RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

A convergência entre cibersegurança e aplicações móveis em ecossistemas empresariais

The convergence between cybersecurity and mobile applications in enterprise ecosystems

La convergencia entre ciberseguridad y aplicaciones móviles en ecosistemas empresariales

Adriano Souza Reis

Tecnólogo em Gestão da Tecnologia da Informação (Uni-Anhanguera);
Pós-Graduado em Inteligência Artificial, Desenvolvimento de Aplicações para Dispositivos Móveis e Cybersecurity (Faculdade Iguaçu);
Doutor Honoris Causa em Tecnologia da Informação (UNISCECAP);
Acadêmico Titular da ABRASCI.

RESUMO

A crescente adoção de aplicações móveis no ambiente corporativo transformou significativamente a forma como organizações executam processos, compartilham informações e apoiam a tomada de decisão. A ampliação da mobilidade proporcionou maior agilidade operacional, porém também expandiu a superfície de exposição a ameaças cibernéticas, tornando a segurança da informação um requisito estratégico no desenvolvimento de software para dispositivos móveis. Este artigo analisa a relação entre desenvolvimento de aplicações móveis e cibersegurança em ecossistemas empresariais, discutindo os principais riscos associados ao uso de dispositivos móveis, bem como as práticas recomendadas para proteção de dados, autenticação de usuários, comunicação segura e monitoramento contínuo dos ambientes corporativos. A pesquisa caracteriza-se como uma revisão sistemática da literatura, fundamentada em livros, artigos científicos, normas técnicas e documentos produzidos por instituições reconhecidas internacionalmente, considerando publicações disponíveis até 2024. Os resultados evidenciam que a proteção das aplicações móveis depende da integração entre arquitetura segura de software, criptografia, gerenciamento de identidades, governança de dispositivos e monitoramento contínuo dos ambientes tecnológicos. Conclui-se que a segurança de aplicações móveis deve ser tratada como elemento integrante do processo de desenvolvimento de software, incorporando princípios de segurança desde as fases iniciais do projeto e acompanhando continuamente a evolução das ameaças digitais.

Palavras-chave: Cibersegurança; Aplicações Móveis; Desenvolvimento Seguro; Proteção de Dados; Mobilidade Corporativa.

ABSTRACT

The increasing adoption of mobile applications in corporate environments has significantly transformed the way organizations execute business processes, exchange information, and support decision-making. Although enterprise mobility has improved operational efficiency, it has also expanded the exposure to cyber threats, making information security a strategic requirement in mobile software development. This article analyzes the relationship between mobile application development and cybersecurity within enterprise ecosystems, discussing the main security risks associated with mobile devices and the best practices for data protection, user authentication, secure communication, and continuous monitoring of corporate environments. The study was conducted through a systematic literature review based on books, peer-reviewed scientific publications, technical standards, and reports issued by internationally recognized institutions, considering publications available up to 2024. The findings indicate that securing mobile applications requires the integration of secure software architecture, cryptography, identity management, device governance, and continuous security monitoring. It is concluded that mobile application security should be incorporated throughout the software development lifecycle, adopting security-by-design principles capable of reducing organizational exposure to emerging cyber threats.

Keywords: Cybersecurity; Mobile Applications; Secure Software Development; Data Protection;

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

Enterprise Mobility.

1 INTRODUÇÃO

A transformação digital alterou profundamente a maneira como organizações desenvolvem suas atividades, compartilham informações e administram processos de negócio. A expansão da computação em nuvem, da conectividade móvel e da disponibilidade de dispositivos inteligentes permitiu que aplicações corporativas deixassem de estar restritas aos ambientes internos das empresas, tornando-se acessíveis em qualquer localidade com conexão à internet. Essa evolução ampliou significativamente a flexibilidade operacional, favorecendo modelos de trabalho remoto, atendimento em campo, logística integrada e tomada de decisão em tempo real.

O crescimento da mobilidade corporativa representa uma das mudanças mais relevantes desse processo. Aplicações desenvolvidas para smartphones e tablets passaram a integrar rotinas relacionadas à gestão comercial, controle logístico, acompanhamento de estoques, atendimento ao cliente, operações financeiras e monitoramento de processos industriais. Como consequência, dispositivos móveis deixaram de funcionar apenas como ferramentas de comunicação para assumir papel estratégico dentro dos ecossistemas empresariais.

Entretanto, a ampliação da mobilidade também modificou o cenário de segurança da informação. Diferentemente das estações de trabalho tradicionais, normalmente protegidas por políticas centralizadas e infraestrutura corporativa, dispositivos móveis operam em ambientes heterogêneos, conectando-se frequentemente a redes públicas, equipamentos pessoais e diferentes serviços em nuvem. Essa característica amplia a superfície de ataque disponível para agentes maliciosos e exige abordagens de segurança compatíveis com a natureza distribuída desses ambientes.

Schneier (2015) observa que a evolução tecnológica amplia simultaneamente as oportunidades de inovação e os desafios relacionados à proteção das informações. À medida que novos pontos de acesso são incorporados à infraestrutura organizacional, aumenta também o número de vetores passíveis de exploração por ataques cibernéticos. Em aplicações móveis, esse cenário torna-se ainda mais complexo devido à diversidade de sistemas operacionais, fabricantes, configurações de hardware e políticas de atualização existentes no mercado.

Entre as ameaças mais frequentes destacam-se ataques de interceptação de tráfego, exploração de vulnerabilidades em APIs, comprometimento de credenciais, instalação de aplicações maliciosas, engenharia social, vazamento de informações armazenadas localmente e exploração de bibliotecas de terceiros vulneráveis. A crescente utilização de dispositivos pessoais em atividades corporativas amplia ainda mais esse cenário, dificultando o controle direto da infraestrutura tecnológica pelas

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

organizações.

Nesse contexto, observa-se uma mudança importante na forma como a segurança de aplicações móveis é concebida. Em vez de concentrar esforços exclusivamente na proteção da infraestrutura de rede, organizações passaram a incorporar mecanismos de segurança durante todas as etapas do desenvolvimento de software. Essa abordagem, conhecida como *Secure by Design*, considera que requisitos relacionados à autenticação, criptografia, gerenciamento de sessões, validação de entradas, proteção de APIs e monitoramento contínuo devem fazer parte da arquitetura da aplicação desde sua concepção, reduzindo vulnerabilidades estruturais e custos de correção posteriores.

Outro aspecto que merece destaque refere-se ao fortalecimento dos modelos de identidade digital. A utilização de autenticação multifator, protocolos modernos de autorização, gerenciamento centralizado de identidades e políticas baseadas no princípio do menor privilégio contribui para reduzir riscos associados ao comprometimento de credenciais. Paralelamente, a adoção do modelo Zero Trust modifica a lógica tradicional da segurança corporativa ao pressupor que nenhum dispositivo, usuário ou conexão deve ser considerado confiável sem validação contínua, independentemente de sua localização na rede.

Além das medidas preventivas, cresce a importância do monitoramento contínuo dos ambientes tecnológicos. Ferramentas de gerenciamento de dispositivos móveis, plataformas de gerenciamento de eventos de segurança, soluções baseadas em inteligência artificial e mecanismos automatizados de resposta a incidentes passaram a desempenhar papel essencial na identificação de comportamentos anômalos, permitindo respostas mais rápidas diante de tentativas de invasão ou comprometimento dos dispositivos.

Diante desse cenário, compreender a integração entre desenvolvimento de aplicações móveis e cibersegurança tornou-se uma necessidade tanto para pesquisadores quanto para profissionais responsáveis pelo desenvolvimento e gestão de soluções corporativas. A proteção das informações deixou de representar uma atividade isolada da área de tecnologia para tornar-se requisito estratégico relacionado à continuidade operacional, à conformidade regulatória e à preservação da confiança de clientes, parceiros e demais partes interessadas.

Assim, este artigo tem como objetivo analisar a convergência entre cibersegurança e desenvolvimento de aplicações móveis em ecossistemas empresariais, discutindo os principais riscos associados à mobilidade corporativa, as práticas contemporâneas de desenvolvimento seguro e os mecanismos tecnológicos empregados para proteger dados, usuários e sistemas em ambientes caracterizados por elevada conectividade e constante evolução das ameaças digitais.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

2 METODOLOGIA

A presente pesquisa caracteriza-se como um estudo qualitativo, de natureza exploratória e descritiva, desenvolvido por meio de revisão sistemática da literatura. Essa estratégia metodológica foi escolhida por permitir a análise crítica do conhecimento científico relacionado à segurança de aplicações móveis, reunindo contribuições provenientes das áreas de Engenharia de Software, Segurança da Informação, Arquitetura de Sistemas, Redes de Computadores e Governança de Tecnologia da Informação.

Segundo Gil (2019), pesquisas exploratórias são apropriadas quando o objetivo consiste em ampliar a compreensão sobre determinado fenômeno e organizar o conhecimento disponível em torno de um tema específico. No contexto da cibersegurança, marcado por constante evolução tecnológica, a revisão sistemática da literatura possibilita identificar tendências, práticas recomendadas, desafios emergentes e convergências entre diferentes abordagens propostas por pesquisadores e organismos internacionais.

O levantamento bibliográfico contemplou livros, artigos científicos revisados por pares, normas técnicas e documentos institucionais publicados até 2024. Foram priorizadas publicações indexadas em bases reconhecidas internacionalmente, como IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Scopus e Google Scholar, além de documentos técnicos produzidos por organizações como OWASP, NIST e FIDO Alliance.

Os critérios de seleção privilegiaram estudos relacionados à segurança de aplicações móveis, Secure Software Development Lifecycle, autenticação multifator, gerenciamento de identidades, criptografia aplicada, proteção de APIs, Mobile Device Management, Zero Trust, DevSecOps e monitoramento contínuo de ambientes corporativos. Foram excluídas publicações sem fundamentação científica, materiais exclusivamente comerciais e estudos que não apresentassem aderência aos objetivos da pesquisa.

Após a seleção das referências, realizou-se leitura analítica e comparativa dos trabalhos, organizando o conteúdo em cinco eixos temáticos: superfície de ataque em ambientes móveis, desenvolvimento seguro de software, mecanismos criptográficos, gestão de identidade e monitoramento contínuo das aplicações. Essa organização permitiu estabelecer relações entre diferentes abordagens presentes na literatura, favorecendo uma análise crítica sobre os fatores que influenciam a segurança das aplicações móveis utilizadas em ambientes corporativos.

Embora a revisão bibliográfica não envolva investigação empírica em organizações específicas, considera-se que a metodologia adotada fornece base consistente para compreender o estado atual do conhecimento científico sobre o tema, identificar boas práticas amplamente reconhecidas e discutir

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

os principais desafios enfrentados pelas organizações na proteção de seus ecossistemas móveis.

3 A SUPERFÍCIE DE ATAQUE EM AMBIENTES MÓVEIS CORPORATIVOS

A consolidação da mobilidade corporativa modificou profundamente a arquitetura dos sistemas de informação utilizados pelas organizações. A possibilidade de acessar aplicações empresariais por meio de smartphones e tablets ampliou a produtividade das equipes, reduziu barreiras geográficas e tornou processos administrativos mais ágeis. Entretanto, essa mesma flexibilidade expandiu significativamente a superfície de ataque das organizações, criando vetores de exploração para agentes maliciosos.

Diferentemente das estações de trabalho tradicionais, dispositivos móveis operam em ambientes altamente dinâmicos. Ao longo de um único dia, um mesmo equipamento pode conectar-se à rede corporativa, utilizar conexões móveis 4G ou 5G, acessar redes Wi-Fi públicas e estabelecer comunicação com diversos serviços em nuvem. Cada mudança de contexto altera o ambiente de segurança e amplia a quantidade de elementos que precisam ser protegidos.

Segundo Stallings (2018), a segurança da informação deve considerar não apenas os mecanismos tecnológicos empregados na proteção dos sistemas, mas também o ambiente em que esses sistemas operam. Em aplicações móveis, essa premissa torna-se particularmente relevante devido à elevada heterogeneidade de dispositivos, sistemas operacionais, fabricantes e versões de software presentes no ambiente corporativo.

Entre os fatores que contribuem para esse aumento da superfície de ataque destaca-se a adoção do modelo Bring Your Own Device (BYOD), no qual colaboradores utilizam dispositivos pessoais para acessar recursos institucionais. Embora essa prática reduza investimentos em infraestrutura e aumente a flexibilidade operacional, também dificulta a aplicação uniforme das políticas corporativas de segurança. Equipamentos particulares frequentemente apresentam configurações distintas, aplicações instaladas sem controle organizacional e diferentes níveis de atualização dos sistemas operacionais, aumentando a exposição a vulnerabilidades.

Outro aspecto relevante refere-se às redes utilizadas durante o acesso às aplicações corporativas. Usuários em deslocamento frequentemente estabelecem conexão por meio de redes públicas disponíveis em aeroportos, hotéis, restaurantes, centros comerciais e outros locais de grande circulação. Quando essas redes apresentam mecanismos insuficientes de proteção, tornam-se ambientes propícios para ataques de interceptação de tráfego, falsificação de pontos de acesso e captura de credenciais.

Conforme descrevem Tanenbaum e Wetherall (2011), ataques do tipo *Man-in-the-Middle* permitem

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

que um invasor intercepte a comunicação entre dois sistemas sem que os usuários percebam a existência dessa intermediação. Caso os mecanismos criptográficos empregados sejam inadequados ou inexistentes, informações confidenciais podem ser capturadas durante a transmissão, comprometendo dados financeiros, credenciais de autenticação e informações estratégicas da organização.

O armazenamento local de informações também representa importante fator de risco. Diversas aplicações móveis mantêm dados temporários para permitir funcionamento offline, reduzir consumo de banda ou melhorar a experiência do usuário. Quando esses registros permanecem armazenados sem mecanismos adequados de criptografia, dispositivos perdidos, furtados ou comprometidos podem expor informações sensíveis relacionadas às atividades da organização.

Além das ameaças relacionadas ao ambiente de comunicação, a fragmentação dos ecossistemas móveis impõe desafios adicionais ao desenvolvimento seguro. No sistema Android, por exemplo, diferentes fabricantes disponibilizam versões personalizadas do sistema operacional, com ciclos distintos de atualização de segurança. Em consequência, muitos dispositivos permanecem durante longos períodos sem receber correções para vulnerabilidades já conhecidas, ampliando a janela de exposição aos ataques.

Outro fator frequentemente explorado por agentes maliciosos refere-se à obtenção de privilégios elevados por meio de procedimentos como *rooting* ou *jailbreaking*. Essas modificações removem restrições impostas pelos fabricantes e comprometem mecanismos fundamentais de isolamento entre aplicações. Como consequência, aplicativos maliciosos podem obter acesso ampliado aos recursos do dispositivo, comprometendo informações armazenadas por aplicações corporativas e reduzindo significativamente a eficácia das proteções originalmente implementadas.

Também merece atenção o crescimento dos ataques direcionados às interfaces de programação de aplicações (APIs). Em arquiteturas modernas, aplicações móveis concentram grande parte de sua lógica de negócio nos servidores, comunicando-se continuamente por meio de APIs REST ou GraphQL. Falhas relacionadas à autenticação, autorização, validação de parâmetros ou limitação de requisições podem permitir acesso indevido a informações corporativas, comprometendo a integridade e a confidencialidade dos dados processados.

A expansão da cadeia de suprimentos de software representa outro vetor relevante de risco. O desenvolvimento contemporâneo utiliza grande quantidade de bibliotecas de código aberto, componentes reutilizáveis e serviços de terceiros. Embora esses recursos acelerem o desenvolvimento das aplicações, também ampliam a possibilidade de introdução de vulnerabilidades decorrentes de dependências comprometidas ou componentes desatualizados. Ataques recentes demonstram que a exploração da cadeia de suprimentos tornou-se uma das estratégias mais utilizadas por grupos

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

especializados em cibercrime.

Diante desse cenário, observa-se que a segurança das aplicações móveis não pode limitar-se à proteção do dispositivo ou da infraestrutura de rede. A literatura recente recomenda a adoção de modelos baseados no princípio do Zero Trust, segundo o qual nenhum usuário, equipamento ou conexão deve ser considerado confiável automaticamente. Todas as solicitações de acesso devem ser continuamente verificadas, autenticadas e autorizadas de acordo com o contexto operacional, reduzindo a probabilidade de movimentação lateral e comprometimento dos ambientes corporativos.

Portanto, a crescente mobilidade empresarial exige que a segurança seja concebida de maneira integrada, considerando simultaneamente dispositivos, usuários, aplicações, infraestrutura de comunicação, identidade digital e governança tecnológica. Somente essa abordagem sistêmica é capaz de responder à complexidade dos ecossistemas móveis contemporâneos e reduzir os riscos associados à transformação digital.

4 ENGENHARIA DE SOFTWARE ORIENTADA À SEGURANÇA (SECURE BY DESIGN)

O aumento da sofisticação das ameaças cibernéticas modificou significativamente a forma como aplicações corporativas são desenvolvidas. Modelos tradicionais, nos quais requisitos de segurança eram incorporados apenas nas etapas finais do desenvolvimento, mostraram-se insuficientes diante da crescente complexidade das arquiteturas modernas. Em resposta a esse cenário, consolidou-se o conceito de *Secure by Design*, que propõe a incorporação dos princípios de segurança desde as fases iniciais do ciclo de vida do software.

Segundo Pressman e Maxim (2020), defeitos identificados durante as etapas iniciais de especificação e arquitetura apresentam custo significativamente inferior ao das vulnerabilidades descobertas após a implantação do sistema em ambiente de produção. Além do impacto financeiro, falhas exploradas em aplicações corporativas podem comprometer a continuidade operacional, provocar vazamento de informações estratégicas e gerar prejuízos relacionados à reputação institucional.

Nesse contexto, o ciclo de desenvolvimento seguro, conhecido como Secure Software Development Lifecycle (SSDLC), amplia as atividades tradicionais de engenharia de software ao incorporar práticas específicas voltadas à identificação, prevenção e mitigação de vulnerabilidades durante todo o processo de desenvolvimento.

Uma das primeiras etapas consiste na modelagem de ameaças (*Threat Modeling*). Antes da implementação das funcionalidades, equipes de desenvolvimento analisam os ativos mais relevantes da aplicação, identificam possíveis agentes de ameaça, avaliam vulnerabilidades existentes e estabelecem controles capazes de reduzir os riscos identificados. Essa abordagem permite antecipar

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

problemas de segurança antes que eles sejam incorporados ao produto final.

Outro princípio amplamente adotado refere-se ao desenvolvimento baseado no conceito de privilégio mínimo. Aplicações móveis devem solicitar apenas as permissões estritamente necessárias ao funcionamento de suas funcionalidades. O acesso irrestrito à câmera, localização, armazenamento, contatos ou microfone aumenta desnecessariamente a superfície de ataque e amplia os impactos decorrentes de eventual comprometimento da aplicação.

A proteção do código-fonte também representa componente importante das estratégias de desenvolvimento seguro. Técnicas de ofuscação dificultam a engenharia reversa dos aplicativos distribuídos aos usuários, reduzindo a possibilidade de extração de regras de negócio, algoritmos proprietários, credenciais incorporadas inadequadamente ao código e mecanismos internos de autenticação. Embora não impeçam completamente a análise do aplicativo, essas técnicas aumentam significativamente o esforço necessário para sua exploração.

As interfaces de programação utilizadas pelas aplicações móveis merecem atenção especial durante o desenvolvimento. APIs expostas à internet constituem frequentemente o principal ponto de comunicação entre dispositivos móveis e sistemas corporativos. Em razão disso, mecanismos robustos de autenticação, autorização, validação de entradas, limitação de requisições (*rate limiting*) e registro de eventos devem integrar a arquitetura dessas interfaces, reduzindo riscos relacionados a ataques de injeção, escalonamento de privilégios e acesso não autorizado.

A crescente utilização de bibliotecas externas também exige políticas rigorosas de gestão de dependências. Grande parte das aplicações modernas incorpora componentes de código aberto responsáveis por autenticação, comunicação em rede, criptografia, persistência de dados e interface gráfica. Embora esses recursos acelerem o desenvolvimento, vulnerabilidades descobertas nessas bibliotecas podem comprometer milhares de aplicações simultaneamente. Dessa forma, torna-se essencial manter inventários atualizados das dependências utilizadas, monitorar vulnerabilidades conhecidas e realizar atualizações contínuas dos componentes empregados.

Nos últimos anos, o conceito de DevSecOps fortaleceu ainda mais essa integração entre desenvolvimento e segurança. Em vez de tratar a segurança como responsabilidade exclusiva de equipes especializadas, o modelo distribui essa responsabilidade ao longo de todo o ciclo de desenvolvimento, incorporando verificações automatizadas diretamente nas esteiras de integração e entrega contínuas.

Ferramentas de análise estática (*Static Application Security Testing – SAST*) permitem identificar vulnerabilidades diretamente no código-fonte antes da compilação da aplicação. Complementarmente, mecanismos de análise dinâmica (*Dynamic Application Security Testing – DAST*) avaliam o comportamento do software em execução, identificando falhas que somente se

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

manifestam durante sua operação. A utilização combinada dessas abordagens amplia significativamente a capacidade de identificação precoce de vulnerabilidades.

Outra prática que ganhou relevância recentemente consiste na utilização de Software Bill of Materials (SBOM), documento que relaciona todos os componentes utilizados durante a construção da aplicação. Essa abordagem facilita o gerenciamento da cadeia de suprimentos de software, permitindo identificar rapidamente quais aplicações utilizam componentes afetados por vulnerabilidades recém-descobertas e acelerando os processos de resposta a incidentes.

Também merece destaque a realização periódica de testes de intrusão e exercícios de validação de segurança. Diferentemente das análises automatizadas, essas atividades simulam o comportamento de agentes maliciosos, permitindo identificar vulnerabilidades decorrentes da interação entre diferentes componentes da arquitetura, erros de configuração ou falhas relacionadas ao ambiente operacional.

Observa-se, portanto, que o desenvolvimento seguro deixou de representar uma etapa complementar da engenharia de software para tornar-se elemento estruturante das aplicações corporativas contemporâneas. A incorporação de requisitos de segurança desde a concepção dos sistemas reduz custos, aumenta a confiabilidade das aplicações e fortalece a capacidade das organizações de responder às ameaças presentes nos ecossistemas digitais atuais.

5 PROTOCOLOS CRIPTOGRÁFICOS PARA PROTEÇÃO DE DADOS EM APLICAÇÕES MÓVEIS

A criptografia constitui um dos pilares fundamentais da segurança da informação e desempenha papel indispensável na proteção das aplicações móveis utilizadas em ambientes corporativos. À medida que dispositivos móveis passaram a processar informações estratégicas relacionadas a operações financeiras, logística, saúde, comércio eletrônico e gestão empresarial, tornou-se necessário adotar mecanismos capazes de garantir confidencialidade, integridade, autenticidade e não repúdio durante todo o ciclo de vida dos dados.

Segundo Katz e Lindell (2020), a segurança criptográfica contemporânea não depende exclusivamente da robustez dos algoritmos utilizados, mas da correta implementação dos protocolos, da gestão adequada das chaves criptográficas e da integração desses mecanismos com a arquitetura da aplicação. Vulnerabilidades relacionadas ao gerenciamento de certificados, armazenamento inadequado de chaves ou utilização incorreta de bibliotecas criptográficas podem comprometer sistemas que empregam algoritmos matematicamente seguros.

No contexto das aplicações móveis, a proteção dos dados em trânsito representa uma das primeiras

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

camadas de defesa. Informações trocadas entre dispositivos e servidores corporativos trafegam continuamente por diferentes infraestruturas de comunicação, incluindo redes móveis, conexões Wi-Fi públicas e provedores de serviços em nuvem. Essa diversidade de ambientes aumenta a possibilidade de interceptação do tráfego por agentes maliciosos caso mecanismos apropriados de proteção não sejam empregados.

Nesse cenário, a utilização do protocolo Transport Layer Security (TLS) consolidou-se como requisito básico para aplicações corporativas modernas. A versão TLS 1.3 reduziu vulnerabilidades presentes em implementações anteriores, simplificou o processo de negociação criptográfica e proporcionou ganhos tanto em desempenho quanto em segurança. Além da confidencialidade da comunicação, o protocolo garante autenticação entre cliente e servidor e mecanismos que preservam a integridade das mensagens transmitidas.

Entretanto, o uso isolado do TLS não elimina completamente os riscos associados à comunicação entre aplicações móveis e serviços corporativos. Diversos ataques exploram certificados digitais fraudulentos ou mecanismos inadequados de validação implementados pelos próprios aplicativos. Para reduzir essa possibilidade, muitas organizações adotam a técnica conhecida como *Certificate Pinning*, que consiste na validação explícita da identidade criptográfica do servidor durante o estabelecimento da conexão.

Essa abordagem impede que certificados emitidos por autoridades certificadoras comprometidas ou certificados inseridos localmente por aplicações maliciosas sejam aceitos pelo aplicativo. Embora o *Certificate Pinning* exija maior controle durante processos de renovação dos certificados digitais, sua utilização reduz significativamente a possibilidade de ataques baseados na interceptação da comunicação.

Outro aspecto relevante refere-se à proteção das informações armazenadas localmente nos dispositivos móveis. Em diversas situações, aplicações corporativas necessitam manter dados temporários para garantir funcionamento offline, sincronização posterior ou melhoria da experiência do usuário. Quando esse armazenamento é inevitável, torna-se imprescindível empregar mecanismos robustos de criptografia capazes de proteger essas informações mesmo em situações de perda, roubo ou comprometimento do dispositivo.

O algoritmo Advanced Encryption Standard (AES), especialmente em implementações com chaves de 256 bits, permanece como uma das principais recomendações para proteção de dados em repouso. Entretanto, a literatura destaca que a eficácia desse mecanismo depende diretamente da forma como as chaves criptográficas são armazenadas e gerenciadas. O armazenamento das chaves diretamente no código da aplicação ou em arquivos de configuração representa prática inadequada, pois facilita sua extração por meio de engenharia reversa.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

Para reduzir esse risco, sistemas operacionais móveis disponibilizam ambientes protegidos destinados especificamente ao armazenamento seguro de credenciais criptográficas. No Android, essa função é desempenhada pelo Android Keystore, enquanto dispositivos iOS utilizam o Keychain Services associado ao Secure Enclave. Esses componentes mantêm as chaves isoladas do restante do sistema operacional, reduzindo significativamente a probabilidade de comprometimento mesmo diante de aplicações maliciosas executadas no dispositivo.

Além da confidencialidade, a integridade das informações também deve ser assegurada. Algoritmos criptográficos destinados à geração de funções resumo (*hash functions*) permitem verificar se determinado arquivo ou mensagem sofreu alterações durante seu armazenamento ou transmissão. Entretanto, algoritmos historicamente utilizados, como MD5 e SHA-1, apresentam vulnerabilidades conhecidas e deixaram de ser recomendados para aplicações que exigem elevados níveis de segurança. Atualmente, recomenda-se a utilização de algoritmos pertencentes às famílias SHA-2 ou SHA-3, de acordo com as necessidades específicas da aplicação.

Outro tema que ganhou importância nos últimos anos refere-se à preparação das arquiteturas criptográficas para o avanço da computação quântica. Embora ataques práticos contra os algoritmos atualmente utilizados ainda não representem risco imediato para a maioria das organizações, instituições responsáveis pela padronização internacional já iniciaram o processo de desenvolvimento e adoção de algoritmos resistentes à computação quântica. Essa perspectiva reforça a necessidade de arquiteturas criptográficas flexíveis, capazes de incorporar novos padrões à medida que forem oficialmente estabelecidos.

Portanto, observa-se que a proteção criptográfica das aplicações móveis depende da combinação entre algoritmos robustos, implementação correta dos protocolos, gerenciamento seguro das chaves e atualização contínua das bibliotecas utilizadas. A criptografia deve ser compreendida como componente integrante da arquitetura da aplicação e não como recurso complementar incorporado apenas nas fases finais do desenvolvimento.

6 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO EM APLICAÇÕES MÓVEIS

À medida que aplicações móveis passaram a disponibilizar funcionalidades críticas para organizações públicas e privadas, o gerenciamento de identidade tornou-se elemento central das estratégias de segurança da informação. A simples utilização de credenciais compostas por nome de usuário e senha mostrou-se insuficiente para responder ao crescimento das ameaças relacionadas ao comprometimento de contas, reutilização de senhas e ataques automatizados direcionados aos sistemas corporativos.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

Diversos estudos demonstram que credenciais comprometidas permanecem entre os principais vetores utilizados para invasões em ambientes corporativos. Ataques baseados em força bruta, *credential stuffing*, engenharia social e campanhas de *phishing* exploram comportamentos recorrentes dos usuários, como reutilização de senhas e adoção de combinações previsíveis. Em razão desse cenário, organizações passaram a incorporar mecanismos adicionais de autenticação capazes de reduzir significativamente a probabilidade de acesso não autorizado.

A autenticação multifator (MFA) consolidou-se como uma das medidas mais eficazes nesse contexto. O princípio consiste na utilização simultânea de dois ou mais fatores independentes para validação da identidade do usuário, combinando informações que ele conhece, possui ou representa biologicamente. Mesmo que uma senha seja comprometida, a ausência dos demais fatores dificulta substancialmente a exploração da credencial obtida pelo atacante.

Nas aplicações móveis, a integração entre autenticação multifator e recursos biométricos tornou-se particularmente eficiente devido à presença de sensores nativos incorporados aos dispositivos modernos. Impressões digitais, reconhecimento facial e outros mecanismos biométricos podem ser utilizados para validar a identidade do usuário sem que os dados biométricos precisem ser transmitidos aos servidores corporativos. Em arquiteturas compatíveis com os padrões da FIDO Alliance, a verificação ocorre localmente no dispositivo, preservando a privacidade do usuário e reduzindo a exposição de informações sensíveis.

Além da autenticação, o gerenciamento das sessões estabelecidas entre dispositivos móveis e servidores corporativos exige mecanismos específicos de proteção. Diferentemente das aplicações tradicionais baseadas em sessões persistentes, arquiteturas modernas frequentemente utilizam protocolos de autorização baseados em tokens, como OAuth 2.0 e OpenID Connect, associados à utilização de JSON Web Tokens (JWT) quando apropriado. Esses mecanismos permitem controlar o tempo de validade das credenciais, limitar os privilégios concedidos e facilitar processos de revogação de acesso.

Entretanto, a literatura também destaca que a utilização de JWT exige cuidados relacionados ao armazenamento dos tokens, ao controle de sua expiração e à proteção contra ataques de reutilização (*replay attacks*). A adoção de tokens com curto período de validade, associada à renovação controlada e ao armazenamento seguro das credenciais, reduz significativamente essas vulnerabilidades.

Outro componente fundamental refere-se ao gerenciamento centralizado de identidades. Soluções de Single Sign-On (SSO) permitem que usuários se autentiquem uma única vez para acessar diferentes aplicações corporativas, simplificando a experiência de uso e reduzindo a proliferação de credenciais independentes. Sob a perspectiva administrativa, essa abordagem facilita o gerenciamento de permissões, auditoria de acessos e revogação imediata das autorizações quando necessário.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

O gerenciamento de privilégios também deve seguir o princípio do menor privilégio (*Least Privilege*), segundo o qual cada usuário recebe apenas as permissões estritamente necessárias ao desempenho de suas atividades. Essa estratégia reduz significativamente os impactos decorrentes do comprometimento de contas e limita a movimentação lateral de atacantes dentro da infraestrutura corporativa.

Nos últimos anos, modelos tradicionais de autenticação passaram a incorporar princípios associados à autenticação adaptativa. Em vez de considerar apenas usuário e senha, esses mecanismos analisam fatores contextuais como localização geográfica, horário de acesso, dispositivo utilizado, endereço IP, comportamento histórico e características da conexão. Sempre que padrões incomuns são identificados, mecanismos adicionais de autenticação podem ser exigidos automaticamente antes da concessão do acesso.

Essa abordagem encontra forte alinhamento com os princípios do modelo Zero Trust, no qual a identidade deixa de ser validada apenas no momento inicial da autenticação e passa a ser continuamente reavaliada durante toda a interação entre usuário e sistema. Assim, alterações comportamentais relevantes podem resultar em bloqueio preventivo, renovação das credenciais ou solicitação de novos fatores de autenticação.

Além dos aspectos tecnológicos, a gestão de identidade também envolve componentes organizacionais relacionados à governança de acesso. Políticas claras de criação, revisão periódica e revogação de permissões contribuem para reduzir contas órfãs, acessos indevidos e inconsistências decorrentes da movimentação de colaboradores entre diferentes funções dentro da organização.

Dessa forma, observa-se que o gerenciamento de identidade representa uma camada estratégica da segurança de aplicações móveis. Sua efetividade depende da integração entre autenticação robusta, gerenciamento centralizado de credenciais, monitoramento contínuo do comportamento dos usuários e políticas de governança capazes de acompanhar a dinâmica operacional das organizações contemporâneas. Esses mecanismos, quando implementados de forma integrada, fortalecem significativamente a proteção dos ativos digitais e reduzem a exposição das organizações às principais ameaças relacionadas ao comprometimento de credenciais.

7 MONITORAMENTO CONTÍNUO, RESPOSTA A INCIDENTES E GOVERNANÇA DA SEGURANÇA MÓVEL

A adoção de mecanismos preventivos representa apenas uma das dimensões da segurança da informação. Em ambientes corporativos caracterizados por elevada conectividade e constante evolução das ameaças digitais, pressupor que controles técnicos serão capazes de impedir todas as

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

tentativas de comprometimento tornou-se incompatível com a realidade operacional das organizações. Nesse contexto, o monitoramento contínuo dos ativos tecnológicos assume papel estratégico na identificação precoce de incidentes e na redução dos impactos decorrentes de ataques cibernéticos.

O conceito contemporâneo de defesa em profundidade pressupõe a utilização integrada de mecanismos preventivos, detectivos e corretivos. Além da implementação de controles de acesso, criptografia e autenticação robusta, torna-se necessário monitorar continuamente o comportamento das aplicações, dos dispositivos e dos usuários, permitindo identificar alterações que possam indicar tentativas de exploração de vulnerabilidades ou comprometimento dos ambientes corporativos.

Entre as tecnologias utilizadas para esse acompanhamento destacam-se as plataformas de *Mobile Device Management* (MDM) e *Enterprise Mobility Management* (EMM). Essas soluções permitem administrar remotamente dispositivos utilizados pela organização, estabelecer políticas de segurança, controlar configurações, restringir funcionalidades incompatíveis com as diretrizes corporativas e aplicar atualizações de maneira centralizada. Em ambientes nos quais coexistem dispositivos institucionais e equipamentos pessoais utilizados em políticas de *Bring Your Own Device* (BYOD), essas ferramentas desempenham papel fundamental na padronização dos requisitos mínimos de segurança.

Além da administração dos dispositivos, o gerenciamento remoto permite executar procedimentos críticos em situações de comprometimento, perda ou furto dos equipamentos. Recursos como bloqueio remoto, revogação de certificados digitais, remoção seletiva de informações corporativas e restauração das configurações de segurança reduzem significativamente o risco de exposição de dados confidenciais.

Outro componente essencial refere-se ao monitoramento dos eventos produzidos pelas próprias aplicações móveis. Registros de autenticação, alterações de configuração, tentativas de acesso não autorizado, modificações de permissões e falhas de comunicação constituem importantes fontes de informação para identificação de atividades suspeitas. Quando devidamente estruturados, esses registros possibilitam reconstruir a sequência dos eventos associados a um incidente e subsidiar processos de investigação forense.

Nesse contexto, plataformas de *Security Information and Event Management* (SIEM) consolidam informações provenientes de diferentes fontes da infraestrutura tecnológica, permitindo correlacionar eventos aparentemente isolados e identificar padrões compatíveis com ataques em andamento. A integração entre aplicações móveis, servidores, dispositivos de rede e serviços em nuvem amplia significativamente a capacidade das equipes de segurança para detectar comportamentos anômalos antes que produzam impactos relevantes sobre as operações organizacionais.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

Nos últimos anos, técnicas baseadas em inteligência artificial e aprendizado de máquina passaram a complementar essas plataformas por meio da análise comportamental de usuários e dispositivos. Modelos conhecidos como *User and Entity Behavior Analytics* (UEBA) permitem estabelecer perfis de utilização considerados normais para cada usuário ou equipamento, identificando automaticamente desvios significativos relacionados ao horário de acesso, localização geográfica, volume de transações ou padrão de utilização dos recursos corporativos.

Embora essas tecnologias não substituam a análise realizada pelas equipes de segurança, sua utilização reduz o tempo necessário para identificação de comportamentos potencialmente maliciosos e contribui para priorizar eventos que exigem investigação imediata. Dessa forma, amplia-se a capacidade das organizações de responder rapidamente a incidentes e minimizar seus impactos operacionais.

Outro aspecto frequentemente negligenciado refere-se ao gerenciamento das atualizações de software. Vulnerabilidades recentemente descobertas tornam indispensável a distribuição rápida de correções para aplicações móveis e sistemas operacionais. Processos automatizados de atualização *Over-the-Air* (OTA) permitem disponibilizar novas versões das aplicações de maneira centralizada, garantindo que dispositivos permaneçam protegidos contra falhas já conhecidas e reduzindo a permanência de versões vulneráveis em operação.

Paralelamente às atividades de monitoramento, organizações devem estabelecer planos formais de resposta a incidentes compatíveis com suas características operacionais. Esses planos definem responsabilidades, procedimentos de comunicação, critérios para classificação dos incidentes, mecanismos de contenção, recuperação dos serviços e análise das causas responsáveis pelos eventos identificados. A existência de processos estruturados reduz o tempo de resposta, minimiza prejuízos operacionais e favorece o aprendizado institucional decorrente dos incidentes ocorridos.

Também merece destaque a realização periódica de testes de intrusão, exercícios de simulação e avaliações de maturidade em segurança da informação. Essas iniciativas permitem validar a eficácia dos controles implementados, identificar vulnerabilidades ainda não exploradas e aperfeiçoar continuamente os processos organizacionais relacionados à proteção das aplicações móveis.

Sob a perspectiva da governança corporativa, o monitoramento contínuo deve ser compreendido como atividade permanente e integrada às estratégias institucionais. A evolução constante das ameaças digitais exige atualização frequente das políticas de segurança, revisão dos mecanismos de controle, capacitação dos profissionais e acompanhamento sistemático dos indicadores relacionados à proteção dos ativos tecnológicos.

Observa-se, portanto, que a segurança das aplicações móveis não depende exclusivamente da adoção de tecnologias avançadas, mas da capacidade das organizações de estabelecer processos contínuos de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

monitoramento, resposta a incidentes e melhoria permanente. A integração entre ferramentas tecnológicas, governança, processos e pessoas constitui elemento determinante para o fortalecimento da resiliência cibernética em ecossistemas empresariais cada vez mais distribuídos e interconectados.

CONCLUSÃO

A crescente utilização de aplicações móveis modificou de forma significativa a dinâmica operacional das organizações, ampliando a disponibilidade dos sistemas corporativos e favorecendo modelos de trabalho cada vez mais flexíveis. Ao mesmo tempo, essa transformação aumentou a complexidade dos ambientes tecnológicos e ampliou a superfície de exposição a ameaças cibernéticas, tornando a segurança da informação um requisito estratégico para o desenvolvimento e a operação dessas aplicações.

A revisão da literatura demonstrou que a proteção dos ecossistemas móveis exige abordagem multidimensional, envolvendo arquitetura segura de software, criptografia, gerenciamento de identidade, proteção das interfaces de comunicação, monitoramento contínuo e governança da segurança da informação. Esses elementos atuam de forma complementar e devem ser incorporados desde as fases iniciais do desenvolvimento das aplicações, reduzindo vulnerabilidades estruturais e aumentando a capacidade de resposta diante de incidentes de segurança.

Também se verificou que modelos tradicionais de proteção baseados exclusivamente no perímetro da rede corporativa deixaram de atender às necessidades impostas pela mobilidade empresarial. A utilização de dispositivos distribuídos, serviços em nuvem e ambientes híbridos exige mecanismos de autenticação contínua, validação contextual dos acessos e aplicação dos princípios associados ao modelo Zero Trust, no qual usuários, dispositivos e conexões são permanentemente avaliados antes da concessão ou manutenção dos privilégios de acesso.

Outro aspecto relevante identificado durante o estudo refere-se à crescente importância da integração entre desenvolvimento de software e segurança da informação. Práticas como Secure by Design, Secure Software Development Lifecycle, DevSecOps e gestão da cadeia de suprimentos de software demonstram que a prevenção de vulnerabilidades deve ocorrer durante todo o ciclo de desenvolvimento, reduzindo custos de manutenção e aumentando a confiabilidade das aplicações corporativas.

Os resultados também evidenciam que o monitoramento contínuo desempenha papel fundamental na proteção dos ambientes móveis. Plataformas de gerenciamento de dispositivos, sistemas de correlação de eventos, análises comportamentais baseadas em inteligência artificial e processos estruturados de resposta a incidentes ampliam significativamente a capacidade das organizações de identificar

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

atividades suspeitas, conter ataques em seus estágios iniciais e reduzir impactos operacionais decorrentes de eventos de segurança.

Entretanto, a efetividade dessas estratégias depende igualmente de fatores organizacionais. A definição de políticas de governança, a atualização permanente dos controles tecnológicos, a qualificação dos profissionais e a conscientização dos usuários permanecem como componentes indispensáveis para o fortalecimento da segurança corporativa. A tecnologia, por si só, não elimina riscos quando não está acompanhada de processos consistentes e cultura organizacional voltada à proteção das informações.

Diante das evidências apresentadas, conclui-se que a convergência entre desenvolvimento de aplicações móveis e cibersegurança constitui elemento essencial para a sustentabilidade dos ecossistemas empresariais contemporâneos. A incorporação sistemática de requisitos de segurança ao longo de todo o ciclo de vida das aplicações contribui para reduzir vulnerabilidades, fortalecer a confiança dos usuários, assegurar conformidade com requisitos regulatórios e preservar a continuidade das operações organizacionais em um cenário caracterizado pela constante evolução das ameaças digitais.

Como perspectiva para pesquisas futuras, recomenda-se a realização de estudos empíricos envolvendo organizações de diferentes segmentos econômicos, com o objetivo de avaliar os impactos da adoção de arquiteturas Zero Trust, práticas de DevSecOps, autenticação sem senha (*passwordless authentication*) e algoritmos criptográficos pós-quânticos na segurança das aplicações móveis corporativas. Investigações dessa natureza poderão ampliar o conhecimento científico sobre a efetividade dessas abordagens em ambientes organizacionais reais.

REFERÊNCIAS

ASSOCIATION FOR COMPUTING MACHINERY (ACM). *ACM Digital Library*. New York, 2024.

FIDO ALLIANCE. *FIDO2: Moving the World Beyond Passwords*. Mountain View, 2024.

GIL, Antonio Carlos. *Métodos e Técnicas de Pesquisa Social*. 7. ed. São Paulo: Atlas, 2019.

KATZ, Jonathan; LINDELL, Yehuda. *Introduction to Modern Cryptography*. 3. ed. Boca Raton: CRC Press, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Cybersecurity Framework 2.0*. Gaithersburg, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Secure Software Development Framework (SSDF): SP 800-218*. Gaithersburg, 2022.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP). *Mobile Application Security Testing Guide (MASTG)*. 2024.

PRESSMAN, Roger S.; MAXIM, Bruce R. *Software Engineering: A Practitioner's Approach*. 9. ed. New York: McGraw-Hill, 2020.

SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your*

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 04/05/2026 | aceito: 07/05/2026 | publicação: 10/05/2026

World. New York: W. W. Norton, 2015.
STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 8. ed. Pearson, 2023.
TANENBAUM, Andrew S.; WETHERALL, David J. *Computer Networks*. 6. ed. Pearson, 2021.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.