ARTIGO

# SEGURANÇA E PRIVACIDADE DE DADOS EM SMARTWATCHES: VULNERABILIDADES E MEDIDAS DE PROTEÇÃO

Murilo Ferrari Angeli

Evelacio Roque Kaufmann

Resumo

Este artigo aborda a segurança em smartwatches, analisando o Apple Watch Series 8 e o Galaxy Watch5 Pro. Com o aumento das preocupações devido à popularidade desses dispositivos, são destacadas vulnerabilidades, como conectividade sem fio, falta de atualizações, coleta de dados e autenticação frágil. Alternativas de proteção são exploradas, como atualizações regulares, autenticação robusta, encriptação de dados, gerenciamento de permissões, proteção contra roubo, autenticação de dois fatores (2FA) e controle de privacidade. O equilíbrio entre conveniência e segurança é enfatizado, ressaltando a importância de proteger os dados dos usuários.

## 1 INTRODUÇÃO

Os smartwatches, como ressaltado por Bandeira (2023), emergem como dispositivos cada vez mais populares, incorporando funcionalidades avançadas e integrando-se ao cotidiano. Contudo, essa ascendente integração tecnológica suscita sérias inquietações acerca da segurança e privacidade dos dados pessoais. Este artigo empreende uma exploração aprofundada das vulnerabilidades vinculadas ao uso de smartwatches, direcionando o foco para modelos proeminentes como o Apple Watch Series 8 e o Galaxy Watch5 Pro, ao mesmo tempo em que propõe estratégias sólidas de proteção.

A análise abordou uma série de vulnerabilidades, destacando desafios como conectividade sem fio suscetível, lacunas na implementação de atualizações de segurança, coleta de dados sensíveis, fragilidades na

autenticação e riscos associados a perdas ou roubos. Nesse contexto, foram delineadas alternativas robustas de proteção, abrangendo desde a implementação regular de atualizações de firmware até iniciativas de educação do usuário, visando assegurar a integridade, confidencialidade e disponibilidade dos dados dos usuários desses dispositivos.

Em consonância com as advertências de Muncaster (2022), torna-se evidente que os cibercriminosos dispõem de diversas táticas para atacar dispositivos vestíveis, desde a interceptação de dados até o desbloqueio de dispositivos perdidos, bem como o compartilhamento não autorizado de dados pessoais. A exposição simultânea a aplicativos de smartphones, comum em smartwatches avançados, amplia o espectro de ameaças, incluindo a possível interceptação de dados confidenciais.

O aprofundamento da consciência acerca dessas ameaças e a implementação diligente de medidas de segurança emergem como elementos cruciais para que os usuários usufruam plenamente dos benefícios oferecidos pelos smartwatches sem comprometer sua segurança pessoal. Este trabalho busca não apenas informar, mas também orientar os usuários, fornecendo insights indispensáveis para um uso seguro desses dispositivos, incentivando a compreensão das ameaças e promovendo a adoção de medidas eficazes de proteção. O equilíbrio delicado entre inovação tecnológica e a salvaguarda dos dados pessoais é, portanto, enfatizado como um aspecto crucial no atual cenário de dispositivos vestíveis.

## 2 **DESENVOLVIMENTO**

Conectividade sem fio: As vulnerabilidades relacionadas à conectividade sem fio, como Wi-Fi e Bluetooth, introduzem riscos substanciais nos smartwatches. A exposição a ataques de interceptação de dados é notável, onde hackers, munidos de conhecimentos técnicos, podem explorar essas conexões para acessar informações confidenciais. Além disso, a comunicação sem fio está sujeita a ataques "man-in-the-middle", nos quais invasores se inserem entre o dispositivo e a rede, possibilitando a captura ou manipulação de dados sensíveis.

Falta de atualizações de segurança: Assim como outros dispositivos eletrônicos, os smartwatches executam sistemas operacionais e aplicativos que podem conter vulnerabilidades conhecidas. A falta de atualizações de segurança oportunas representa uma brecha crítica, deixando os dispositivos vulneráveis a ataques que exploram essas fragilidades. A ausência de correções pode comprometer a integridade do sistema e a privacidade do usuário.

Coleta e armazenamento de dados pessoais: A coleta de dados sobre atividade física, batimentos cardíacos, localização e outros parâmetros de saúde torna-se um ponto sensível. Se essas informações não forem devidamente protegidas, os invasores podem obter insights valiosos sobre a vida do usuário. Dados de saúde, devido à sua natureza sensível, tornam-se alvos atraentes para exploração maliciosa.

Autenticação frágil: A autenticação em smartwatches frequentemente utiliza sensores biométricos, como sensores de frequência cardíaca e reconhecimento de impressão digital. No entanto, esses sistemas não são infalíveis. Hackers podem empregar técnicas de falsificação para contornar a autenticação biométrica, comprometendo assim a segurança do dispositivo e permitindo acesso não autorizado a dados armazenados.

Risco de perda ou roubo: A natureza compacta e portátil dos smartwatches os torna suscetíveis a perdas e roubos. Quando um dispositivo é perdido ou roubado, os dados pessoais armazenados nele ficam expostos a terceiros não autorizados. Isso resulta na violação da privacidade do usuário e na possível exposição de informações confidenciais.

ALTERNATIVAS DE PROTEÇÃO DOS SMARTWATCHES

Atualizações de Firmware Regulares: Conforme destacado por Felix (2021), a implementação de "Atualizações regulares de firmware" é fundamental para a segurança e desempenho contínuo dos smartwatches. Essas atualizações corrigem vulnerabilidades conhecidas, fortalecem a segurança contra ameaças emergentes, aprimoram o desempenho geral e auxiliam na conformidade com regulamentações. Além disso, as atualizações reduzem significativamente o risco de exploração de vulnerabilidades, sendo

também um lembrete crucial para os usuários sobre a importância da segurança cibernética.

Autenticação Robusta: Em consonância com Kaspersky (2023), a "Autenticação Robusta" é essencial. A aplicação de métodos sólidos, como senhas robustas, PINs, reconhecimento de impressões digitais e reconhecimento facial, é crucial para proteger o acesso ao smartwatch. A educação do usuário sobre a importância da segurança de suas credenciais, além da conscientização sobre ameaças, é vital. Medidas como autenticação de dois fatores (2FA) e proteção contra ataques de força bruta adicionam camadas adicionais de segurança, garantindo um equilíbrio entre segurança e usabilidade.

Encriptação de Dados: Conforme ressaltado por Fernandes (2020), a "Encriptação de Dados" é uma salvaguarda essencial. Essa prática é crucial para a segurança dos smartwatches, protegendo informações armazenadas e transmitidas contra acesso não autorizado. A correta implementação, incluindo a escolha de algoritmos de criptografia seguros e a consideração da sensibilidade dos dados, é fundamental para extrair todos os benefícios dessa medida.

Gerenciamento de Permissões: Fernandes (2020) enfatiza a importância do "Gerenciamento de Permissões". Permitir que os usuários controlem quais informações e recursos os aplicativos podem acessar, seguindo o princípio da "menor privacidade", é crucial. Os usuários têm controle total sobre a concessão ou negação de permissões, e a transparência é priorizada, informando por que um aplicativo solicita uma permissão específica. Isso protege contra o acesso não autorizado a informações confidenciais, permite a revisão e modificação das permissões e mantém um equilíbrio entre segurança e usabilidade.

Verificação de Aplicativos: Conforme destaca Felix (2021), a "Verificação de Aplicativos" é essencial para garantir que apenas aplicativos confiáveis sejam instalados em smartwatches. Isso envolve verificações antes da instalação, incluindo revisões de segurança e a promoção de fontes confiáveis, como lojas de aplicativos oficiais. Após a instalação, a detecção

e remoção rápidas de aplicativos maliciosos são vitais. A implementação de assinaturas digitais, avaliação de políticas de privacidade, educação do usuário e auditoria contínua são elementos-chave. A colaboração com desenvolvedores é importante para promover a segurança.

Proteção Contra Roubo e Perda: Kaspersky (2023) destaca a "Proteção Contra Roubo e Perda" como essencial para a segurança de smartwatches, com recursos de rastreamento, bloqueio e apagamento remoto. Isso permite aos usuários localizar o dispositivo, bloqueá-lo e apagar dados sensíveis em caso de perda ou roubo. A autenticação do proprietário é necessária para usar esses recursos, e a recuperação de dados é facilitada pela sincronização em nuvem. É fundamental que os usuários relatem perdas rapidamente. A implementação adequada é crítica para garantir a eficácia dessas medidas de segurança.

Autenticação de Dois Fatores (2FA): Conforme sublinha Fernandes (2020), a "Autenticação de Dois Fatores (2FA)" é uma medida de segurança essencial que protege as contas conectadas a smartwatches, exigindo dois métodos de verificação para confirmar a identidade do usuário. Isso oferece uma camada adicional de proteção além das senhas tradicionais. Incentivar a adoção da 2FA, diversidade de métodos, educação do usuário e integração fácil são fundamentais para sua eficácia. A 2FA é vital para proteger informações pessoais e garantir a segurança das contas conectadas a smartwatches.

Educação do Usuário: Kaspersky (2023) enfatiza a "Educação do Usuário" em smartwatches como crucial para promover boas práticas de segurança. Isso inclui ensinar aos usuários a importância de senhas fortes, reconhecimento de conexões seguras e identificação de links suspeitos. Além disso, a educação abrange a necessidade de manter dispositivos e aplicativos atualizados, instalar aplicativos de fontes confiáveis e revisar permissões. Os usuários também são incentivados a desempenhar um papel ativo na segurança e relatar atividades suspeitas. Recursos de suporte estão disponíveis para ajudar em caso de problemas.

Controle de Privacidade: Segundo Felix (2021), o "Controle de Privacidade" em smartwatches é crucial para proteger a privacidade dos usuários. Isso começa com o consentimento informado, onde os usuários são informados sobre a coleta de dados. Eles também devem ter a capacidade de desativar sensores e controlar permissões de aplicativos, bem como o direito de solicitar a exclusão de seus dados. A anonimização de dados e a transparência nas políticas de privacidade são essenciais. A segurança de dados, a educação do usuário e a conformidade com regulamentações são partes fundamentais desse controle.

Testes de Segurança: Fernandes (2020) enfatiza que os "Testes de Segurança" em smartwatches são cruciais para manter a integridade do sistema e dos aplicativos. Eles identificam vulnerabilidades, garantem atualizações regulares e a conformidade com normas de segurança. Isso inclui proteção da privacidade do usuário, treinamento da equipe de desenvolvimento e comunicação transparente em casos de vulnerabilidades críticas. Além disso, os testes monitoram constantemente ameaças em tempo real, mantendo a segurança do ecossistema. Em resumo, os "Testes de Segurança" são essenciais para prevenir ameaças e proteger os dispositivos dos usuários.

## 3 **CONCLUSÃO**

Neste trabalho foi explorada a crescente popularidade dos smartwatches e sua relevância na vida diária, enquanto também identificando as vulnerabilidades significativas que esses dispositivos apresentam. A conclusão deste estudo destaca a importância de abordar essas vulnerabilidades e fornecer alternativas de proteção para garantir a segurança e a privacidade dos usuários de smartwatches. Durante nossa análise das vulnerabilidades, destacam-se as ameaças relacionadas à conectividade sem fio, a falta de atualizações regulares de segurança, a coleta e o armazenamento de dados sensíveis, autenticação frágil e riscos associados à perda ou roubo. Essas questões exigem atenção e ação para

proteger os usuários contra potenciais violações de segurança e privacidade. Para combater essas vulnerabilidades, foi apresentado um conjunto abrangente de alternativas de proteção. Isso inclui atualizações regulares de firmware, autenticação robusta, encriptação de dados, gerenciamento de permissões, verificação de aplicativos, proteção contra roubo e perda, autenticação de dois fatores (2FA), educação do usuário, controle de privacidade e testes de segurança contínuos. Essas medidas visam fortalecer a segurança dos smartwatches, garantindo que os usuários possam desfrutar de todos os benefícios desses dispositivos sem comprometer sua privacidade e segurança. Em última análise, à medida que a sociedade continua a adotar a tecnologia dos smartwatches, é crucial que fabricantes, desenvolvedores e usuários trabalhem em conjunto para garantir um ambiente seguro e confiável. A proteção eficaz contra vulnerabilidades exige uma abordagem proativa, conscientização e a adoção de práticas recomendadas de segurança. Com essas medidas de proteção implementadas, os smartwatches podem continuar a ser uma adição valiosa à vida diária, sem comprometer a segurança dos usuários.

## REFERÊNCIAS

APPLE. Apple Watch Series 8: Um grande salto para sua saúde. 2022. Disponível em: https://www.apple.com/br/apple-watch-series-8/. Acesso em: 09 jul. 2023.

BANDEIRA, Katarina. O pai do Apple Watch: conheça o primeiro smartwatch do mundo. 2023. Disponível em: https://www.techtudo.com.br/noticias/2023/02/o-pai-do-apple-watch-conheca-o-primeiro-smartwatch-do-mundo-edmobile.ghtml. Acesso em: 3 mar. 2023.

BRASIL. Michel Temer. Presidente da República Secretaria-Geral. Subchefia para Assuntos Jurídicos. LEI Nº 13.709. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 jun. 2023.

CLOUDFLARE. O que é privacidade de dados? Disponível em: https://www.cloudflare.com/pt-br/learning/privacy/what-is-data-privacy/. Acesso em: 04 mar. 2023.

FELIX, Bruno. Wearables: saiba como proteger sua privacidade ao usar smartwatches e fitness trackers. 2021. Disponível em:

https://olhardigital.com.br/2021/01/22/noticias/wearables-saiba-como-proteger-sua-privacidade-ao-usar-smartwatches-e-fitness-trackers/. Acesso em: 05 out. 2023.
KASPERSKY. Segurança do Smartwatch - Segurança e Riscos. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/smartwatch-security-risks. Acesso em: 04 out. 2023.
KUSHMARO, Philip. Por que a privacidade de dados é um direito humano (e o que as empresas devem fazer sobre isso). 2021. Disponível em: https://www.forbes.com/sites/forbescommunicationscouncil/2021/06/07/why-data-privacy-is-a-human-right-and-what-businesses-should-do-about-it/?sh=44d6197b4ec3. Acesso em: 14 fev. 2023.
LURYE, Sergey. Seu relógio pode espionar você? 2018. Disponível em: https://www.kaspersky.com.br/blog/smart-watch-research/10384/. Acesso em: 5 mar. 2023.
MINHACONEXÃO. Smartwatch: como funciona e quais são suas vantagens? 2022 Disponível em: https://www.minhaconexao.com.br/blog/tech/smartwatch. Acesso em: 18 fev. 2023.
NEGREIROS, Marcos. A evolução dos wearables como ferramentas de inclusão e acessibilidade. 2023. Disponível em: https://saude.abril.com.br/coluna/com-a-palavra/a-evolucao-dos-wearables-como-ferramentas-de-inclusao-e-acessibilidade/. Acesso em: 14 mar. 2023.
SAMSUNG. Galaxy Watch5 Pro. 2022. Disponível em: https://www.samsung.com/br/watches/galaxy-watch/galaxy-watch5-pro-black-titanium-bluetooth-sm-r920nzkpzto/. Acesso em: 08 jul. 2023.
TIBAHIA. A EVOLUÇÃO DOS RELÓGIOS INTELIGENTES, O QUE É O SMARTWATCHES. 2021. Disponível em: https://tibahia.com/artigos/a-evolucao-dos-relogios-inteligentes-o-que-e-o-smartwatches/. Acesso em: 11 jun. 2023.

Sobre o(s) autor(es)
Discente do Curso de Ciência da Computação
Unoesc-Campus de São Miguel do Oeste
Rua Oiapoc, 211. São Miguel do Oeste-SC
muriloferrariangeli@gmail.com

Mestre em Administração
Docente do Curso de Ciência da Computação
Unoesc-Campus de São Miguel do Oeste
Rua Oiapoc, 211. São Miguel do Oeste-SC
evelacio.kaufmann@unoesc.edu.br

Imagem 01: Apple Watch Series 8, produzido pela Apple e lançado em 2022.


Fonte: APPLE, 2023

Imagem 02: Galaxy Watch5 Pro, desenvolvido pela Samsung e lançado em 2022


Fonte: SAMSUNG, 2023

Quadro 1: Comparativo entre os modelos de smartwatches

| Critério | Apple *Watch* Series 8 | Galaxy *Watch* 5 Pro |
|---|---|---|
| Sistema Operacional | watchOS (Apple) | Tizen (Samsung) |
| Compatibilidade | IOS (principalmente Iphones) | Android (várias marcas) |
| Design e Tamanhos | Retangular, 40mm e 44mm | Circular, 40mm e 44mm |
| Integração com Ecossistema | Integração profunda com ecossistema Apple | Integração com dispositivos Samsung, menos profunda com Android |
| Recursos de Saúde e Fitness | Monitoramento de batimentos cardíacos, sono, passos e exercícios | Monitoramento de batimentos cardíacos, sono, passos e exercícios |
| Oferece Eletrocardiograma (ECG) e detecção de quedas | Sim | Não |
| Assistentes Virtuais | Siri (Apple) | Bixby (Samsung) |
| Recursos Adicionais | Apple Pay, integração com AirPods | Samsung Pay, integração com fones de ouvido sem fio da Samsung |
| Duração da Bateria | Aproximadamente 1 dia | Geralmente 2 a 4 dias |
| Material e Personalização | Opções de materiais premium e pulseiras personalizadas | Opções de materiais premium, pulseiras personalizadas e designs temáticos |
| Preço e Disponibilidade | Tendência premium, disponibilidade variável | Preços competitivos, ampla disponibilidade |

Fonte: O Autor (2023)