DESAFIOS DE SEGURANÇA NO DESENVOLVIMENTO DE APLICATIVOS: SOLUÇÕES TÉCNICAS E PREVENTIVAS

Antônio Lopes de Freitas Neto[1], Gabriel do Nascimento[2], Isabella Caetano Spier[3], Lucas Gabriel Novak[4]

RESUMO

O artigo investiga os desafios de segurança no desenvolvimento de aplicativos móveis, com o objetivo de analisar os riscos e apresentar soluções técnicas e preventivas. A metodologia consiste na análise de literatura especializada, abordando as principais vulnerabilidades listadas pela OWASP, os diferentes modelos de segurança dos sistemas Android e iOS e os princípios da Lei Geral de Proteção de Dados (LGPD). Como resultados, o estudo identifica ameaças críticas como o uso indevido de credenciais e a comunicação insegura, analisa casos de falhas de segurança de grande repercussão e apresenta ferramentas para análise de segurança. Conclui-se que a proteção de dados no ecossistema móvel exige uma cultura de segurança proativa, recomendando-se a adoção de um checklist de segurança e o uso de ferramentas de análise para desenvolver aplicações resilientes, garantindo a integridade e a privacidade dos dados do usuário.

Palavras-chave: Desenvolvimento mobile; Segurança da informação; Vulnerabilidades; Android; iOS; LGPD.

ABSTRACT

The article investigates the security challenges in the development of mobile application, aiming to analyze risks and present technical and preventive solutions. The methodology consists of analyzing specialized literature, addressing the main vulnerabilities listed by OWASP, the different security models of the Android and iOS operating systems and the principles of the General Data Protection Law (LGPD). In conclusion the study identifies

[1]Análise e Desenvolvimento de Sistemas - Universidade Tuiuti do Paraná - antonio.neto3@utp.edu.br
[2]Análise e Desenvolvimento de Sistemas - Universidade Tuiuti do Paraná - gabriel.nascimento@utp.edu.br
[3]Análise e Desenvolvimento de Sistemas - Universidade Tuiuti do Paraná - isabella.spier@utp.edu.br
[4]Análise e Desenvolvimento de Sistemas - Universidade Tuiuti do Paraná - lucas.novak@utp.edu.br

critical threats such as improper credential usage and insecure communication, analyzes high-profile security failure cases and presents tools for security analysis. It is concluded that data protection in the mobile ecosystem requires a proactive security culture, recommending the adoption of a security checklist and the use of analysis tools to develop resilient applications, ensuring the integrity and privacy of user data.

Keywords: Mobile development; Information security; Vulnerabilities; Android; iOS; LGPD.

1 INTRODUÇÃO

Com o crescimento exponencial do uso de aplicativos móveis para atividades sensíveis como transações financeiras, troca de mensagens e armazenamento de dados pessoais, a segurança tornou-se um fator crítico no desenvolvimento mobile.

Segundo os dados mais recentes de Ceci (2025) foram gastos aproximadamente 40 bilhões de dólares na Apple App Store e na Google Play Store no primeiro trimestre de 2025, o que representa um aumento de 11% em comparação com o mesmo semestre de 2024, desconsiderando aplicativos móveis de jogos.

Vulnerabilidades comuns, má configuração de permissões e práticas inseguras de programação podem comprometer seriamente a privacidade e a integridade dos dados dos usuários. Este estudo propõe uma investigação sobre os principais riscos de segurança no desenvolvimento mobile e as boas práticas para mitigá-los.

2 PRINCIPAIS VULNERABILIDADES EM APPS

De acordo com Chekuri (2024) existem mais de 6,8 bilhões de usuários de smartphones em todo o mundo. O autor também informa que aplicativos móveis representam 70% das interações digitais. Somente em 2023, vulnerabilidades em aplicativos móveis contribuíram para aproximadamente 40% das violações de dados envolvendo dados pessoais.

Chekuri (2024) apresenta a lista OWASP Mobile Top 10 de 2024 para identificar e analisar de forma aprofundada as ameaças mais urgentes à segurança móvel. A seguir apresentam-se as 5 principais vulnerabilidades e suas soluções, conforme listado pela OWASP

2.1. USO INDEVIDO DE CREDENCIAIS

Chekuri (2024) apresenta a vulnerabilidade como a “manipulação ou armazenamento inadequado de credenciais do usuário” que conduzem a acessos não autorizados ou vazamentos de credenciais. Para mitigar a exploração desta vulnerabilidade o autor recomenda que os programadores evitem incorporar credenciais em seus códigos, bem como a autenticação de usuários utilizando tokens de acesso seguros e revogáveis.

2.2. SEGURANÇA INADEQUADA NA CADEIA DE SUPRIMENTOS

São fragilidades em componentes ou bibliotecas de terceiros que introduzem vulnerabilidades no aplicativo (Chekuri, 2024). O uso de bibliotecas ou componentes de terceiros verificados e confiáveis é fundamental para mitigar esta vulnerabilidade.

2.3. AUTENTICAÇÃO/AUTORIZAÇÃO INSEGURA

Consiste em falhas nos processos de verificação de identidade que usuários não autorizados podem explorar para acessar funções sensíveis. Chekuri (2024) sugere evitar métodos de autenticação falsificáveis, citando como exemplo os identificadores (Ids) de dispositivos ou geolocalização.

2.4. VALIDAÇÃO DE ENTRADA/SAÍDA INSUFICIENTE

A falha ao validar ou sanitizar corretamente as entradas/saídas do usuário pode levar a ataques de injeção (Chekuri, 2024). O autor recomenda utilizar técnicas de validação rigorosas e sanitização adequada dos dados de saída para evitar ataques.

2.5. COMUNICAÇÃO INSEGURA

O uso de canais de comunicação não criptografados ou até mesmo mal configurados expõe os dados do sistema à interceptação. Para Chekuri (2024) é preciso desautorizar o uso de certificados inválidos, destacando os certificados auto assinados, expirados, os de raiz não confiável, os revogados ou gerados por hosts incompatíveis.

3 BOAS PRÁTICAS DE SEGURANÇA

A crescente popularização dos dispositivos móveis e a sua ampla utilização em atividades pessoais e profissionais intensificaram a necessidade de práticas seguras no desenvolvimento de aplicativos.

O sistema Android, por sua natureza aberta e dominante no mercado global, tornou-se um alvo atrativo para ameaças cibernéticas, exigindo dos desenvolvedores uma postura proativa em relação à segurança (Medeiros & Barbosa, 2014).

3.1. BOAS PRÁTICAS DE SEGURANÇA NO ANDROID

3.1.1. Uso Racional de Permissões

Uma prática essencial é a limitação consciente das permissões solicitadas pelos aplicativos. Aplicações que requerem mais permissões do que o necessário se tornam vetores potenciais para abusos e ataques. Um exemplo notório foi o caso de clones maliciosos do jogo Flappy Bird, que solicitavam acesso a SMS e dados sensíveis do usuário, características ausentes na versão original (Medeiros & Barbosa, 2014).

3.1.2. Isolamento e Controle de Acesso

O Android implementa controle de acesso baseado em sandboxing, no qual cada aplicativo é executado com um identificador de usuário (UID) exclusivo. Isso impede o acesso direto de um aplicativo aos dados de outro, garantindo isolamento no nível do kernel.

A aplicação do SELinux, que “foi desenvolvido pela Agência de Segurança Americana, NSA”, implementa políticas de segurança obrigatórias baseadas em rotulagens e regras (Medeiros & Barbosa, 2014, p. 23).

3.1.3. Assinatura e Identificação de Aplicativos

Cada aplicativo Android deve ser assinado digitalmente com uma chave privada do desenvolvedor. Essa assinatura permite a verificação da autoria e possibilita o compartilhamento seguro de permissões entre aplicativos com a mesma assinatura. Essa prática

é fundamental para prevenir alterações maliciosas e assegurar a integridade do software (Medeiros & Barbosa, 2014).

3.1.4. Verificação e Monitoramento de Aplicativos

Ferramentas como o *Verify Apps* e o *Bouncer* verificam automaticamente aplicativos em busca de comportamentos suspeitos. Enquanto o *Bouncer* atua no ambiente da Google Play, o *Verify Apps* examina aplicativos localmente antes da instalação. Medeiros e Barbosa (2014) destacam a importância de estender essa verificação para o tempo de execução, aumentando a eficácia da detecção de ameaças.

3.1.5. Atualizações e Patches de Segurança

A fragmentação do Android dificulta a distribuição rápida de atualizações de segurança. Medeiros e Barbosa (2014, p. 34) defendem que o ideal seria a Google "desenvolvesse um método que possibilitasse enviar as atualizações de segurança diretamente para os usuários, sem ter que depender das fabricantes, pois isso tornaria muito mais rápida a distribuição das correções".

3.1.6. Perfis Isolados para Uso Corporativos

No contexto de ambientes corporativos com políticas de BYOD (*Bring Your Own Device*), a criação de perfis isolados — um pessoal e outro profissional — seria uma medida eficaz para proteger dados empresariais sem comprometer a privacidade do usuário. Essa separação permitiria monitoramento seletivo e maior controle sobre o uso dos recursos corporativos (Medeiros & Barbosa, 2014).

3.2. BOAS PRÁTICAS DE SEGURNÇA NO IOS

3.2.1. Modelo Fechado e Controle Centralizado

Diferentemente do Android, o iOS adota uma arquitetura fechada com forte centralização pela Apple. Aplicativos só podem ser instalados via App Store, que impõe um

rigoroso processo de aprovação, reduzindo significativamente o risco de distribuição de aplicativos maliciosos (Medeiros & Barbosa, 2014).

3.2.2. Atualizações de Segurança Imediatas

O iOS possui vantagem na distribuição de atualizações de segurança, pois a Apple é responsável direta pela liberação das atualizações, sem depender de terceiros. Isso garante uma resposta mais rápida a vulnerabilidades críticas, ao contrário do Android, onde o atraso das fabricantes compromete a eficácia das correções (Medeiros & Barbosa, 2014).

3.2.3. Ferramentas nativas para o Ambiente Corporativo

No ambiente empresarial, o iOS também se sobressai por oferecer ferramentas nativas de gerenciamento de dispositivos, que permitem às organizações aplicar restrições e monitoramento de forma eficaz. Essa capacidade de controle reforça a adoção do iOS em políticas corporativas de mobilidade (Medeiros & Barbosa, 2014).

4 PERMISSÕES DE APPS E PRIVACIDADE DO USUÁRIO

Historicamente o Android anterior a versão concedia todas as permissões que um aplicativo solicitava no momento da instalação. Segundo Medeiros & Barbosa (2014) e corroborado por Mueller *et al* (2023) no momento da instalação era obrigatório a autorização de todas as permissões exigidas pelo aplicativo ou o cancelamento da instalação. Isso mudou a partir da versão 23 da API, que passou a exigir a permissão no momento da utilização do recurso de forma explicita (*runtime permissions*).

Na versão de API 26 do Android 8.0 as permissões solicitadas durante a execução são apenas para o recurso solicitado, mas uma vez autorizado o sistema não apresentará mais a caixa de diálogo ao usuário (Mueller *et al*, 2023).

Na versão de API 29 do Android 10 surgiu a opção de permitir acesso à localização “somente enquanto usa o aplicativo”. Para isso o aplicativo precisa estar em primeiro plano. Nesta mesma versão as permissões de armazenamento foram modificadas para permitir ao aplicativo o poder de leitura e escrita irrestrito apenas em sua pasta específica no armazenamento externo, exigindo as permissões do usuário apenas nos momentos de acesso a arquivos compartilhados (Mueller *et al*, 2023)

Na API versão 30 do Android 11 surgiu a redefinição automática de permissões, que remove permissões concedidas para aplicativos sem uso por um longo período. Na versão 31 da API do Android 12 surgiu o Painel de privacidade, que informa as permissões utilizadas pelos aplicativos nos últimos 7 dias. (Mueller *et al*, 2023).

Por sua vez o sistema operacional do iOS solicita ao usuário as permissões em tempo de execução na primeira tentativa de uso de uma API sensível desde a sua concepção. As permissões concedidas são listadas no menu de ajuste de privacidade, permitindo ao usuário a revisão e modificação qualquer momento (Mueller *et al*, 2023).

Outros recursos como o *UIImagePickerController* (iOS 11+) e seu sucessor *PHPickerViewController* (iOS 14+) autorizam o acesso a imagens em formato "somente leitura" par as imagens selecionadas no lugar de solicitar acesso a todo rolo de câmera do usuário, o que Mueller *et al* (2023) classificam como uma boa prática.

4.1. LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

Conforme Chekuri (2024) o gerenciamento inadequado das credenciais de privacidade e permissões podem ter impactos severos para indivíduos e corporações.

A Lei Geral de Proteção de Dados (LGPD) no Brasil busca proteger os direitos fundamentais de liberdade e privacidade dos indivíduos. Neste sentido o Comitê Central de Governança de Dados (2020) elaborou o Guia de boas práticas da LGPD na administração pública, mas que desenvolvedores de aplicativos móveis devem obedecer para não infringir a lei.

O Comitê Central de Governança de Dados (2020) apresenta o Princípio da Finalidade, em que o tratamento dos dados do titular deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular. No Princípio da Segurança o agente de tratamento de dados, leia-se o desenvolver, deve utilizar medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

O princípio da necessidade estabelece a limitação do tratamento ao mínimo necessário para a realização das finalidades, abrangendo dados pertinentes, proporcionais e não excessivos. (Comitê Central de Governança de Dados, 2020). Este entendimento é corroborado por Mueller *et al* (2023), que argumentam que os aplicativos devem solicitar apenas as permissões que são absolutamente essenciais para a funcionalidade proposta.

No princípio da transparência a LGPD garante aos titulares o “a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de Tratamento” (Comitê Central de Governança de Dados, 2020, p. 15). Mueller *et al* (2023) apresenta a criação das chaves de descrição de propósito (*purpose strings*) na versão 10.0.0 do iOS, em que a tentativa de acessar dados protegidos sem que o desenvolvedor forneça esta chave de finalidade resulta em falha de acesso. A existência e o preenchimento destas chaves é uma forma de atender a LGPD.

5 CASOS REAIS DE FALHAS DE SEGURANÇA EM APPS POPULARES

Segundo matéria do G1, foi revelada falhas na segurança do aplicativo para os Jogos Olímpicos de Inverno que aconteceram em Pequim, no ano de 2022. De acordo com a matéria,

> “atletas, jornalistas e dirigentes esportivos estão potencialmente expostos a sérios perigos. Sua privacidade pode ser desrespeitada e seus dados não são protegidos contra roubo e vigilância. Além disso, os especialistas em informática forense encontraram uma lista de censura no aplicativo”. (Mannteufel & Linow, 2022)

Segundo o Portal, foi solicitado para que os atletas instalassem o aplicativo oficial 2022 em seus smartphones.

> “Entretanto, os dados são mal criptografados pelo aplicativo, o que pode deixar atletas olímpicos, jornalistas e dirigentes esportivos vulneráveis a hackers, a violações de privacidade e violações de dados, conforme aponta um relatório do laboratório interdisciplinar Citizen Lab, da Universidade de Toronto, recebido pela Deutsche Welle.” (Mannteufel & Linow, 2022)

Ainda segundo a matéria (Mannteufel & Linow, 2022):

> “Essa vulnerabilidade foi encontrada por Jeffrey Knockel, do Citizen Lab, não só no que diz respeito aos dados de saúde, mas também em outros serviços importantes oferecidos no aplicativo, como o processamento dos anexos de arquivos e as mensagens de voz. Além disso, o especialista em TI também descobriu que, para alguns serviços, o tráfego de dados no aplicativo não é de forma alguma criptografado. Isso significa que os metadados do próprio serviço de bate-papo do aplicativo podem ser lidos muito facilmente por um espião.”

Outro caso que veio a pública foi de um ataque hacker ao aplicativo Uber. De acordo com notícia veiculada pelo Portal Incuca por Stefanello (2025):

> “A Uber admitiu ser alvo de um ataque hacker em 2016, que resultou no roubo de dados de 57 milhões de motoristas e clientes em todo o mundo. A empresa não revelou inicialmente o incidente e tentou manter o assunto em sigilo, pagando US$ 100 mil aos hackers responsáveis. Os invasores obtiveram endereços de e-mail e números de celular, com 600 mil motoristas tendo seus dados de licença expostos nos Estados Unidos.”

Outro caso que veio a público foi da empresa Netshoes.

> “O site de comércio eletrônico Netshoes foi afetado por um vazamento de dados de quase dois milhões de clientes no ano de 2018. O incidente comprometeu informações pessoais, como nome, CPF, e-mail, data de nascimento e histórico de compras dos clientes.” (Stefanello, 2025)

A mesma fonte complementa.

> “Como resultado, o Netshoes foi obrigado a pagar R$ 500 mil em indenização por danos morais. Embora informações sensíveis, como detalhes de cartão de crédito ou senhas de clientes, não tenham sido divulgadas, o vazamento deixou os clientes vulneráveis a várias formas de fraudes.” (Stefanello, 2025)

6 FERRAMENTAS E TÉCNICAS DE ANÁLISE DE SEGURANÇA MOBILE

De acordo com o Instituto Brasileiro de Cibersegurança (2024), existem algumas ferramentas e práticas essenciais de segurança em aplicativos Android e Web.

Alguns dessas fermentas são: o Jadx, para descompilação de aplicativos Android, permitindo a análise do código-fonte e identificação de vulnerabilidades. Já o Apktool é utilizado para decompilar e recompilar arquivos APK, o que é essencial para a análise de aplicativos Android e modificação de pacotes. O Android Studio por sua vez é o “Ambiente de desenvolvimento integrado (IDE) oficial para Android, utilizado para testes e desenvolvimento de aplicativos seguros.” (Instituto Brasileiro de Cibersegurança, 2024)

Já segundo o Portal WeLiveSecurity (González, 2023):

> “a APKLab é uma ferramenta projetada para o Virtual Studio Code que integra outras ferramentas, tais como Quark-Engine, APKtool, JADX, entre outras. Ela facilita a análise devido a sua interface integrada, da qual é possível renomear várias classes, funções e variáveis. Além disso, com o APKLab é possível facilmente "construir" o .apk novamente com as modificações dentro do arquivo para facilitar a análise de um malware específico.”

Uma prática comum de cibercriminosos é ofuscar o código do malware, mas aplicações como o APKLab permitem ao analista cruzar e renomear classes e métodos. (González, 2023)

Ainda segundo Instituto Brasileiro de Cibersegurança (2024) existem diversas ferramentas de segurança para dispositivos móveis. Algumas delas são o Bitdefender Mobile Security Free, que “oferece proteção básica contra malware, com escaneamento automático e manual de arquivos, além de verificar o armazenamento removível.”

O Avast Mobile Security proporciona “segurança em tempo real, proteção contra ransomware e análise de redes Wi-Fi.” (Instituto Brasileiro de Cibersegurança, 2024). O Malwarebytes Mobile Security é focado na “remoção de adware e malware, proteção contra ransomware e alertas de phishing.” (Instituto Brasileiro de Cibersegurança, 2024). Por sua vez o Sophos Intercept X for Mobile protege contra malware, ransomware e aplicativos maliciosos, e oferece proteção anti-phishing. (Instituto Brasileiro de Cibersegurança, 2024)

Para o Blog TD Synnex (2025) uma das ferramentas de segurança para dispositivos móveis é ativar a autenticação de dois fatores:

> “O processo de proteção de camada dupla é mais conhecido como autenticação de dois fatores e basicamente significa que para acessar suas principais contas como

> Google ou Dropbox, uma série de serviços financeiros e até mesmo apps de gerenciamento de senhas como o que citamos acima, você precisará tanto de um password regular quanto um password secundário gerado por um código de um dispositivo que apenas você tem acesso. Com a combinação dessas duas "chaves", as chances de alguém indesejado invadir seu e-mail ou sua conta bancária são bem pequenas."

Outra hipótese é utilizar um aplicativo de gerenciamento de senhas:

> "Uma ferramenta interessante para resolver esse problema é o LastPass. O app simplifica a geração e o armazenamento de senhas mais fortes para cada site que você se cadastra. Inclusive ele preenche automaticamente as senhas em cada aplicativo ou site que você acessa, e faz o mesmo no seu tablet, desktop ou notebook. O programa usa criptografia avançada para manter suas informações seguras. Tudo o que você precisa é lembrar uma única senha segura para desbloquear uma sessão inicial do app." (TD Synnex, 2025)

7 CHECKLIST DE SEGURANÇA PARA DESENVOLVEDORES

Para mitigar os riscos das 5 maiores vulnerabilidades apresentados conforme Chekuri (2024) um checklist de segurança para desenvolvedores deve exigir uma resposta afirmativa para os seguintes elementos e práticas.

7.1. USO DE CREDENCIAIS

- O código da aplicação está completamente livre de credenciais, chaves de API ou outros segredos incorporados (hardcoded)?
- A autenticação dos usuários é realizada por meio de tokens de acesso que são seguros e podem ser revogados?
- A geração e armazenamento de senhas de acesso é feita por aplicativo dedicado?
- O aplicativo de gerenciamento de senhas escolhido utiliza criptografia?

7.2. SEGURANÇA NA CADEIA DE SUPRIMENTOS

- As bibliotecas utilizadas são verificadas regularmente por ferramenta dedicada?
- A confiabilidade dos componentes de terceiros é auditada?

7.3. AUTENTICAÇÃO/AUTORIZAÇÃO

- A aplicação utiliza autenticação de dois fatores para proteger o acesso a contas e funcionalidades críticas?

- Foram evitados métodos de autenticação facilmente falsificáveis, como o uso de geolocalização ou IDs de dispositivo?

7.4. VALIDAÇÃO DE ENTRADA/SAÍDA

- São utilizadas técnicas de validação para todas as entradas de dados para prevenir ataques de injeção?
- É realizada a sanitização adequada de todos os dados de saída do aplicativo?

7.5. COMUNICAÇÃO

- A comunicação está tráfego de dados da aplicação é obrigatoriamente criptografado para protegê-lo contra interceptação?
- O sistema desautoriza o uso de certificações autoassinadas, expiradas, de raiz não confiável, revogadas ou geradas por hosts incompatíveis?

8 CONCLUSÃO

A análise aprofundada dos desafios de segurança no desenvolvimento de aplicativos móveis revela que a proteção de dados e a privacidade do usuário são pilares indispensáveis no ecossistema digital contemporâneo.

O crescimento exponencial do uso de aplicações para atividades sensíveis, como transações financeiras, torna a segurança um fator crítico. As vulnerabilidades detalhadas pela OWASP, como o uso indevido de credenciais, comunicação insegura e falhas na cadeia de suprimentos, constituem ameaças recorrentes que exigem uma postura proativa dos desenvolvedores.

Apesar das abordagens distintas dos sistemas operacionais Android e iOS, ambos se fundamentam em princípios de segurança essenciais, como isolamento de aplicações e gerenciamento de permissões.

A evolução do modelo de permissões, especialmente no Android, e a conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) reforçam a necessidade de um desenvolvimento pautado pela transparência, finalidade e necessidade.

Os casos reais de falhas de segurança em aplicativos como os dos Jogos Olímpicos de Pequim, Uber e Netshoes servem como um alerta sobre as consequências tangíveis da negligência, que vão desde perdas financeiras a danos irreparáveis à confiança do usuário.

Neste sentido recomenda-se adotar um checklist de segurança abrangente, aliada à utilização de ferramentas de análise de segurança como Jadx ou Apktool para o desenvolvimento de aplicativos móveis mais resilientes. A mitigação eficaz dos riscos não depende apenas da aplicação de ferramentas, mas da adoção de uma cultura de segurança em todo o ciclo de vida do desenvolvimento do aplicativo.

A segurança móvel representa um compromisso contínuo com a integridade, a confidencialidade e a privacidade dos dados, elementos fundamentais para a sustentabilidade e a confiança no ambiente digital.

REFERÊNCIAS

CECI, L. **Combined global Apple App Store and Google Play app consumer spending from 2nd quarter 2023 to 1st quarter 2025 (in billion U.S. dollars).** Publicado em 19 jun. 2025. Disponível em: <https://www.statista.com/statistics/1489711/total-global-app-spending/>. Acesso em: 1 jul. 2025.

CHEKURI. L. **OWASP Mobile Top 10 Vulnerabilities [2024 Updated]**. Publicado em 10 dez. 2024. Disponível em: <https://strobes.co/blog/owasp-mobile-top-10-vulnerabilities-2024-updated/>. Acesso em: 31 mai. 2025.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Guia de boas práticas lei geral de proteção de dados (LGPD): Guia de boas práticas para implementação na administração pública federal.** 2. ed. Brasília, DF, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em:

GONZÁLEZ, S. **6 ferramentas úteis para análise de malware no Android**. Publicado em 19 jan. 2023. Disponível em: < https://www.welivesecurity.com/br/2023/01/19/6-ferramentas-uteis-para-analise-de-malware-no-android/>. Acesso em: 1 jul. 2025

INSTITUTO BRASILEIRO DE CIBERSEGURANÇA. **10 Ferramentas E Práticas Essenciais Para Análise De Segurança Em Aplicativos Android E Web**. In: BLOG IBSEC. São Paulo: IBSEC, 28 jun. 2024. Disponível em: < https://ibsec.com.br/10-ferramentas-seguranca-em-aplicativos-android-e-web/>. Acesso em: 1 jul. 2025.

MANNTEUFEL, I.; LINOW, O. **Relatório revela falhas de segurança do app dos Jogos de Pequim**. G1, Rio de Janeiro, 18 jan. 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/01/18/relatorio-revela-falhas-de-seguranca-do-app-dos-jogos-de-pequim.ghtml>. Acesso em: 1 jul. 2025

MEDEIROS, A. L. S.; BARBOSA, L. H. L. **Análise de segurança na plataforma Android**. Rio de Janeiro: Instituto Militar de Engenharia, 2014. 47 p. Iniciação à Pesquisa (Graduação em Engenharia de Computação) – Instituto Militar de Engenharia. Disponível em: < http://www.defesacibernetica.ime.eb.br/pub/repositorio/2014-Sombra_Helder.pdf>.Acesso em 14 jun. 2025.

MUELLER, B.; HOLGUERA, C; SCHLEIER, S.; GUPTA, V. **Mobile application security testing guide (MASTG)**. 1.7.0 ed. [S.l.]: The OWASP Foundation, 2023. Disponível em: https://mas.owasp.org/MASTG. Acesso em: 1 jul. 2025

STEFANELLO, L. **4 casos de empresas que tiveram falhas de segurança no site**. InCuca Tech, Florianópolis, SC, 30 maio 2025. Disponível em: <https://incuca.net/4-casos-de-empresas-que-tiveram-falhas-na-seguranca-do-site/>. Acesso em: 1 jul. 2025.

TD SYNNEX. **7 ferramentas para garantir a segurança de dispositivos móveis Android**. Disponível em: < https://blog-pt.lac.tdsynnex.com/7-ferramentas-para-garantir-a-seguranca-de-dispositivos-moveis-android>. Acesso em: 1 jul. 2025