ANÁLISE COMPARATIVA ACERCA DAS RECOMENDAÇÕES DE SEGURANÇA AOS USUÁRIOS DE DISPOSITIVOS SMARTWATCH

PATRICK TOBIAS VALENTE[1]
MARIÂNGELA FERREIRA FUENTES MOLINA[2]

RESUMO

O número de dispositivos conectados à rede é cada vez maior e, consequentemente, maior é o número de incidentes relacionados à privacidade e proteção dos dados de seus usuários. Dispositivos em Internet das Coisas assumem um papel significativo em nossas vidas com destaque à promoção da qualidade de vida que estes oferecem através de suas funcionalidades. Contudo, estes mesmos dispositivos coletam dados de seus usuários o tempo todo. A proteção dos dados, da privacidade e da segurança dos usuários é importante tanto para os usuários, quanto para as fabricantes. Neste estudo, foi realizado um comparativo acerca das orientações relacionadas à segurança a informação voltada às práticas dos usuários dos dispositivos *smartwatches* das marcas Apple e Samsung. Através do comparativo, identificamos que orientações adotadas pelas fabricantes correspondem às orientações encontradas em folheto informativo CERT, para usuários da internet e que, por meio da disponibilidade de informações, fabricantes dividem com seus usuários a responsabilidade de protegerem os seus dados.

Palavras-chave: Internet das Coisas; Segurança da Informação; Privacidade.

ABSTRACT

As the number of devices connected to the network increases, the number of users incidents related to privacy and data protection increases. Internet of Things devices plays a significant role in our lives with emphasis on benefits on the quality of life they can offer through their functionality. However, these same devices are collecting data from their users all time. Protecting user's data, privacy, and security is important for both users and manufacturers. In this study, a comparison was made about guidelines related to the information security focusing on practice of users for Apple and Samsung smartwatches device brands. With the comparison, we identified that guidelines adopted by manufactures correspond to the guidelines found in CERT papers for internet users. Moreover, through the available information, manufacturers share with their users the responsibility of protecting their data.

Key words: Internet of Things; Information Security; Privacy.

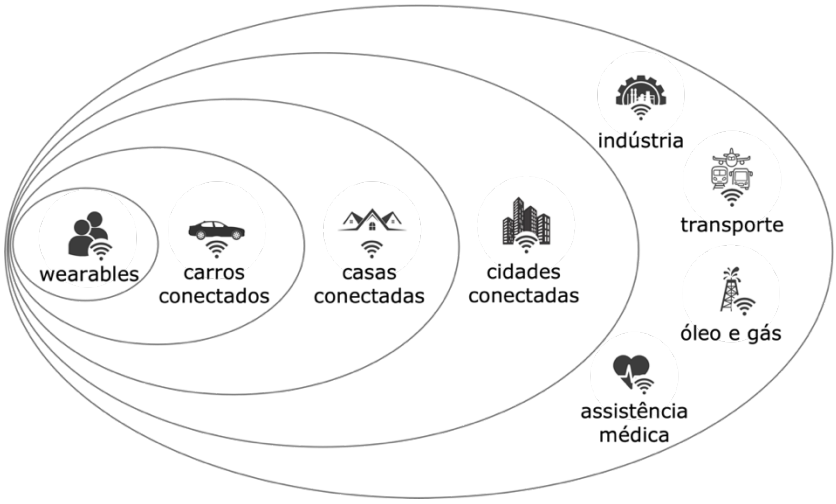
[1]Graduando, Faculdade de Tecnologia de Mogi das Cruzes – Mogi das Cruzes, SP. E-mail: patrick.valente@fatec.sp.gov.br
[2]Docente, Faculdade de Tecnologia de Mogi das Cruzes – Mogi das Cruzes, SP.

INTRODUÇÃO

O termo Internet das Coisas (IoT) é utilizado como referência à capacidade de conectarmos objetos à rede. Em material publicado em seu site, a Oracle descreve a IoT como uma das tecnologias mais importantes do século XXI. Estimava-se que, em 2014 seriam aproximadamente 10 bilhões de dispositivos IoT conectados e que esse número cresceria para aproximadamente 25 bilhões em 2025 (Oracle, 2014). Para Simona Jankowski (2014), publicado em Harvard Business Review, estimava-se que, em 2020, estariam conectados à internet aproximadamente 28 bilhões de "coisas".

As "coisas" em Internet das Coisas podem ser qualquer objeto, dos televisores às escovas de dente, quaisquer objetos que seja permitido comunicarem-se e compartilhar informações. A Figura 1 ilustra a abrangência das "coisas" dentro do paradigma. Entre as "coisas" englobadas pelo paradigma, estão os *wearables*. Segundo F. John Dian et al (2020), *wearables* são dispositivos inteligentes e que podem ser 'vestidos' como um acessório externo.

Figura 1: Abrangência das "coisas" em internet das coisas.



Fonte: Adaptado de The Internet of Things: Making sense of the next mega-trend (The Goldman Sachs Group, Inc., 2014).

À medida que os computadores foram diminuídos e passaram do tamanho de salas para as palmas das mãos, eles também passaram para um modelo computacional passivo (BILLINGHURST e STARNER, 1999), no qual dispositivos atuam e coletam dados 24h, mesmo que isso não seja percebido pelo usuário. Ainda assim, usuários demonstram um interesse crescente nesses dispositivos, os quais prometem aumentar nossa qualidade de vida (SENEVIRATNE et al, 2017). A Figura 2 ilustra como os diferentes dispositivos *wearables* incorporam o cotidiano de uma pessoa.

Figura 2: Abrangência dos dispositivos *wearables.*

Fonte: Adaptado de Enabling Technologies for the Internet of Health Things (RODRIGUES, 2018).

Apesar de interessante, o paradigma IoT traz uma preocupação relacionada à segurança e a proteção dos dados que são compartilhados. Autores como S. Seneviratne et al (2017) e F. John Dian et al (2020) apontam a questão da

segurança como um desafio, o qual pode resultar em complicações em diferentes aspectos de nossas vidas caso ignorado.

Nos últimos anos, uma variedade de *wearables* surgiram no mercado e, com eles, diferentes práticas e implementações de segurança foram definidos. Nesta pesquisa, será realizada uma análise sobre o que é definido acerca da utilização segura dos dispositivos e dos protocolos utilizados nos *smartwatches* das marcas Apple e Samsung, com o objetivo de encontrar alguma convergência ou padrão estabelecido, que seja comum às fabricantes.

MATERIAL E MÉTODOS

Para a elaboração deste material, foi realizada uma pesquisa exploratória, a fim de analisar medidas de segurança e proteção dos dados inerentes ao uso dos *smartwacthes*, voltadas aos comportamentos do usuário. A caracterização da pesquisa é do tipo bibliográfica, baseada em trabalhos publicados sobre o assunto, e de investigação de campo, ainda que baseada em materiais publicados.

No que diz respeito às etapas definidas para o desenvolvimento do estudo, a primeira etapa consistiu na definição das marcas, definição esta estratégica e influenciada pelo que se observa no mercado e consumo dos dispositivos, e no comparativo entre os dispositivos, sendo estes os das marcas Apple e Samsung. Na segunda etapa, teórica, caracterizamos a segurança da informação e exploramos os riscos envolvidos na comunicação e na conexão que implementam os dispositivos e, por fim, a terceira etapa consiste no comparativo entre as marcas e discussão dos resultados.

O comparativo entre os dispositivos foi realizado sobre os protocolos utilizados na comunicação entre dispositivos e no acesso à internet e nas recomendações de segurança voltadas aos usuários. O comparativo tem a finalidade de estabelecer uma relação entre as diferentes marcas e identificar algum padrão de recomendação ou de implementação.

Esta pesquisa restringe-se à avaliação dos riscos relacionados à segurança da informação. Outros riscos associados ao uso dos dispositivos, como os riscos relacionados a integridade física do usuário e da proteção dos dados no caso de perda, roubo ou furto do dispositivo não serão considerados neste estudo.

Segurança da Informação

Segurança da informação compreende o conjunto de métodos e medidas, oferecidos para uma organização ou indivíduo, e que visam a proteção da informação; a segurança da informação baseia-se em três pilares, comumente referido como a tríade CIA (acrônimo para seus correspondentes em inglês *confidentiality*, *integrity* e *availability*), definidos, a seguir, de acordo com o que se lê em material EGI/ CERT de segurança da internet (HOEPERS e JESSEN, 2016). W. Stallings (2015) aponta o que seria uma violação destes pilares no que se segue:

- Confidencialidade: garantia de que as informações estejam disponíveis tão somente para aqueles que possuírem autorização para tal. Perda de confidencialidade resulta da divulgação não autorizada da informação.
- Integridade: garantia de que a informação mantenha sua exatidão e pureza, ou seja, de que não tenha ocorrido qualquer alteração não autorizada. Perda de integridade resulta da modificação não autorizada da informação.
- Disponibilidade: garantia de que as informações estejam acessíveis e disponíveis àqueles que possuam autorização, sempre que necessário. Perda de disponibilidade resulta da perda de acesso ou de uso da informação.

Dispositivos conectados à rede, independentemente da tecnologia utilizada, estão sujeitos a ameaças, é o que diz cartilha CERT de Segurança para Internet (CERT, 2012). Dispositivos como *smartwatches* são capazes de conectarem-se a internet por diversas finalidades. Aproveitar esse recurso com segurança requer

cuidados, tanto de implementação, por parte dos fabricantes, quanto de utilização, por parte dos usuários.

Segurança na Internet

O “grande risco relacionado ao uso da internet é o de você achar que não corre riscos” (CERT, 2012). É importante que usuários conheça os riscos a que estão sujeitos na internet para que, assim, possam desenvolver uma postura de maior atenção na internet. Para tanto, cartilha CERT Segurança para internet, expõe aos usuários os riscos associados ao uso da internet, bem como mecanismos e posturas de segurança que podem ser adotadas pelo usuário

Atacar, fraudar e roubar dados não é assim tão simples. Por isso, golpistas concentram-se nos usuários e em suas vulnerabilidades. Diferentes técnicas, meios e discursos podem ser utilizados com o objetivo de extrair dados e informações das vítimas. De acordo com matéria publicada por Renato Rodrigues (2021), em blog Kaspersky Daily, levantamento realizado pela Kaspersky aponta que brasileiros estão entre os principais alvos de ataques do tipo *phishing* no mundo.

O *phishing* é uma das fraudes listadas pela cartilha e trata-se da tentativa de obtenção de dados através da combinação da tecnologia com a engenharia social. Ataques na internet podem se utilizar dessa estratégia para obter acesso não autorizado a um dispositivo, outras estratégias incluem varredura em redes, *spoofing*, *sniffing*, *denial of service* (DoS), entre outros (CERT, 2012).

Emparelhamento Bluetooth

Em dispositivos operantes a baterias, o consumo de energia é fator relevante em suas aplicações. De modo geral, se um dispositivo em IoT desempenhar um alto volume de processamento e/ ou transmissão de dados, então sua bateria precisará ser recarregada com maior frequência (DIAN et al, 2020). Por este motivo, é comum que o processamento do que se é coletado ocorra fora destes dispositivos. Além disso, transferir os dados para um *smartphone*, por exemplo, permite aos usuários que visualizem melhores apresentações através de dashboards (SENEVIRATNE, 2017).

Dispositivos podem interagir com outros dispositivos, como *smartphones*, através da conexão Bluetooth. Bluetooth é uma tecnologia de comunicação e troca de dados sem fio. Bluetooth Low Energy (BLE) é a tecnologia aplicada aos dispositivos com limitação de recursos, que podem ser bateria e/ ou poder computacional (CASAR et al, 2022) como é o caso dos *smartwatches*.

Assim como em outros protocolos de comunicação sem fio, a conexão Bluetooth/ BLE está sujeita a potenciais ataques. Estudos promovidos por M. Ryan (2013) demonstraram a interceptação de pacotes neste tipo de comunicação, em um ataque do tipo *sniffing*. Do que se apresenta, a interceptação de pacotes transmitidos neste tipo de conexão, configuram violação à confidencialidade, um dos pilares da segurança da informação.

Em relação ao ataque, o autor demonstrou ser capaz de interceptar os pacotes não somente nos estágios iniciais da comunicação, mas também de comunicações que já haviam sido estabelecidas. K. Fawaz e K. Shin (2016) discutem a característica dos dispositivos equipados com a tecnologia de anunciarem sua presença; esta característica permite que outros dispositivos o localizem e iniciem a comunicação, mas que, contudo, pode ser prejudicial e desencadear um ataque.

Em relação à conexão, apesar dos riscos, as especificações Bluetooth/ BLE oferecem medidas de segurança que protegem a conexão de atacantes; entretanto, essas medidas serão efetivas quando devidamente especificadas e implementadas. As especificações BLE são flexíveis em relação aos mecanismos de segurança, isso porque a tecnologia atende a um elevado número de dispositivos, cada um com suas restrições e níveis de seguranças adequados (CASAR et al, 2022).

Conexão à Rede

Em sua maioria, *smartwatches* conectam-se à internet através das tecnologias BLE e Wi-fi, neste caso dependente de um parceiro, ou seja, um

recurso externo, que pode ser um *smartphone* ou um computador com acesso a internet. Embora essa conexão ainda ocorra, não é difícil encontrar *smartwatches* que se conectam diretamente à internet nos dias de hoje.

Estudos analisados sobre os riscos em conexões de rede Wi-fi dividem-se em duas vertentes: (a) do proprietário da rede e (b) do usuário da rede. Seja pelo usuário ou pelo proprietário da rede, inseguranças em conexões Wi-fi representam uma séria ameaça pessoal e de negócio (SARGES et al, 2015). Riscos associados ao proprietário da rede não serão considerados nessa pesquisa.

Riscos associados ao comportamento do usuário da rede incluem *honeypot* e *evil twin*. *Honeypot*, neste contexto, são redes criadas e controladas por administradores maliciosos, para atrair usuários ingênuos e então iniciar seus ataques. *Evil twin* são redes criadas por administradores maliciosos, assim como *honeypot*, mas que atraem usuários porque se parecem com redes legítimas existentes (KOLIAS et al, 2015). Conectados a redes maliciosas, usuários podem ter suas informações interceptadas, violando, assim, a confidencialidade.

RESULTADOS E DISCUSSÃO

No comparativo realizado em relação à conexão com a internet, observamos que, embora os dispositivos sejam capazes de conectarem-se à internet utilizando a rede celular, ambos ainda utilizam o *smartphone* como recurso primário para a conexão; o emparelhamento entre dispositivos ocorre via Bluetooth e tanto no Apple Watch quanto no Samsung Galaxy Watch, o emparelhamento é estabelecido através da conexão BLE. A Tabela 1 expõe os tipos de conexões suportada pelos dispositivos.

Tabela 1: Comparação dos tipos de conexão suportada pelos dispositivos.

	Bluetooth	**Wi-fi**	**Celular**
Apple Watch	✓	✓	✓
Samsung Galaxy	✓	✓	✓

Fonte: Os Autores (2023).

Dispositivos alternam entre as conexões para melhor eficiência da bateria, utilizando o Bluetooth quando o *smartphone* está presente, o Wi-fi quando o *smartphone* não está presente, mas uma rede Wi-fi compatível está disponível e, por fim, redes de celular, quando nem *smartphone* nem Wi-fi estão disponíveis.

Ainda que tenha sido exposto a interceptação de pacotes durante as transmissões BLE e em conexões Wi-fi, os ataques requereram um certo nível de conhecimento e disponibilidade de hardware por parte do atacante, demostrando não ser, então, uma atividade extremamente simples. Atacantes concentram-se, então, no comportamento do usuário em busca de fragilidades e/ ou que coloquem em risco a segurança da informação. A Tabela 2 expõe as recomendações das fabricantes voltadas aos seus usuários.

Tabela 2: Comparação primária das recomendações aos usuários.

	Apple	**Samsung**
Bluetooth	Não foram encontradas recomendações sobre o uso da função.	Escolher um local seguro para conectar-se, não sendo recomendado lugares públicos para conectar-se com um *smartphone* (SAMSUNG, 2022). Desativar a função Bluetooth, quando esta não estiver em uso (SAMSUNG, 2022). Certificar-se de estar compartilhando dados com um dispositivo confiável (SAMSUNG, 2022).

Fonte: Os Autores (2023).

Sobre o acima disposto, não foram encontradas recomendações explícitas em relação ao uso da função Bluetooth pela fabricante Apple. Sabemos que o Apple Watch emprega muitas das capacidades de segurança que se encontram no iOS e iPadOS. Para iPhone (iOS), a recomendação é que o usuário tente manter Bluetooth e Wi-fi ativos, para uma melhor experiência no dispositivo. Apesar do observado, nenhuma inferência pode ser feita para o *smartwatch* (APPLE, 2022).

Orientações aos usuários não é inédito às fabricantes dos dispositivos. Nesta comparação primária, identificamos que recomendações convergem com orientações CERT e que, assim, orientações acerca do uso da função Wi-Fi podem ser inferida a partir das orientações acerca da função Bluetooth. A Tabela 3 realiza um comparativo entre orientações CERT acerca das funções.

Tabela 3. Comparativo entre orientações CERT.

	Bluetooth	**Wi-Fi**
Orientações CERT	Manter a interface inativa e habilitá-la somente quando em uso (CERT, 2012). Evitar a realização do pareamento em locais públicos (CERT, 2012). Não responder a solicitações que você não tenha certeza de que seja o dispositivo correto. (CERT, 2012).	Habilitar a interface Wi-Fi somente quando usá-la e desabilitá-la após o uso (CERT, 2012). Evitar conexões em redes abertas ou públicas (CERT, 2012). Evitar conexões as quais você não conheça a origem (CERT, 2012).

Fonte: Os Autores (2023).

Outras recomendações voltadas aos usuários são expostas em Tabela 4.

Tabela 4. Comparação secundária das recomendações aos usuários.

	Apple	Samsung
Download de Aplicativos	Recomenda-se que faça o download e instale apps somente do App Apple Store (APPLE, 2017).	Recomenda-se não baixar aplicativos desconhecidos (SAMSUNG, 2022).

Fonte: Os Autores (2023).

Download de aplicativos de fontes desconhecidas ou não confiáveis não são encorajados pelas fabricantes; usuários que desejam fazê-lo devem permitir o acesso do aplicativo e concedê-lo confiança de forma manual. Aplicações maliciosas podem utilizar dos recursos dos dispositivos para coletar dados sobre os usuários, sendo possível, por exemplo, identificar padrões do comportamento e atividades confidenciais do usuário. Relatório Kaspersky Lab pode ser encontrado em referências para consulta (KASPERSKY, 2018).

É responsabilidade do usuário conhecer seu dispositivo e funcionalidades, bem como os riscos envolvidos em sua utilização. Materiais que contém informações sobre o uso correto do dispositivo estão disponíveis ao usuário para consulta. Com base nisso, fabricantes isentam-se de algumas responsabilidades relacionadas ao uso indevido do dispositivo, como exposto em Tabela 5.

Tabela 5. Isenção de Responsabilidade.

	Apple	Samsung
Isenção de Responsabilidade	A Apple isenta-se da responsabilidade em relação à escolha, ao desempenho e ao uso de produtos de terceiros (APPLE, 2017).	A Samsung isenta-se da responsabilidade pela perda, interceptação ou mau uso dos dados transmitidos via Bluetooth (SAMSUNG, 2022)

Fonte: Os Autores (2023).

Implementações de segurança utilizadas pelas fabricantes nem sempre estão disponíveis para o acesso e conhecimento do usuário. Algumas práticas são mencionadas, entre elas a criptografia e de políticas de armazenamento dos dados. Contudo, sobre o observado, não foi possível realizar um comparativo para análise.

CONCLUSÃO

A proteção dos dados é relevante a todos os usuários da internet. Deste estudo, destacamos o comportamento das fabricantes em relação à segurança da informação que, além das implementações de segurança que incorporam em seus dispositivos, preocupam-se com o comportamento dos seus usuários. Conscientizar seus usuários é benéfico para ambos, usuários e fabricantes, na manutenção da segurança dos dados e dispositivos. Perda de privacidade impacta não somente aos usuários, mas também as atividades, ao mercado e a credibilidade das fabricantes. Assim, fabricantes dedicam-se à conscientização de seus usuários através de seus manuais, materiais e suporte, disponíveis para consulta online.

Sobre o estudo, conclui-se que usuários e fabricantes dividem a responsabilidade da proteção dos dados. Ao usuário, cabe conhecer os riscos que envolvem a utilização do seu dispositivo, bem como as informações disponibilizadas pelos fabricantes acerca do sistema para, assim, adotar uma melhor postura. Em relação a utilização da internet, segue a máxima do grande risco na internet ser o de achar que não corremos risco.

REFERÊNCIAS BIBLIOGRÁFICAS

APPLE. **Instalar apps empresariais personalizados no iOS**. Apple Inc., 2017. Disponível em: https://support.apple.com/pt-br/HT204460. Acesso em: 21/11/2022

APPLE. **Segurança da Plataforma Apple**. Apple Inc., 2022. Disponível em: https://support.apple.com/pt-br/guide/security/welcome/web. Acesso em: 21/11/2022

APPLE. **Usar o Bluetooth e Wi-Fi na Central de Controle**. Apple Inc., 2022. Disponível em: https://support.apple.com/pt-br/HT208086. Disponível em: 21/11/2022

BILLINGHURST, M.; STARNER, T. **Wearable Devices New Ways to Manage Information**. IEEE. v. 32, pg. 57-64, 1999. Disponível em: https://ieeexplore.ieee.org/document/738305. Acesso em: 19/08/2021

CASAR, M., et al. **A Survey on Bluetooth Low Energy security and privacy**. Elsevier. v. 205, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128621005697. Acesso em: 26/09/2022

CERT. **Cartilha de Segurança para Internet**. v. 4.0, São Paulo: 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 05/09/2022

DIAN, F. J., et al. **Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A survey**. IEEE. v.8, pg. 69200-69211, 2020. Disponível em: https://ieeexplore.ieee.org/document/9058658. Acesso em: 22/08/2022

FAWAZ, K., et al. **Protecting Privacy of BLE Devices Users**. In: Proceedings 25th USENIX Security Symposium, Austin, TX, USA, USENIX Association, 2016. Disponível em: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fawaz. Acesso em: 03/10/2022

HOEPERS, C.; JESSEN, K. S. **Fundamentos de Segurança da Internet**. Escola de Governança da Internet no Brasil (EGI), 2016. Disponível em: https://www.cert.br/docs/palestras/certbr-fundamentos-egijur2016.pdf. Acesso em: 05/09/2022

JANKOWSKI, S. **The Sectors Where the Internet of Things Really Matters**. Harvard Business Review, 2014. Disponível em: https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters. Acesso em: 15/08/2022

KASPERSKY. **Kaspersky Lab descobre quantas informações um relógio inteligente revela sobre o usuário**. Kaspersky Lab, 2018. Disponível em: https://www.kaspersky.com.br/about/press-releases/2018_digital-profiling. Acesso em: 12/09/2022

KOLIAS, C., et al. **Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset**. IEEE. v. 18, pg. 184-208, 2015. Disponível em: https://ieeexplore.ieee.org/document/7041170. Acesso em: 10/10/2022

ORACLE. **O que é Internet of Things (IoT)?** Oracle, 2014 Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/. Acesso em 05/11/2022

RODRIGUES, D., et. al. **Enabling Technologies for the Internet of Health Things**. IEEE. v. 6, pg. 13129-13141, 2018. Disponível em: https://ieeexplore.ieee.org/document/8246498. Acesso em: 05/11/2022

RODRIGUES, R. **Brasileiros são principais alvos de ataques de phishing no mundo**. Kaspersky Daily, 2021. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/. Acesso em: 12/09/2022

RYAN, M., et al. **Bluetooth: With Low Energy Comes Low Security**. In: Proceedings 7th USENIX Workshop on Offensive Technologies (WOOT 13), Washington, DC, USA, USENIX Association, 2013. Disponível em: https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan. Acesso em: 03/10/2022

SAMSUNG. **Manual do Usuário**. Rev. 1.0. Samsung Electronics Co., 2022. Disponível em: https://www.samsung.com/br/support/model/SM-R910NZAPZTO/#downloads. Acesso em: 21/11/2022

SAMSUNG. **Instruções de Segurança**. Rev. 1.4. Samsung Electronics Co., 2022. Disponível em: https://www.samsung.com/br/support/model/SM-R910NZAPZTO/#downloads. Acesso em: 21/11/2022

SAMSUNG. **O Galaxy Watch é compatível com smartphones de sistema operativo Android e iOS através da ligação bluetooth**. Samsung Electronics Co., 2022. Disponível em: https://www.samsung.com/pt/wearables/galaxy-watch/device-compatibility/. Acesso em: 21/11/2022

SARGES, G., et al. **Where's the Security in WiFi? An Argument for Industry Awareness**. IEEE. pg. 5453-5461, 2015. Disponível em: https://ieeexplore.ieee.org/document/7070471. Acesso em: 10/10/2022

SENEVIRATNE, S., et al. **A Survey of Wearable Devices and Challenges**. IEEE. v. 19, pg. 2573-2620, 2017. Disponível em: https://ieeexplore.ieee.org/document/7993011. Acesso em: 22/08/2022

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

The Goldman Sachs Group, Inc. **The Internet of Things: Making sense of the next mega-trend**. IoT Primer, 2014. Disponível em: https://www.goldmansachs.com/insights/pages/internet-of-things/iot-report.pdf. Acesso em: 05/11/2022