Revista ARACÊ
ISSN: 2358-2472

SEGURANÇA DA INFORMAÇÃO: DESAFIOS, PRINCÍPIOS E PRÁTICAS NO CENÁRIO DIGITAL CONTEMPORÂNEO

INFORMATION SECURITY: CHALLENGES, PRINCIPLES AND PRACTICES IN THE CONTEMPORARY DIGITAL SCENARIO

SEGURIDAD DE LA INFORMACIÓN: RETOS, PRINCIPIOS Y PRÁCTICAS EN EL ESCENARIO DIGITAL CONTEMPORÁNEO

https://doi.org/10.56238/arev7n12-315

Data de submissão: 29/11/2025 **Data de publicação:** 29/12/2025

Felipe Menezes de Abreu
Pós-graduado em Gestão de Tecnologia da Informação
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: felipe.md.abreu@aluno.uepa.br

Charlhes das Graças Vilhena do Nascimento
Formação: Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: chdavilarissa@gmail.com

David Alves Luna
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: davidlunapocket@gmail.com

Edinaldo Cunha da Silva
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: edcunha01silva@gmail.com

Edinaldo Nogueira Araujo
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: naldo.nogueira.zzz@gmail.com

Elias Ramos Quaresma
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: eliasramos.educ@gmail.com

Emerson Leandro da Silva Silva
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: emersonleandrodss@gmail.com

Revista ARACÊ
ISSN: 2358-2472

Francisco da Silva Pontes
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: francisco.pontesfds@gmail.com

Francisco de Paula Cunha
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: engenhariadesoftware2471@gmail.com

Glaucia Nunes de Lima Santos
Graduanda em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: glauciaa.nunes@gmail.com

Jader da Silva Oliveira
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: jdsilva977@gmail.com

Raimundo Celestino do Amaral Junior
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: amaraljunior.es@gmail.com

Samira Dias Silva
Graduanda em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: samira.d.silva25@gmail.com

Yago Rodrigues Cabral
Graduando em Engenharia de Software
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: yagorodriguescabral@gmail.com

RESUMO
A Segurança da Informação constitui um campo estratégico para a proteção de dados e ativos tecnológicos em organizações públicas, privadas e no uso pessoal. Com a crescente digitalização das interações sociais, econômicas e políticas, os riscos associados a invasões, fraudes, vazamentos e desinformação tornam-se mais amplos e sofisticados. Tecnologias emergentes, como computação em nuvem, dispositivos IoT e inteligência artificial, ampliam a eficiência dos processos, mas também aumentam a superfície de ataque e a dependência de sistemas digitais. Nesse cenário de ameaças em constante evolução, a Segurança da Informação deixa de ser apenas uma responsabilidade técnica e passa a integrar a governança organizacional, envolvendo políticas de proteção, gestão de riscos, conformidade legal e capacitação contínua dos usuários. Assim, este estudo discute princípios, desafios e práticas essenciais de mitigação, alinhadas às melhores normas e diretrizes internacionais, como a ISO/IEC 27001, destacando a importância da conscientização como elemento fundamental para a construção de ambientes digitais mais seguros e resilientes.

Revista ARACÊ
ISSN: 2358-2472

Palavras-chave: Segurança da Informação. Cibersegurança. Proteção de Dados. Riscos Digitais.

ABSTRACT
Information Security constitutes a strategic field for the protection of data and technological assets in public and private organizations, as well as for personal use. With the increasing digitalization of social, economic, and political interactions, the risks associated with intrusions, fraud, leaks, and disinformation become broader and more sophisticated. Emerging technologies, such as cloud computing, IoT devices, and artificial intelligence, increase the efficiency of processes but also expand the attack surface and dependence on digital systems. In this scenario of constantly evolving threats, Information Security ceases to be merely a technical responsibility and becomes integrated into organizational governance, involving protection policies, risk management, legal compliance, and continuous user training. Thus, this study discusses essential mitigation principles, challenges, and practices, aligned with the best international standards and guidelines, such as ISO/IEC 27001, highlighting the importance of awareness as a fundamental element for building safer and more resilient digital environments.

Keywords: Information Security. Cybersecurity. Data Protection. Digital Risks.

RESUMEN
La seguridad de la información constituye un campo estratégico para la protección de datos y activos tecnológicos en organizaciones públicas y privadas, así como para uso personal. Con la creciente digitalización de las interacciones sociales, económicas y políticas, los riesgos asociados a intrusiones, fraudes, filtraciones y desinformación se vuelven más amplios y sofisticados. Las tecnologías emergentes, como la computación en la nube, los dispositivos IoT y la inteligencia artificial, aumentan la eficiencia de los procesos, pero también amplían la superficie de ataque y la dependencia de los sistemas digitales. En este escenario de amenazas en constante evolución, la seguridad de la información deja de ser una mera responsabilidad técnica para integrarse en la gobernanza organizacional, abarcando políticas de protección, gestión de riesgos, cumplimiento legal y formación continua de usuarios. Por ello, este estudio analiza principios, desafíos y prácticas esenciales de mitigación, alineados con los mejores estándares y directrices internacionales, como la norma ISO/IEC 27001, destacando la importancia de la concienciación como elemento fundamental para construir entornos digitales más seguros y resilientes.

Palabras clave: Seguridad de la Información. Ciberseguridad. Protección de Datos. Riesgos Digitales.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

O avanço das Tecnologias da Informação e Comunicação (TIC) ampliou o acesso à informação e transformou profundamente as relações sociais, econômicas e culturais. A digitalização passou a permear atividades cotidianas, desde transações bancárias e interação em redes sociais até a gestão de infraestruturas críticas, como saúde, energia e transporte. Essa evolução trouxe inúmeros benefícios relacionados à conectividade, produtividade e inovação. Contudo, ao mesmo tempo em que promove novas possibilidades, também expandiu a superfície de ataque e expôs indivíduos e organizações a um número crescente de ameaças cibernéticas **(STALLINGS, 2015)**.

Nesse contexto, crimes como invasões de sistemas, fraudes eletrônicas, sequestro de dados (*ransomware*), espionagem e vazamentos de informações passaram a ocorrer em larga escala, explorando vulnerabilidades tecnológicas e, principalmente, falhas humanas. As consequências desses ataques vão além de prejuízos financeiros: podem comprometer a continuidade de operações, abalar a confiança dos usuários, impactar a imagem institucional e violar direitos fundamentais à privacidade e à proteção de dados pessoais **(WHITMAN; MATTORD, 2019)**.

Diante de um cenário de riscos cada vez mais complexos e sofisticados, a Segurança da Informação emerge como área central e estratégica para organizações públicas e privadas, bem como para cidadãos que dependem intensamente de recursos digitais. Ela busca proteger ativos informacionais por meio de políticas, controles técnicos, processos de governança e práticas preventivas e reativas que garantam a confidencialidade, integridade e disponibilidade dos dados **(BEAL, 2008)**.

Além disso, o crescimento de tecnologias como computação em nuvem, Big Data, inteligência artificial e Internet das Coisas (IoT) reforça a necessidade de novos modelos de proteção capazes de acompanhar a velocidade da inovação. O fator humano ainda se destaca como o elo mais vulnerável da cadeia de segurança, o que torna imprescindível o investimento em educação digital e cultura organizacional voltada à prevenção **(MITNICK; SIMON, 2003)**.

Portanto, a discussão sobre Segurança da Informação não se restringe a questões técnicas, mas envolve também aspectos comportamentais, éticos, legais e de governança. Considerando esse panorama desafiador, este artigo analisa os principais conceitos, princípios, ameaças emergentes e práticas de mitigação que sustentam uma postura de segurança robusta e alinhada às normas internacionais, como a ISO/IEC 27001, reforçando a importância da conscientização de todos os envolvidos para a construção de ambientes digitais mais seguros e resilientes.

Revista ARACÊ
ISSN: 2358-2472

2 METODOLOGIA

Este estudo caracteriza-se como uma pesquisa bibliográfica e exploratória, baseada na análise de obras, artigos científicos, normas técnicas e documentos oficiais relacionados à Segurança da Informação. A pesquisa bibliográfica permite compreender o estado da arte, bem como identificar conceitos, práticas e desafios atuais no campo da proteção de dados **(GIL, 2008)**. A abordagem exploratória foi adotada com o objetivo de ampliar o entendimento sobre as ameaças cibernéticas emergentes e sobre os modelos de governança que orientam a implementação de políticas de segurança em diferentes contextos organizacionais.

A coleta de dados teóricos considerou referenciais clássicos da segurança, além de documentos normativos internacionalmente reconhecidos, como a ISO/IEC 27001 **(ABNT, 2022)** e diretrizes de organismos especializados em cibersegurança, como o **CERT.br (2012)**. Também foram consultadas bases e publicações atualizadas que tratam da influência da tecnologia e do fator humano na formação de ambientes digitais seguros.

Após a seleção do material, procedeu-se à análise qualitativa do conteúdo, com o intuito de identificar pontos convergentes sobre princípios, riscos e práticas de mitigação. Os resultados dessa análise foram organizados em seções temáticas, buscando apresentar uma síntese crítica do tema e contribuir para o fortalecimento do debate sobre estratégias de proteção da informação no cenário digital contemporâneo.

3 CONCEITOS FUNDAMENTAIS

A Segurança da Informação é definida como o conjunto de políticas, práticas, tecnologias e controles adotados com o objetivo de proteger ativos informacionais contra acessos indevidos, danos, modificações não autorizadas ou indisponibilidade **(ABNT, 2022)**. Para que essa proteção seja efetiva, o campo se baseia em princípios essenciais que guiam a implementação de estratégias de segurança em ambientes organizacionais e pessoais. Esses princípios formam o chamado Triângulo da Segurança da Informação, composto por confidencialidade, integridade e disponibilidade, além de outros valores complementares que fortalecem a proteção dos dados.

3.1 PRINCÍPIOS ESSENCIAIS DA SEGURANÇA DA INFORMAÇÃO

3.1.1 Confidencialidade

Garante que a informação seja acessada somente por pessoas, sistemas ou dispositivos devidamente autorizados. O objetivo é impedir vazamentos, espionagem ou exposição indevida de

Revista ARACÊ
ISSN: 2358-2472

dados sensíveis. Entre os recursos utilizados destacam-se criptografia, controle de acessos e políticas de autenticação **(PFLEEGER; PFLEEGER, 2006)**.

3.1.2 Integridade

Visa assegurar que a informação permaneça completa, precisa e livre de alterações não autorizadas durante todo o seu ciclo de vida. Mecanismos como assinaturas digitais, *hash* e auditorias são adotados para detectar ou impedir qualquer modificação maliciosa ou acidental **(STALLINGS, 2015)**.

3.1.3 Disponibilidade

Busca garantir que sistemas e dados estejam acessíveis sempre que necessário para a continuidade das operações. Para isso, utilizam-se recursos como redundância, backups, servidores de alta disponibilidade e planos de recuperação de desastres **(NAKAMURA; GEUS, 2007)**.

3.2 PRINCÍPIOS COMPLEMENTARES

Além do tripé base, outros princípios reforçam a proteção e o controle sobre o fluxo da informação:

3.2.1 Autenticidade

Refere-se à capacidade de confirmar a identidade de usuários, sistemas ou dispositivos, garantindo que a comunicação ocorra entre partes legítimas. Métodos comuns incluem autenticação multifator, certificados digitais e tokens **(KIM; SOLOMON, 2014)**.

3.2.2 Rastreabilidade (ou Auditabilidade)

Permite acompanhar o ciclo de vida da informação, registrando ações realizadas, responsáveis e momentos em que ocorreram. Essa rastreabilidade é fundamental para investigações, detecção de incidentes e prestação de contas **(WHITMAN; MATTORD, 2019)**.

3.2.3 Não Repúdio

Assegura que ações realizadas em sistemas e transações eletrônicas não possam ser negadas posteriormente pelos envolvidos. Isso fortalece a confiança e a validade legal dos processos digitais **(NAKAMURA; GEUS, 2007)**.

Revista ARACÊ
ISSN: 2358-2472

3.3 ATIVOS INFORMACIONAIS E CICLO DE VIDA DOS DADOS

A proteção da informação abrange não apenas sistemas computacionais, mas todo e qualquer ativo que possua valor para a organização, incluindo documentos físicos, pessoas, infraestrutura e conhecimento organizacional. Além disso, a segurança deve ser aplicada em todas as etapas do ciclo de vida dos dados: criação, armazenamento, processamento, transmissão, arquivamento e descarte seguro **(BEAL, 2008)**.

4 PRINCIPAIS AMEAÇAS E VULNERABILIDADES

O crescimento do uso da internet e da transformação digital tem aumentado a complexidade e a diversidade das ameaças cibernéticas. Ataques que antes eram simples e facilmente identificáveis tornaram-se altamente sofisticados, explorando falhas em sistemas, redes e principalmente no comportamento humano **(SCHNEIER, 2000)**. As vulnerabilidades podem surgir devido a erros de configuração, falta de atualizações, baixo nível de conhecimento dos usuários ou até mesmo por ações mal-intencionadas de indivíduos internos às organizações. A seguir, destacam-se algumas das principais categorias de ataques e ameaças existentes.

4.1 ENGENHARIA SOCIAL E PHISHING

A engenharia social consiste em manipular usuários para que revelem informações confidenciais ou realizem ações que comprometam a segurança. O *phishing* é a técnica mais comum, em que o criminoso utiliza comunicações falsas — e-mails, mensagens ou páginas clonadas — para enganar vítimas e roubar dados pessoais, bancários ou credenciais de acesso **(MITNICK; SIMON, 2003)**. Suas variações incluem *spear phishing* (alvos específicos) e *smishing* (via SMS).

4.2 MALWARES

Malwares são softwares maliciosos desenvolvidos com o intuito de causar danos, roubo ou sequestro de dados. Segundo o **CERT.br (2012)**:

- **Vírus:** se replicam inserindo código malicioso em arquivos.
- **Ransomware:** sequestra dados, exigindo pagamento para a liberação do acesso.
- **Trojans:** disfarçam-se como programas legítimos para obter controle do dispositivo.
- Spyware: monitora e coleta informações do usuário sem consentimento.

A evolução desses softwares ameaça desde dispositivos pessoais até grandes infraestruturas corporativas.

Revista ARACÊ
ISSN: 2358-2472

4.3 VAZAMENTO DE DADOS E INVASÃO DE PRIVACIDADE

O acesso não autorizado a informações sensíveis pode gerar graves prejuízos legais e reputacionais. Dados pessoais, quando expostos, podem ser utilizados para extorsão, roubos de identidade e fraudes diversas. Além disso, leis como a LGPD estabelecem responsabilização e exigem medidas robustas de segurança **(BRASIL, 2018)**.

4.4 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)

Esses ataques têm como objetivo sobrecarregar sistemas e servidores com alto volume de requisições, tornando serviços indisponíveis para os usuários legítimos. São frequentemente utilizados contra sites corporativos, bancos, serviços de governo e plataformas online críticas **(TANENBAUM; WETHERALL, 2011)**.

4.5 EXPLORAÇÃO DE FALHAS EM IOT E DISPOSITIVOS CONECTADOS

Com a popularização de dispositivos conectados, como câmeras, sensores industriais, *wearables* e eletrodomésticos inteligentes, surgiram novas vulnerabilidades. Muitos desses equipamentos possuem baixa proteção, senhas fracas ou não recebem atualizações, facilitando invasões e formação de *botnets* para ataques automatizados **(STALLINGS, 2015)**.

4.6 AMEAÇAS INTERNAS

Funcionários, terceirizados ou usuários com acesso autorizado podem representar riscos, seja por falhas humanas, erros operacionais ou condutas maliciosas motivadas por interesses pessoais. Esse tipo de ameaça costuma ser o mais difícil de detectar, exigindo monitoramento, controle de privilégios e políticas claras de segurança **(WHITMAN; MATTORD, 2019)**.

5 NORMAS E GOVERNANÇA EM SEGURANÇA

A governança em Segurança da Informação refere-se ao conjunto de estratégias, políticas e processos adotados por uma organização com o objetivo de proteger seus ativos informacionais e garantir que decisões relacionadas à segurança estejam alinhadas às metas corporativas. Para isso, diferentes normas, legislações e *frameworks* internacionais oferecem diretrizes estruturadas que orientam as melhores práticas de gestão de riscos e conformidade legal. A adoção dessas referências contribui para a criação de ambientes seguros, confiáveis e com maior resiliência diante das constantes ameaças digitais **(ABNT, 2022)**.

Revista ARACÊ
ISSN: 2358-2472

5.1 NORMAS E LEGISLAÇÕES RELEVANTES

5.1.1 ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Norma internacional que estabelece requisitos para implementar, manter e aprimorar continuamente um sistema de gestão de segurança. Baseia-se na análise de riscos e na definição de controles, garantindo proteção adequada à criticidade das informações **(ABNT, 2022)**.

5.1.2 LGPD – Lei Geral de Proteção de Dados Pessoais (Brasil)

Lei que regulamenta o tratamento de dados pessoais em território nacional, assegurando direitos aos titulares de dados e impondo obrigações às organizações. Visa à proteção da privacidade e à transparência no uso das informações, prevendo sanções para violações **(BRASIL, 2018)**.

5.1.3 NIST Cybersecurity Framework

Modelo desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos que oferece diretrizes para prevenção, detecção e resposta a incidentes, estruturado em cinco funções principais: identificar, proteger, detectar, responder e recuperar **(NIST, 2018)**.

5.2 POLÍTICA ORGANIZACIONAL DE SEGURANÇA

Para aplicar as diretrizes normativas de forma eficaz, as instituições devem desenvolver políticas internas que estabeleçam regras, responsabilidades e mecanismos de proteção. Entre os elementos fundamentais estão:

5.2.1 Políticas de Acesso e Senhas

Definição de critérios e controles para autenticação e gerenciamento de privilégios, garantindo que usuários tenham acesso apenas ao que é necessário para suas funções **(BEAL, 2008)**.

5.2.2 Gestão de Incidentes de Segurança

Processos estruturados para identificação, registro, contenção, análise e recuperação após ocorrências de incidentes cibernéticos, reduzindo impactos e prevenindo recorrências **(KIM; SOLOMON, 2014)**.

5.2.3 Classificação e Tratamento da Informação

Organização dos dados em categorias com diferentes níveis de criticidade, definindo procedimentos adequados para armazenamento, compartilhamento e descarte.

Revista ARACÊ
ISSN: 2358-2472

5.2.4 Auditorias e Monitoramento Contínuo

Avaliações periódicas e ferramentas de monitoramento são utilizadas para verificar conformidade, identificar vulnerabilidades e garantir aprimoramento contínuo das medidas de segurança.

6 BOAS PRÁTICAS DE PROTEÇÃO

A adoção de boas práticas de segurança é fundamental para reduzir a exposição a riscos, preservar a continuidade das operações e proteger a integridade dos dados. Essas práticas envolvem tanto soluções tecnológicas quanto a conscientização dos usuários, uma vez que a proteção efetiva depende da integração entre pessoas, processos e ferramentas. A seguir, destacam-se medidas essenciais para a construção de um ambiente digital seguro.

6.1 AUTENTICAÇÃO E CONTROLE DE ACESSO

O uso de autenticação multifator (MFA) fortalece a validação da identidade do usuário, dificultando o acesso indevido mesmo em casos de vazamento de senhas. Além disso, o controle de acessos baseado em privilégios mínimos assegura que cada usuário tenha apenas as permissões necessárias ao exercício de suas funções **(PFLEEGER; PFLEEGER, 2006)**.

6.2 ATUALIZAÇÕES E CORREÇÕES DE VULNERABILIDADES

A aplicação regular de atualizações e *patches* em sistemas, softwares e dispositivos corrige falhas conhecidas e fecha brechas exploradas por criminosos. A ausência desse cuidado pode permitir a exploração de vulnerabilidades já catalogadas e amplamente utilizadas em ataques automatizados.

6.3 GESTÃO DE BACKUP E CONTINUIDADE

O backup sistemático de dados, realizado em múltiplos locais e com verificação periódica de integridade, é essencial para recuperação após incidentes como *ransomware*, falhas de hardware ou desastres naturais. Essa prática deve estar alinhada a planos de continuidade de negócios e recuperação de desastres **(WHITMAN; MATTORD, 2019)**.

6.4 CRIPTOGRAFIA E PROTEÇÃO DE DADOS SENSÍVEIS

A criptografia protege informações armazenadas e transmitidas, tornando-as inacessíveis a invasores mesmo que interceptadas. Essa medida é especialmente importante para dados pessoais, financeiros e estratégicos **(STALLINGS, 2015)**.

Revista ARACÊ
ISSN: 2358-2472

6.5 DEFESA DE PERÍMETRO E MONITORAMENTO

Ferramentas como *firewalls*, sistemas de detecção e prevenção de intrusão (IDS/IPS) e antivírus corporativos monitoram o tráfego de rede e identificam comportamentos suspeitos. O monitoramento proativo contribui para a rápida detecção de ataques, mitigando danos **(NAKAMURA; GEUS, 2007)**.

6.6 CONSCIENTIZAÇÃO E CULTURA ORGANIZACIONAL

A educação continuada dos usuários é considerada uma das medidas mais eficazes, pois o fator humano permanece como a principal fonte de vulnerabilidades. Treinamentos, campanhas internas e simulações de ataques ajudam a promover comportamentos seguros no ambiente digital **(SCHNEIER, 2000)**.

7 CONSIDERAÇÕES FINAIS

A segurança da informação é uma estratégia contínua e essencial em um cenário digital cada vez mais complexo, no qual a tecnologia evolui rapidamente e as ameaças se tornam mais sofisticadas. Investir em soluções tecnológicas, alinhadas à governança e à capacitação humana, reduz riscos e fortalece a resiliência organizacional diante de incidentes que podem causar sérios impactos financeiros, operacionais e reputacionais. A proteção de dados deixou de ser apenas uma demanda técnica e passou a constituir um requisito legal e ético, especialmente diante da crescente preocupação social com a privacidade e o uso responsável das informações **(BRASIL, 2018)**.

Nesse sentido, a construção de uma postura de segurança eficaz depende da combinação entre práticas preventivas robustas, mecanismos eficientes de resposta a incidentes e, sobretudo, do desenvolvimento de uma cultura organizacional voltada ao uso consciente e responsável da tecnologia. À medida que novas ferramentas digitais surgem — como inteligência artificial, computação em nuvem e Internet das Coisas — também emergem desafios inéditos que exigem atualização constante de políticas e processos de segurança.

Conclui-se que a segurança da informação deve ser tratada como prioridade estratégica e compartilhada por todos os setores de uma organização, já que qualquer falha humana ou técnica pode comprometer a proteção dos dados e a continuidade das operações. Assim, o futuro da segurança está na integração entre inovação tecnológica, gestão eficiente de riscos e fortalecimento das competências humanas, garantindo ambientes digitais mais confiáveis, éticos e resilientes.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: Segurança da informação, segurança cibernética e proteção de privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

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: 03 dez. 2025.

CERT.br. **Cartilha de Segurança para Internet**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/. Acesso em: 03 dez. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

KIM, David; SOLOMON, Michael G. **Fundamentals of Information Systems Security**. 2. ed. Burlington: Jones & Bartlett Learning, 2014.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

NIST. National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity**. Version 1.1. Gaithersburg: NIST, 2018.

PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence. **Security in Computing**. 4. ed. Upper Saddle River: Prentice Hall, 2006.

SCHNEIER, Bruce. **Secrets and Lies**: Digital Security in a Networked World. New York: John Wiley & Sons, 2000.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of Information Security**. 6. ed. Boston: Cengage Learning, 2019.