INTERFACE TECNOLÓGICA

TECNOLOGIA EM INFORMÁTICA
Interface Tecnológica · v. 23, n. 1, 2026 · p. 136–144
ISSN on-line 2447-0864 · ISSN impresso 1807-3980
https://doi.org/10.31510/infa.v23i1.2467

CYBER SEGURANÇA E PERÍCIA FORENSE

Cybersecurity and digital forensics

Stephanie Fortunato Tavares[1]

AUTORIA

[1] **Stephanie Fortunato Tavares**
Fatec Taquaritinga – SP – Brasil
stephaniefortava@gmail.com
ORCID: https://orcid.org/0009-0003-1335-9952

HISTÓRICO

Recebido	27/04/2026
Aceito	06/06/2026
Publicado	30/06/2026

COMO CITAR

TAVARES, S. F. Cyber segurança e perícia forense. **Interface Tecnológica**, Taquaritinga, v. 23, n. 1, p. 136-144, 2026. DOI: 10.31510/infa.v23i1.2467.

LICENÇA

Artigo de acesso aberto distribuído sob a licença Creative Commons Atribuição 4.0 Internacional.

cc BY 4.0

RESUMO

O avanço das tecnologias da informação ampliou significativamente a dependência de sistemas digitais nas organizações, trazendo consigo novos desafios relacionados à segurança da informação. Nesse contexto, o analista de sistemas assume papel essencial na prevenção de vulnerabilidades, no desenvolvimento seguro de software e no suporte a investigações forenses. Este trabalho tem como objetivo analisar os fundamentos da segurança da informação, as práticas de desenvolvimento seguro, os aspectos da perícia digital em ambientes tecnológicos e a legislação brasileira aplicada à cibersegurança. A metodologia utilizada é de caráter bibliográfico e qualitativo. Conclui-se que a integração entre práticas técnicas e conformidade legal é fundamental para garantir a proteção de dados e a confiabilidade dos sistemas.

Palavras-chave: Segurança da informação. Desenvolvimento seguro. Perícia digital. LGPD. Analista de sistemas.

ABSTRACT

The advancement of information technologies has significantly increased the dependence of organizations on digital systems, bringing with it new challenges related to information security. In this context, the systems analyst plays a crucial role in preventing vulnerabilities, developing secure software, and supporting forensic investigations. This study aims to analyze the fundamentals of information security, secure development practices, aspects of digital forensics in technological environments, and Brazilian legislation applied to cybersecurity. The methodology used is bibliographic and qualitative in nature. It is concluded that the integration between technical practices and legal compliance is essential to ensure data protection and system reliability.

Keywords: Information security. Secure development. Digital forensics. LGPD. Systems analyst.

1 SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA

A segurança da informação é um dos principais pilares da gestão de sistemas modernos, sendo responsável por proteger dados contra acessos indevidos, alterações não autorizadas e indisponibilidade. Seus fundamentos estão baseados na chamada tríade CIA: confidencialidade, integridade e disponibilidade.

De acordo com Laudon e Laudon (2020, p. 312), “a segurança da informação envolve políticas, procedimentos e medidas técnicas destinadas a proteger os ativos informacionais de uma organização”. A confidencialidade assegura que apenas usuários autorizados tenham acesso às informações; a integridade garante que os dados permaneçam corretos e inalterados; e a disponibilidade assegura o acesso quando necessário.

Além desses princípios, a governança de segurança da informação estabelece diretrizes para alinhar a segurança aos objetivos organizacionais. Segundo a norma ISO/IEC 27001, a gestão da segurança deve ser baseada na análise de riscos e na implementação de controles adequados.

Nesse cenário, o analista de sistemas desempenha um papel estratégico, pois participa diretamente da implementação dessas políticas no desenvolvimento e manutenção de sistemas. Conforme Behl e Behl (2017, p. 58), "a governança eficaz de segurança depende tanto de políticas bem definidas quanto da correta implementação técnica dessas diretrizes".

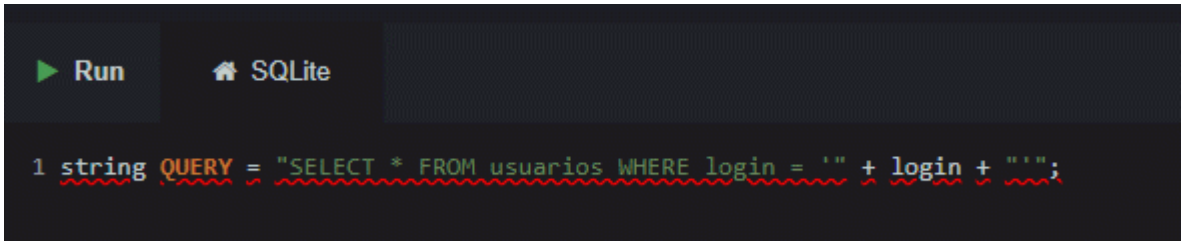
A auditoria também é um componente essencial, permitindo verificar se os controles estão sendo aplicados corretamente. Assim, a atuação do analista não se limita ao desenvolvimento, mas envolve também a garantia de conformidade e a melhoria contínua dos processos de segurança.

2 DESENVOLVIMENTO DE CÓDIGO SEGURO

O desenvolvimento de código seguro consiste na adoção de práticas que minimizem vulnerabilidades desde as fases iniciais do ciclo de vida do software. Falhas de segurança frequentemente decorrem de erros simples de programação, como ausência de validação de entrada ou uso inadequado de dados sensíveis.

Segundo McGraw (2006, p. 4), "a maioria dos problemas de segurança em software poderia ser evitada se práticas seguras fossem aplicadas desde o início do desenvolvimento". Entre as vulnerabilidades mais comuns destacam-se ataques de injeção, falhas de autenticação e exposição de dados.

Figura 1 – SQL Injection: forma incorreta

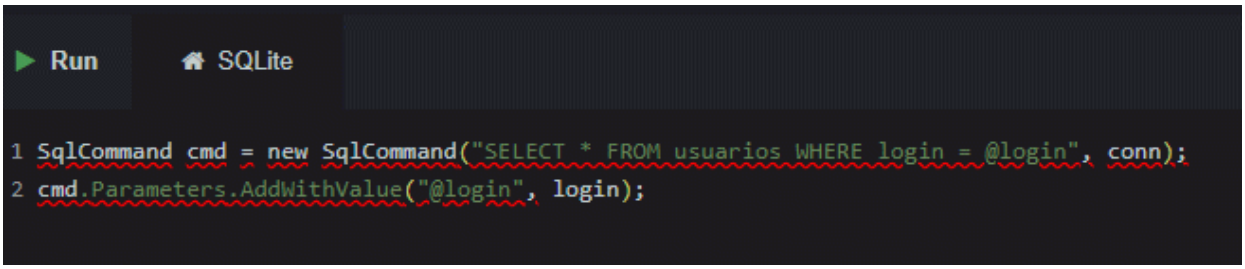


Fonte: Elaborado pelo autor (2026).

Um exemplo clássico é a vulnerabilidade de SQL Injection, causada pela construção inadequada de consultas:

Nesse caso, o sistema permite que o usuário insira comandos maliciosos. A forma correta de evitar esse problema é utilizar consultas parametrizadas:

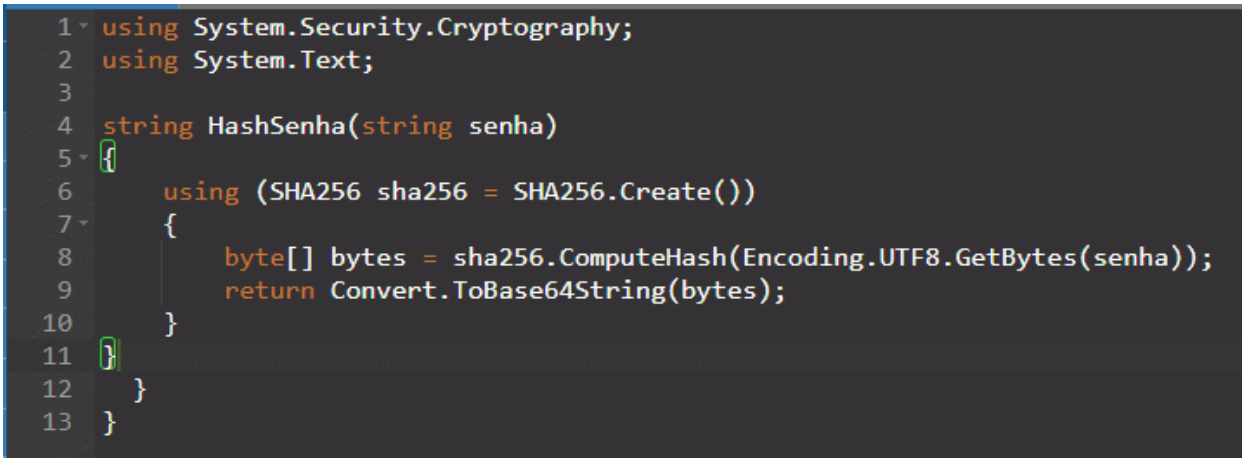
Figura 2 – SQL Injection: forma correta



Fonte: Elaborado pelo autor (2026).

De acordo com a OWASP (2021), "consultas parametrizadas são uma das formas mais eficazes de prevenir ataques de injeção".

Figura 3 – Segurança em C#



```
1  using System.Security.Cryptography;
2  using System.Text;
3
4  string HashSenha(string senha)
5  {
6      using (SHA256 sha256 = SHA256.Create())
7      {
8          byte[] bytes = sha256.ComputeHash(Encoding.UTF8.GetBytes(senha));
9          return Convert.ToBase64String(bytes);
10     }
11 }
12   }
13 }
```

Fonte: Elaborado pelo autor (2026).

Outro ponto crítico é o armazenamento de senhas. Conforme Kurose e Ross (2021, p. 45), "senhas nunca devem ser armazenadas em texto puro, devendo ser protegidas por funções de hash seguras". Um exemplo simples de proteção seria:

O analista de sistemas deve ainda adotar práticas como autenticação multifator, controle de acesso e registro de logs. Essas ações não apenas aumentam a segurança, mas também facilitam auditorias e investigações futuras.

3 PERÍCIA DIGITAL EM AMBIENTES EM NUVEM

A perícia digital consiste no conjunto de técnicas e procedimentos utilizados para identificar, coletar, preservar, analisar e apresentar evidências digitais de forma juridicamente válida. Sua aplicação torna-se indispensável no contexto atual, marcado pelo crescimento exponencial de crimes cibernéticos e pela digitalização de processos organizacionais.

De acordo com Casey (2011, p. 7), "a evidência digital deve ser coletada e preservada de forma que sua integridade seja mantida, garantindo sua admissibilidade em tribunal". Esse princípio está diretamente relacionado à cadeia de custódia, que assegura a rastreabilidade da evidência

desde sua coleta até sua apresentação em juízo, evitando qualquer tipo de contaminação ou adulteração.

Nesse contexto, a atuação do analista de sistemas torna-se estratégica, pois é ele quem projeta e implementa sistemas capazes de registrar eventos relevantes com precisão. Logs de sistema, trilhas de auditoria e registros de acesso são fundamentais para reconstruir incidentes de segurança. Um exemplo típico de log pode ser observado a seguir:

2025-03-10 02:14:33 - login_failed - usuario: admin - IP: 185.23.45.12

Esse tipo de registro permite identificar padrões suspeitos, como tentativas repetidas de acesso, indicando possíveis ataques de força bruta. Conforme Carrier (2005, p. 120), "a análise de logs é frequentemente o ponto de partida para a reconstrução de incidentes de segurança".

Com a adoção crescente da computação em nuvem, a perícia digital passou a enfrentar desafios adicionais. Entre eles destacam-se a descentralização dos dados, a volatilidade das informações e a dependência de provedores externos. Segundo Behl e Behl (2017, p. 143), "a computação em nuvem introduz complexidades na aquisição de evidências devido à falta de controle físico sobre a infraestrutura".

Além disso, questões legais relacionadas à jurisdição e à localização dos dados tornam o processo pericial ainda mais complexo. Em muitos casos, as informações podem estar armazenadas em servidores localizados em diferentes países, exigindo cooperação internacional para acesso às evidências.

Outro ponto relevante é a necessidade de ferramentas especializadas para análise forense, capazes de lidar com grandes volumes de dados e identificar padrões ocultos. A automação desse processo tem se mostrado essencial, especialmente em ambientes corporativos.

3.1 Perícia digital e crimes cibernéticos com o uso de inteligência artificial

O avanço da Inteligência Artificial (IA) trouxe benefícios significativos para a área de tecnologia, mas também abriu novas possibilidades para a prática de crimes cibernéticos, tornando o trabalho pericial ainda mais complexo e desafiador.

Entre os principais crimes associados ao uso de IA, destacam-se os chamados *deepfakes*, que consistem na criação de vídeos, áudios ou imagens falsificadas com alto grau de realismo. Segundo Chesney e Citron (2019, p. 1753), "os deepfakes representam uma ameaça significativa à confiança na informação digital, podendo ser utilizados para fraudes, manipulação política e extorsão".

Outro exemplo relevante envolve ataques automatizados, nos quais algoritmos de IA são utilizados para explorar vulnerabilidades em sistemas de forma mais rápida e eficiente. Esses ataques podem incluir:

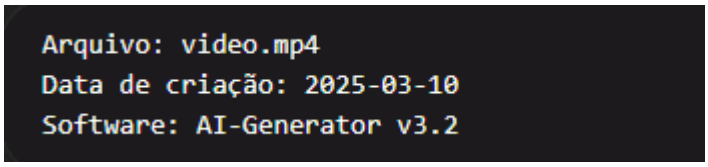
- Tentativas automatizadas de invasão (ataques de força bruta inteligentes);
- Phishing altamente personalizado;
- Geração de códigos maliciosos adaptativos.

Além disso, a IA também pode ser utilizada para análise de comportamento de usuários, permitindo ataques mais sofisticados e difíceis de detectar. Conforme Russell e Norvig (2021, p. 1021), "sistemas baseados em IA podem aprender padrões e adaptar estratégias, o que aumenta significativamente o potencial de uso malicioso".

Do ponto de vista da perícia digital, a identificação desses crimes exige técnicas mais avançadas. No caso de deepfakes, por exemplo, peritos utilizam análise de inconsistências em pixels, padrões de compressão e assinaturas digitais para verificar a autenticidade de arquivos.

Um exemplo prático de análise pode envolver a verificação de metadados de um arquivo:

Figura 4 – Verificação de arquivo



Fonte: Elaborado pelo autor (2026).

Essas informações podem indicar a utilização de ferramentas automatizadas na criação do conteúdo, servindo como evidência em investigações.

Nesse cenário, o analista de sistemas assume um papel ainda mais relevante, sendo responsável por:

- Implementar mecanismos de detecção de atividades anômalas;
- Garantir a integridade dos registros digitais;
- Desenvolver sistemas resilientes a ataques automatizados;
- Apoiar a coleta de evidências confiáveis.

Além disso, a integração entre segurança da informação, desenvolvimento seguro e perícia digital torna-se essencial para enfrentar os desafios impostos pela evolução tecnológica.

Conclui-se, portanto, que a perícia digital não apenas acompanha a evolução da tecnologia, mas também precisa se adaptar continuamente às novas ameaças, especialmente aquelas potencializadas pela Inteligência Artificial.

4 LEGISLAÇÃO E CIBERSEGURANÇA

A legislação brasileira voltada à cibersegurança tem evoluído de forma significativa nas últimas décadas, acompanhando o avanço das tecnologias digitais e o aumento expressivo de incidentes de segurança. Esse conjunto normativo busca não apenas proteger dados pessoais, mas também estabelecer responsabilidades legais para organizações e indivíduos no ambiente digital.

Um dos principais marcos regulatórios nesse cenário é a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que introduziu no Brasil um modelo estruturado de governança de dados. Conforme destaca Doneda (2020, p. 85), “a LGPD estabelece um novo paradigma de proteção de dados no Brasil, baseado na responsabilidade, transparência e no respeito aos direitos fundamentais”.

A LGPD define princípios essenciais, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados e segurança. Na prática, isso exige que sistemas sejam desenvolvidos com mecanismos de proteção desde sua concepção, conceito conhecido como *privacy by design*. Segundo Bioni (2019, p. 102), “a proteção de dados deve ser incorporada ao ciclo de vida dos sistemas, e não tratada como um elemento adicional posterior”.

Nesse contexto, o analista de sistemas assume papel fundamental ao implementar soluções técnicas que garantam a conformidade legal. Um exemplo claro é a utilização de criptografia para proteção de dados sensíveis:

Figura 5 – Erro de criptografia

```
using System.Security.Cryptography;
using System.Text;

string Criptografar(string texto)
{
    using (Aes aes = Aes.Create())
    {
        var encryptor = aes.CreateEncryptor(aes.Key, aes.IV);
        byte[] bytes = Encoding.UTF8.GetBytes(texto);
        return Convert.ToBase64String(encryptor.TransformFinalBlock(bytes, 0, bytes.Length));
    }
}
```

Fonte: Elaborado pelo autor (2026).

A adoção de criptografia atende diretamente ao princípio da segurança previsto na LGPD, que determina a utilização de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados (BRASIL, 2018).

Além da LGPD, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece diretrizes fundamentais para o uso da internet no Brasil. A legislação determina, por exemplo, a obrigatoriedade da guarda de registros de acesso, que devem ser armazenados de forma segura e sigilosa. Conforme o texto legal, "o provedor de aplicações de internet deverá manter os registros de acesso sob sigilo, em ambiente controlado e de segurança" (BRASIL, 2014).

Esses registros possuem grande relevância em investigações de crimes digitais, pois permitem rastrear atividades e identificar possíveis responsáveis por incidentes. A ausência ou falha na coleta desses dados pode comprometer diretamente processos judiciais.

Outro importante instrumento legal é a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipifica crimes relacionados à invasão de dispositivos informáticos. Essa legislação surgiu após o vazamento de imagens pessoais da atriz Carolina Dieckmann, evidenciando a necessidade de proteção jurídica no ambiente digital.

Casos reais demonstram a relevância dessas legislações. Um exemplo marcante foi o ataque cibernético sofrido pela empresa brasileira de e-commerce Submarino, em 2022, que resultou na indisponibilidade do sistema após um ataque do tipo ransomware. Esse incidente evidenciou a importância de políticas de segurança, backups e planos de resposta a incidentes.

Outro caso relevante ocorreu com o Superior Tribunal de Justiça (STJ), que foi alvo de um ataque hacker em 2020, comprometendo seus sistemas internos. Segundo informações divulgadas na época, o ataque utilizou técnicas avançadas de invasão, reforçando a necessidade de mecanismos robustos de segurança e monitoramento.

Além disso, ataques envolvendo vazamento de dados pessoais têm se tornado frequentes no Brasil. O megavazamento de dados ocorrido em 2021, que expôs informações de milhões de brasileiros, demonstrou a fragilidade de sistemas e a importância da aplicação efetiva da LGPD.

De acordo com Pinheiro (2021, p. 132), “a proteção de dados não é apenas uma exigência legal, mas um diferencial competitivo e um fator essencial para a confiança do usuário”. Nesse sentido, organizações que investem em segurança tendem a se destacar no mercado.

Do ponto de vista técnico, o analista de sistemas deve implementar controles como:

- Criptografia de dados em trânsito e em repouso;
- Controle de acesso baseado em perfis;
- Registro e monitoramento de atividades (logs);
- Políticas de autenticação forte;
- Gestão de vulnerabilidades.

Essas práticas não apenas garantem conformidade com a legislação, mas também fortalecem a postura de segurança da organização.

Outro aspecto importante é a responsabilização em caso de incidentes. A LGPD prevê sanções administrativas que incluem advertências, multas e até a suspensão das atividades de tratamento de dados. Segundo Bioni (2019, p. 145), “a responsabilização incentiva a adoção de boas práticas e a criação de uma cultura organizacional voltada à proteção de dados”.

Dessa forma, observa-se que a legislação brasileira de cibersegurança não atua de forma isolada, mas integrada a práticas técnicas e organizacionais. O analista de sistemas, nesse cenário, desempenha um papel essencial ao traduzir requisitos legais em soluções tecnológicas eficazes.

Conclui-se, portanto, que a conformidade legal em cibersegurança depende diretamente da implementação de boas práticas no desenvolvimento de sistemas, sendo indispensável a atuação qualificada do profissional de tecnologia para garantir a proteção de dados e a segurança digital.

5 ESTUDO DE CASO

A análise de casos reais é fundamental para compreender a aplicação prática dos conceitos de segurança da informação, desenvolvimento seguro e perícia digital. Um dos incidentes mais relevantes no contexto brasileiro foi o ataque cibernético sofrido pelo Superior Tribunal de Justiça (STJ), em novembro de 2020.

O ataque comprometeu significativamente a infraestrutura tecnológica do tribunal, resultando na paralisação de sistemas internos e externos, incluindo o acesso a processos judiciais. De acordo com informações divulgadas pelo próprio órgão, tratou-se de um ataque sofisticado, com indícios de utilização de ransomware, que consiste no sequestro de dados mediante criptografia maliciosa.

Segundo relato técnico divulgado à época, “o ataque afetou múltiplos servidores e exigiu o desligamento preventivo da rede para contenção do incidente” (STJ, 2020). Esse tipo de ação é comum em cenários onde há risco de propagação lateral dentro da infraestrutura.

Do ponto de vista da perícia digital, a investigação de um incidente dessa natureza envolve diversas etapas. Inicialmente, é realizada a contenção do ataque, isolando sistemas comprometidos para evitar a continuidade da invasão. Em seguida, inicia-se o processo de coleta de evidências digitais, que inclui logs de acesso, registros de rede e imagens de disco dos servidores afetados.

Um exemplo de registro analisado em cenários semelhantes pode ser representado da seguinte forma:

2020-11-03 01:45:12 - acesso_suspeito - usuário: admin - IP: 203.0.113.45

2020-11-03 01:47:33 - execução_remota - arquivo: ransomware.exe

Esses registros permitem identificar o momento inicial da invasão, bem como as ações realizadas pelo atacante dentro do sistema. Conforme Carrier (2005, p. 134), "a correlação de eventos é essencial para reconstruir a linha do tempo de um incidente".

No caso do STJ, a investigação indicou que o ataque pode ter explorado vulnerabilidades existentes ou credenciais comprometidas, possibilitando o acesso inicial ao ambiente. A partir disso, os invasores realizaram movimentação lateral, ampliando o alcance do ataque dentro da rede.

A atuação da perícia digital nesse contexto envolve não apenas a identificação da origem do ataque, mas também a análise do impacto causado e a recuperação de dados. Segundo Casey (2011, p. 89), "a resposta a incidentes deve ser conduzida de forma estruturada, garantindo a preservação das evidências e a continuidade das operações".

Outro aspecto relevante é a importância dos backups. Em ataques de ransomware, a existência de cópias seguras e atualizadas dos dados pode evitar perdas irreversíveis. No caso analisado, a recuperação dos sistemas dependia diretamente da integridade dessas cópias.

Além disso, a investigação pode envolver a análise de artefatos digitais, como:

- Arquivos maliciosos executados no sistema;
- Registros de autenticação;
- Tráfego de rede;
- Metadados de arquivos.

Esses elementos auxiliam na identificação da técnica utilizada pelo atacante e na construção de evidências que podem ser utilizadas em processos judiciais.

Do ponto de vista do analista de sistemas, esse caso evidencia a importância de práticas preventivas, como:

- Implementação de autenticação multifator;
- Atualização constante de sistemas (patch management);
- Monitoramento contínuo de eventos;
- Segmentação de rede;
- Registro detalhado de logs.

Conforme Behl e Behl (2017, p. 167), "a prevenção continua sendo a estratégia mais eficaz contra ataques cibernéticos, especialmente quando combinada com monitoramento e resposta rápida".

Além disso, a conformidade com a legislação, como a LGPD, também se torna relevante, pois incidentes de segurança que envolvam dados pessoais podem gerar sanções legais.

O caso do STJ demonstra como ataques cibernéticos podem impactar instituições críticas e reforça a necessidade de integração entre segurança da informação, desenvolvimento seguro e perícia digital.

Conclui-se que a análise forense de incidentes reais não apenas contribui para a responsabilização dos envolvidos, mas também fornece subsídios para o aprimoramento das práticas de segurança, sendo essencial para a evolução da área de tecnologia da informação.

6 CONCLUSÃO

A segurança da informação tornou-se um elemento essencial no contexto atual, diante do aumento de ameaças digitais e da crescente dependência de sistemas tecnológicos. Ao longo deste trabalho, evidenciou-se a importância da integração entre desenvolvimento seguro, perícia digital e conformidade com a legislação brasileira.

A adoção de boas práticas de programação contribui diretamente para a redução de vulnerabilidades, enquanto a perícia digital permite a identificação e análise de incidentes de forma tecnicamente e juridicamente válida. Conforme Casey (2011, p. 7), a preservação da integridade das evidências é fundamental para sua utilização em processos legais.

No âmbito jurídico, normas como a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet reforçam a necessidade de proteção dos dados e responsabilização em casos de falhas de segurança. Segundo Doneda (2020, p. 85), a LGPD estabelece um modelo baseado na transparência e responsabilidade.

Dessa forma, conclui-se que o analista de sistemas desempenha papel fundamental na implementação de soluções seguras e na adequação às exigências legais, sendo peça-chave na construção de ambientes digitais mais seguros e confiáveis.

REFERÊNCIAS

BEHL, A.; BEHL, K. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: Oxford University Press, 2017.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre crimes informáticos.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

CARRIER, Brian. **File system forensic analysis**. Boston: Addison-Wesley, 2005.

CASEY, Eoghan. **Digital evidence and computer crime**. 3. ed. [*S. l.*]: Academic Press, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Forense, 2020.

KUROSE, James; ROSS, Keith. **Redes de computadores e a Internet**. 7. ed. São Paulo: Pearson, 2021.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de informação gerenciais**. 16. ed. São Paulo: Pearson, 2020.

MCGRAW, Gary. **Software security**: building security in. Boston: Addison-Wesley, 2006.

OWASP. **OWASP Top 10 – 2021**. [*S. l.*], 2021. Disponível em: https://owasp.org. Acesso em: 2026.

PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva, 2021.

STALLINGS, William. **Criptografia e segurança de redes**. 7. ed. São Paulo: Pearson, 2018.

Os conceitos e as opiniões expressos neste artigo são de responsabilidade exclusiva de seus autores.