensões geopolíticas da cibersegurança. Conclui-se que, apesar das dificuldades estruturais, o Brasil segue em trajetória de maturação institucional, exigindo investimentos sustentados, cooperação multissetorial e fortalecimento da resiliência digital para garantir um ambiente seguro e propício ao desenvolvimento econômico e social.

REFERÊNCIAS

AGÊNCIA BRASIL. **Sites e aplicativo do Ministério da Saúde sofrem ataque cibernético**, 10 dez. 2021. Agência Brasil. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico. Acesso em: 20 out. 2025.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. **Diário Oficial da União**: Seção 1, Brasília, DF, 5 ago. 2025. Disponível em: https://agenciagov.ebc.com.br/noticias/202508/governo-federal-institui-a-terceira-geracao-da-politica-nacional-de-seguranca-da-informacao. Acesso em: 20 out. 2025

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança – E-Ciber. **Diário Oficial da União:** Seção 1, nº 146, p. 2, 5 ago. 2025. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber. Acesso em: 20 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais, inclusive nos meios digitais, e altera dispositivos das leis nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), e nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 out. 2025.

CHECKPOINT. **As 6 principais ameaças à segurança cibernética**. Disponível em: https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/. Acesso em: 20 out. 2025.

CNN BRASIL. **Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar**. Disponível em: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/. Acesso em: 20 out. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL**. e-Ciber 2025-2028:** documento apresentado na Reunião do Comitê Gestor da Internet no Brasil de 23 de agosto de 2024, relativo à Estratégia Nacional de Cibersegurança. **s.l.**: Comitê Gestor da Internet no Brasil, 23 ago. 2024. Disponível em: https://cgi.br/media/atas/pdf/reuniao_do_cgi.br_de_23_de_agosto_de_2024_0_30092024.pdf . Acesso em: 20 out. 2025.

DATA SCIENCE ACADEMY. **10 casos de uso de inteligência artificial na segurança cibernética**. Disponível em:https://blog.dsacademy.com.br/10-casos-de-uso-de-inteligencia-artificial-na-seguranca-cibernetica/. Acesso em: 20 out.2025.

DATACAMP. **Arquitetura Zero Trust**: uma maneira moderna de proteger sistemas, s.d. DataCamp. Disponível em: https://www.datacamp.com/pt/tutorial/zero-trust-architecture. Acesso em: 20 out. 2025.

FORTINET. **Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataqu es-ciberneticos-na-a. Acesso em: 20 out. 2025.

FORTINET. **Segurança quântica segura**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/quantum-safe-security. Acesso em: 20 out. 2025.

FORTINET. **Tipos de ataque cibernético**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/types-of-cyber-attacks. Acesso em: 20 out. 2025.

KASPERSKY. **O que é segurança para blockchain?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-blockchain-security. Acesso em: 20 out. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **O que é a LGPD?** — Lei Geral de Proteção de Dados. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. Acesso em: 20 out. 2025.

SECURITY LEADERS. **Brasil sofreu 103,16 bilhões de tentativas de ataques cibernéticos em 2022**, 30 out. 2023. Security Leaders. Disponível em: https://securityleaders.com.br/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022/. Acesso em: 20 out. 2025.

TI EXAMES. **Comparando Frameworks**: NIST CSF, ISO/IEC 27001 e CIS Controls, s.d. TI EXAMES. Disponível em: https://tiexames.com.br/novosite2015/blog-detalhe.php?id=38. Acesso em: 20 out. 2025.