Recibido: 31 de octubre del 2022 / Aceptado: 5 de diciembre del 2022
doi: https://doi.org/10.26439/interfases2022.n016.6028

DISPOSITIVOS *WEARABLES* Y LOS RIESGOS A LA PRIVACIDAD: UNA REVISIÓN DE LA LITERATURA

Angelo Rodrigo Taco Jimenez
angelotacoj@gmail.com
https://orcid.org/0000-0001-9806-5379
Universidad de Lima, Perú

RESUMEN. En la actualidad, está en auge del uso de dispositivos que se pueden llevar puestos (*wearable devices,* en inglés): tanto niños como adultos han incorporado en su día a día este tipo de dispositivos adicionales al celular, que hoy son una extensión más del ser humano. Esta investigación hace una revisión de qué son los *wearables*, su uso y los riesgos que implican para el usuario en cuanto a su privacidad y su seguridad. Se eligió la metodología de identificación y control de riesgos entre los resultados de una revisión de alcance en la literatura pertinente.

PALABRAS CLAVE: *wearables*, riesgos, privacidad, seguridad, controles

WEARABLE DEVICES AND PRIVACY RISKS: A LITERATURE REVIEW

ABSTRACT. Currently, the use of wearable devices is booming: both children and adults have incorporated this type of device in addition to cell phones into their day-to-day lives, which today are another extension of the human being. This research reviews what wearable devices are, their use, and the risks they imply for the user in terms of privacy and security. The risk identification and control methodology was chosen from the results of a scoping review in the relevant literature.

KEYWORDS: wearable devices, risks, privacy, security, controls

1. INTRODUCCIÓN

Según Wells (2019), en el año 2018, cerca de 3,7 billones de dispositivos con tecnología *bluetooth* han sido distribuidos alrededor del mundo. Además, en años recientes, la producción de estos dispositivos ha aumentado notablemente y han crecido sus ventas desde el año 2015 hasta el año 2020 (Laricchia, 2022).

Los dispositivos *wearables* pueden favorecer e impulsar el crecimiento tecnológico; sin embargo, al no controlar este crecimiento exponencial, pueden surgir problemas en la garantía de estándares de calidad, seguridad y privacidad. A diferencia de otros tipos de dispositivos *wearables*, los actuales tienen la capacidad de recopilar información del usuario y, además, funcionan como portadores de internet de las cosas (IoT, por sus siglas en inglés), a través de la cual se interconectan los objetos físicos entre sí (Gubbi et al., 2013).

La transformación digital, en el año 2020, provocó que se generara poco más de un billón de megabytes de datos, y esta cantidad se duplica cada cierto tiempo (González, 2020). A ello se suma el negocio de la compra y venta de los datos personales de los usuarios, por lo que estos aparecen en numerosas bases de datos. Como consecuencia, existe un riesgo notable para la privacidad de los usuarios, debido a que en un momento dado no saben cómo su información llega a ser conocida por terceros.

Por lo anteriormente mencionado, el propósito del siguiente trabajo de investigación es aprender los conceptos relacionados con los dispositivos *wearables* y analizar los riesgos que implica el uso de este tipo de dispositivos, a fin de identificar medidas para controlarlos.

2. MARCO TEÓRICO

2.1 Dispositivos *wearables*

Estos dispositivos son utilizados por usuarios de manera externa, de ahí el término *wearable,* que en español significa "llevable". Permiten que el usuario pueda interactuar con sus registros personales y, a su vez, intercambiar o compartir datos como estos:

- Frecuencia cardíaca
- Hábitos de sueño
- Geolocalización
- Parámetros fisiológicos

- Parámetros clínicos
- Hábitos alimenticios
- Calendario

Este tipo de dispositivos tiene mayor exposición en el deporte o en el entretenimiento, y por ese motivo las empresas apuestan por su constante desarrollo y crecimiento, y buscan que usarlos sea lo más sencillo posible para el usuario. Además, las empresas desarrolladoras de aplicaciones también son un pilar importante, ya que al crear aplicaciones más intuitivas, accesibles en precio y óptimas, los usuarios hallan una motivación para llevar a cabo actividades físicas, pues pueden tener un control de su progreso.

2.2 Riesgo

La palabra *riesgo* tiene distintas definiciones que se adaptan a cada situación. La Organización Internacional de Normalización (ISO, 2015) la define como un efecto de la incertidumbre, mientras que para la ISO (2018) es el efecto de la incertidumbre sobre el logro de los objetivos. También es definida como la combinación de que se lleve a cabo un evento y sus posibles consecuencias positivas y negativas. Dentro del concepto de riesgo también encontramos dos factores importantes:

2.2.1 Amenaza

Es un fenómeno que potencialmente puede ocasionar daños y pérdidas. Se determina en función de su frecuencia e intensidad. Son ejemplos de amenazas:

- *Malware*, *ransomware*, virus, etcétera
- Fallas técnicas u operativas

2.2.2 Vulnerabilidad

Se refiere a las características y circunstancias de un sistema que pueden hacerlo susceptible a los efectos provocados por una amenaza latente.

Con los dos factores mencionados, amenaza y vulnerabilidad, se formula la siguiente ecuación:

$$\text{Riesgo} = \text{vulnerabilidad x amenaza} \quad (1)$$

2.3 Privacidad

El derecho a la privacidad se ha visto afectado, como explica Laricchia (2022), debido a la creación de nuevas tecnologías y el constante desarrollo de internet, que

genera nuevos retos a las empresas en el ámbito de protección de datos personales de los usuarios. Según información recopilada por Argentina Cibersegura (2020), la privacidad se entiende como el control que ejerce un usuario respecto a su información y datos, para poder limitar el acceso a terceros o instituciones.

2.4 Gestión del riesgo

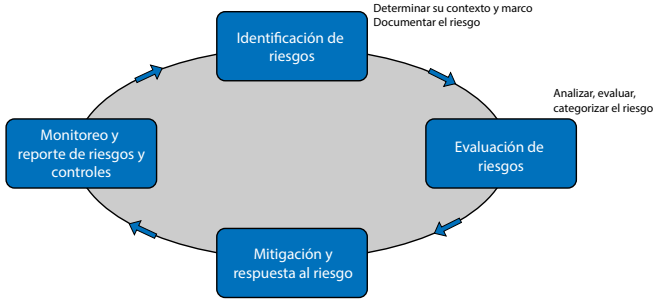
Es un conjunto de técnicas y herramientas que ayudan en la toma de las decisiones más apropiadas para las empresas o personas, según criterios que tengan en cuenta la incertidumbre, la posibilidad del futuro y los efectos de los objetivos. Su fin es la prevención de los riesgos, en lugar de mitigarlos o corregirlos, lo que es beneficioso para las empresas u organizaciones que pongan en uso la ISO 9000 (2015).

2.5 Ciclo de vida de la gestión del riesgo

Para definir el ciclo de vida de la gestión del riesgo, se debe tener en cuenta cuán importante es la toma de decisiones estratégicas, pues estas son, en muchas ocasiones, la causa principal de los desaciertos en escenarios de las empresas u organizaciones. En la Figura 1 se ilustra los cuatro elementos del ciclo de vida de la gestión del riesgo.

Figura 1

Ciclo de vida de la gestión del riesgo



Nota. Reproducido de *Certified in Risk and Information Systems Control (CRISC)*, por ISACA Madrid Chapter, 2010.

3. ANTECEDENTES

La presente investigación se centrará en el uso de una metodología para el descubrimiento y tratamiento de los riesgos para la privacidad y seguridad de los usuarios que acarrean los dispositivos *wearables*. Este tipo de dispositivos son

capaces de proporcionar servicios inteligentes, como la recopilación de información, procesamiento de datos y salida de información (Fernández-Caramés & Fraga-Lamas, 2018); pero el problema radica en la gran cantidad de datos de cada usuario en todo el mundo que puede estar disponible para terceros. Esto plantea una preocupación en la comunidad de investigadores de seguridad y privacidad.

Por tanto, se ha llevado a cabo una búsqueda y análisis de la literatura en bases de datos existentes que ahondan en las vulnerabilidades de la seguridad y de la privacidad que se encuentran en los dispositivos *wearables* y en sus aplicaciones.

En primer lugar, Cyr et al. (2014) hicieron un análisis de las características de la seguridad y de la privacidad de los datos de los usuarios en dispositivos de Fitbit, ahondando específicamente en las debilidades de la seguridad en estos, que usaban *bluetooth* y una aplicación de *smartphone* durante la sincronización del tráfico. El resultado arrojó que Fitbit recopilaba datos del usuario sin su consentimiento y, además, que la dirección MAC de estos dispositivos no cambiaba jamás, lo que facilitaba cualquier ataque de un tercero.

Luego, Seneviratne et al. (2017) realizaron un estudio y una clasificación de dispositivos *wearables* que están disponibles en el mercado; asimismo, analizaron las amenazas en términos de confidencialidad y la disponibilidad de la información que hay en estos dispositivos. Usando el BLE (*Bluetooth Low Energy*) como medio de comunicación, se concluye que existen hasta tres tipos de ataques a los que son vulnerables los dispositivos *wearables*:

- Espionaje
- Análisis de tráfico
- Compilación de información

También Hale et al. (2019) llevaron a cabo una investigación en la que analizaron tres dispositivos: Pebble, Fitbit y Jawbone. Detectaron que los tres expusieron su conexión, por lo que volvieron vulnerable al servidor y abrían la posibilidad de que un atacante pueda seguir la conexión luego de iniciar.

Finalmente, se revisó un informe de Wu y Luo (2019) acerca de la confidencialidad y la seguridad de los datos de los usuarios, el cual se realizó para garantizar el cumplimiento de la regulación de datos, por la vulnerabilidad sensible de dispositivos *wearables*. Los autores identificaron que terceros podrían tener acceso privilegiado a los dispositivos por desencriptar la clave de acceso, debido a un débil sistema de seguridad. Por tanto, sugirieron que, siguiendo las pautas de la HIPAA (Health Insurance Portability and Accountbaility Act), la distribución de la clave de seguridad de los usuarios sea parte de un proceso adicional de autenticación más sólido, con

el fin de tener un estándar de mayor de calidad en privacidad y seguridad para los usuarios.

4. METODOLOGÍA

Se hizo una revisión de alcance para introducir la definición de riesgos y conceptos dependientes a fin de abordar el tema de la privacidad en dispositivos *wearables*. La revisión de alcance usualmente tiene el objetivo de examinar la literatura que esté disponible sin evaluaciones de calidad formales y, a su vez, ayuda a decidir si es necesario llevar a cabo una revisión sistemática (Grant & Booth, 2009; Peters et al., 2015). Según la propuesta de Arksey y O'Malley (2005) de pasos de revisión para la definición de alcance, el presente trabajo realizó búsquedas de literatura existente en tres bases de datos especializadas: IEEE, Web of Science y Scopus.

4.1 Planificación del estudio

En esta subsección se presentan las preguntas de relevancia para la revisión:

- ¿Cuáles son las definiciones de los dispositivos *wearables*?
- ¿Cuál es el riesgo de los dispositivos *wearables* para la privacidad de los usuarios?
- ¿Cuál es el riesgo de los dispositivos *wearables* para la seguridad de los usuarios?
- ¿Cómo identificar los riesgos de dispositivos *wearables*?

Tabla 1

Keywords y query de búsqueda

Bases de datos	Palabras clave	Cadena de búsqueda	Cantidad de artículos
IEEE	"risk", "wearables", "privacy"	TITLE-ABS-KEY (risk AND wearables AND privacy) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (EXACTKEYWORD , "Data privacy") OR LIMIT-TO (EXACTKEYWORD , "Data Privacy") OR LIMIT-TO (EXACTKEYWORD , "Wearables computers") OR LIMIT-TO (EXACTKEYWORD , "Internet Of Things"))	8

(*continúa*)

(*continuación*)

Web of Science	"risk", "wearables", "privacy"	TITLE-ABS-KEY (risk AND wearables AND privacy) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (DOCTYPE , "ar"))	6
Scopus	"user", "risk", "wearables", "privacy"	TITLE-ABS-KEY (risk AND wearables AND privacy AND user) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (EXACTKEYWORD , "Wearable Technology") OR LIMIT-TO (EXACTKEYWORD , "Data Privacy") OR LIMIT-TO (EXACTKEYWORD , "Wearables") OR LIMIT-TO (EXACTKEYWORD , "Internet Of Things"))	10

Para la búsqueda de la literatura en las bases de datos, se usaron palabras clave con relación a dispositivos *wearables* y a riesgos, además de priorizar los artículos más recientes.

Se utilizaron distintos criterios de exclusión y de inclusión para seleccionar los artículos. El primer criterio de exclusión se refiere a los artículos relacionados con el ámbito de la salud y que estudian cómo los dispositivos *wearables* apoyan en el tratamiento o prevención de enfermedades, pero sí se incluye a aquellos que hacen una revisión de conceptos importantes para el desarrollo de la investigación. El segundo criterio comprende a los artículos que describen vulnerabilidades y amenazas del uso de dispositivos *wearables*, pero se excluye a aquellos que tenían información muy similar y que no aportaban lo suficiente. Finalmente, luego del proceso de exclusión e inclusión, fueron seleccionados diez artículos; cabe destacar que la revisión se limitó a publicaciones de artículos en español y en inglés.

Tabla 2

Literatura revisada para dar respuesta a las preguntas

ID	Año	Nombre	Autores
01	2019	Threat Analysis for Wearable Health Devices and Environment Monitoring Internet of Things Integration System	Tzu Wei Tseng, Chia Tung Wu, Feipei Lai
02	2018	Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things	Youngjoo Lee, Wonseok Yang, Taekyoung Kwon

(*continúa*)

(*continuación*)

03	2019	"Worth One Minute": An Anonymous Rewarding Platform for Crowd-Sensing Systems	Lorenz Cuno Klopfenstein, Saverio Delpriori, Alessandro Aldini, Alessandro Bogliolo
04	2020	Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain	Antonio Emerson Barros Tomaz, José Cláudio do Nascimento, Abdelhakim Senhaji Hafid, José Neuman de Souza
05	2020	Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review	Bin Liao, Yasir Ali, Shah Nazir, Long He, Habib Ullah Khan
06	2019	A Review on Intelligent Wearables: Uses and Risks	Yukang Xue
07	2021	Are Serious Games Too Serious? Diffusion of Wearable Technologies and the Creation of a Diffusion of Serious Games Model	Ton A. M. Spil, Vincent Romijnders, David Sundaram, Nilmini Wickramasinghe, Björn Kijl
08	2022	Análisis de problemas de seguridad y privacidad en *wearables* usados por menores	Sonia Solera-Cotanilla, Jaime Fúster, Jaime Pérez, Rafael Palacios, Mario Vega-Barbas, Manuel Álvarez-Campana, Gregorio López
09	2018	A Review on Smart Home Present State and Challenges: Linked to Context-Awareness Internet of Things (IoT)	Zahrah A. Almusaylim, Noor Zaman
10	2021	Systematically Quantifying IoT Privacy Leakage in Mobile Networks	Shuodi Hui, Zhenhua Wang, Xueshi Hou, Xiao Wang, Huandong Wang, Yong Li, Depeng Jin

5. RESULTADOS

5.1 ¿Cuáles son las definiciones de los dispositivos *wearables*?

Lee et al. (2018) definen los dispositivos *wearables* como dispositivos informáticos portátiles; los describen como productos electrónicos en miniatura que son usados por los usuarios y, según los autores, estos representan la siguiente era de la internet de las cosas (IoT, por sus siglas en inglés). Asimismo, aclaran que estos dispositivos poseen una interfaz de usuario particular por sus condiciones y que su tipo de conectividad es ágil.

Según Klopfenstein et al. (2019), estos dispositivos son un poderoso instrumento con capacidad de detección, poder de cómputo y medio de comunicación, que además ayuda en la salud y el estado físico; igualmente, cada uno de estos dispositivos tiene la capacidad de recopilar, procesar y transmitir datos. Tomaz et al. (2020) los definen como accesorios tecnológicos vestibles o implantables usados para el monitoreo de salud de un paciente y que permiten ofrecer servicio médico a distancia. Para Xue (2019), los dispositivos *wearables* se pueden usar en prendas o como accesorio

personal adherido al cuerpo y son capaces de recopilar información, realizar procesamiento de datos y salida de información procesada.

5.2 ¿Cuál es el riesgo de los dispositivos *wearables* para la privacidad de los usuarios?

El artículo publicado por Tomaz et al. (2020) corresponde a una investigación en el ámbito de la salud, y hace una crítica a las empresas creadoras y distribuidoras de dispositivos *wearables* que no se interesan por la privacidad de sus usuarios; se asume por las empresas que los datos recibidos por los teléfonos inteligentes no son manipulados y que su origen no representa un riesgo. La propuesta de Tomaz et al. (2020) es la creación de una asociación exclusiva entre un dispositivo *wearable* y una aplicación de salud; el factor diferenciador se basa en la no dependencia de terceras empresas que se encarguen del almacenamiento de datos de pacientes y que se integre una arquitectura con *blockchain*/IPFS, donde los datos privados de pacientes solo puedan ser administrados por ellos mismos.

Un estudio realizado por Spil et al. (2020) realizó una encuesta a 97 usuarios respecto a la difusión de los juegos serios y cómo impacta en ellos. De esta encuesta, se rescata que solo el 40 % de la población entrevistada mostró interés y preocupación por su privacidad frente al manejo de información de dispositivos *wearables* compatibles con los juegos serios.

Por su parte, Lee et al. (2018) acuñan el término *data transfusion* para referirse a la información que se comparte de un dispositivo móvil a un reloj inteligente cuando se emparejan. Comentan que es inevitable la transferencia de datos cuando este hecho ocurre, ya que es necesario para la inicialización del dispositivo. Lo preocupante es que los usuarios no tienen conocimiento de qué tipo de datos son los que se comparten. Concluyen que, en comparación con los dispositivos móviles, los usuarios no toman conciencia del riesgo que conlleva el desconocimiento de datos compartidos y de que esto es un problema para su privacidad.

5.3 ¿Cuál es el riesgo de los dispositivos *wearables* para la seguridad de los usuarios?

Los dispositivos *wearables* están expuestos, sin excepción, a distintos tipos de problemas de seguridad, los cuales se componen de amenazas, vulnerabilidades y ataques. De acuerdo con Girma (2018), la relación entre la comunicación y la conectividad es la amenaza principal para la seguridad de los usuarios y, en consecuencia, provoca una preocupación en ellos. Por su parte, Liao et al. (2020) señalan que los dispositivos *wearables* son muy susceptibles a sufrir amenazas en su seguridad debido a su bajo costo de producción, por lo que tienen bajo rendimiento

y potencia en comparación con teléfonos móviles y computadoras de escritorio. En el ámbito de IoT, donde trabajan los dispositivos *wearables*, los datos generados por el uso del usuario se recopilan y procesan la mayoría de veces, a excepción de algunas compañías, por terceras empresas, sin que el usuario tenga conocimiento de ello (Almusaylim & Zaman, 2018); así, un atacante puede recibir la comunicación y extraer contenido sin cifrar que se encuentre disponible en el tráfico (Dziubinski & Bandai, 2020).

En la literatura revisada, Hui et al. (2021) reflexionan acerca de la seguridad de los datos de los usuarios y cómo estos son manipulados y compartidos entre proveedores de servicios y terceros maliciosos, lo que da como resultado un monitoreo ilegal, riesgos financieros o amenazas personales. Por ello, proponen un método para cuantificar sistemáticamente la fuga de privacidad de IoT en el tráfico de red móvil; esto implica que los datos de los usuarios están expuestos y son de fácil acceso para cualquier tercero malicioso en el tráfico de red. Con base en su marco de trabajo propuesto, analizan estos datos y presentan estudios de caso que concluyen que los dispositivos *wearables* tienen mayor escala de fuga que cualquier otra entidad de red. Finalmente, se recomienda a usuarios y empresas desarrolladoras que no dejen pasar por alto la importancia de su seguridad en el mundo real, pues cualquier tipo de filtración a pequeña escala puede desencadenar riesgos de suma importancia para los usuarios y sus intereses.

5.4 ¿Como identificar riesgos de dispositivos *wearables*?

Tseng et al. (2019) mencionan en su investigación distintos métodos de prueba, como el escaneo de puertos y el escaneo de vulnerabilidades de seguridad y privacidad con herramientas especializadas, por ejemplo, Wireshark (2022), Nmap (2022) y OpenVAS (2022). Adicionalmente, especifican que los dispositivos IoT se clasifican de dos modos: *bluetooth* y wifi; y que en estos se implementan diferentes protocolos. La literatura de riesgos revisada por Tseng et al. (2019) resalta que la evaluación de riesgos se clasifica en dos tipos: cuantitativa y cualitativa. Ahonda en los métodos de evaluación para identificar la probabilidad e impacto de un riesgo, así como en estudios de evaluación de riesgos que se basan en el modelo STRIDE, que identifica seis amenazas: (i) *spoofing*, (ii) *tampering*, (iii) *repudiation*, (iv) *information disclosure*, (v) *denial of service* y (vi) *elevation of privilege*.

Este método se relaciona con el método DREAD (Altawy & Youssef, 2016), que se usa para calcular la relación de riesgos usando preguntas base para valorar las amenazas como bajas, medias, altas y críticas. Se presenta, a continuación, el método DREAD:

- *Damage*: ¿cuánto daño puede hacer?

- *Reproducibility*: ¿qué tan difícil es realizar el ataque?
- *Explotability*: ¿qué es necesario para ejecutar un ataque?
- *Affected users*: ¿cuántas personas pueden verse afectadas?
- *Discoverability*: ¿qué tan difícil es descubrir vulnerabilidades?

La literatura presenta diversos casos donde existen potenciales riesgos para las personas. Por ejemplo, para los niños que necesitan supervisión de sus padres o apoderados, hay aplicaciones para supervisar su navegación y limitar el uso de distintas funcionalidades incorporadas en sus dispositivos. Cabe destacar que estas aplicaciones requieren permisos especiales para su correcto funcionamiento, lo que da pie a una nueva preocupación acerca de la privacidad de los niños por los datos expuestos en estas aplicaciones. El estudio de Feal et al. (2020) comparó 46 aplicaciones de este rubro en Google Play Store y demostró que el 34 % de ellas recopilan y envían información personal sin consentimiento del usuario, mientras que el 72 % envía los datos con terceros, todo ello sin informar al usuario en sus términos y condiciones. Por eso, luego de hacer la experimentación, se concluye que no son recomendables por su falta de claridad con los usuarios.

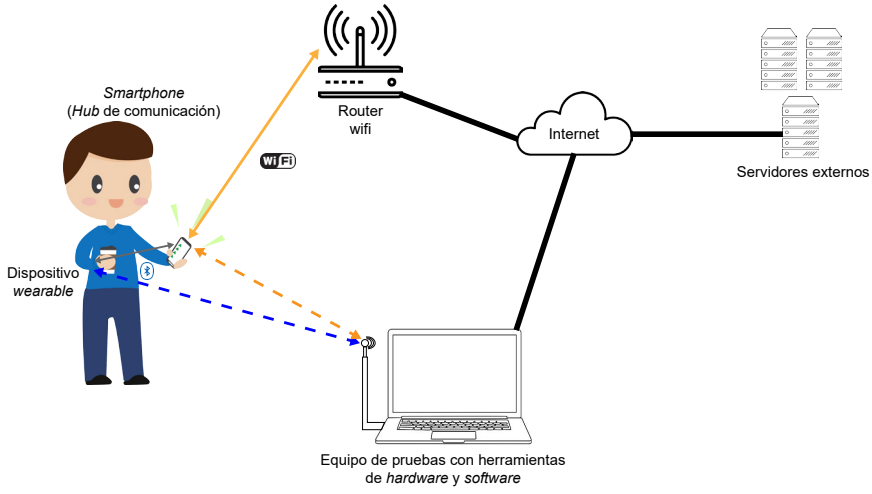
Adicionalmente, con respecto al entorno de Android, Reardon et al. (2019) demostraron que existen aplicaciones de Google Play Store que, con permisos específicos y con la suposición de que el usuario utilice una tarjeta SD (*Secure Digital*), podrían ser utilizadas por un tercero y funcionar como un canal encubierto para compartir el código IMEI del dispositivo móvil.

Aunque los problemas de privacidad parecen ser motivo de gran preocupación, muchas personas no toman medidas o precauciones específicas para mejorar la privacidad (Udoh & Alkharashi, 2016).

Existen diversos aportes metodológicos para la identificación de vulnerabilidades que, en consecuencia, determinan los potenciales riesgos. Por ejemplo, Solera-Cotanilla et al. (2022) proponen una metodología para analizar la seguridad y la privacidad de dispositivos *wearables*; su investigación pone a prueba dispositivos de distintas gamas y características técnicas con el fin de crear conciencia entre fabricantes y usuarios acerca del estado de seguridad y privacidad de estos dispositivos. El esquema de comunicación comúnmente utilizado por los dispositivos *wearables* actuales se muestra en la Figura 2 (Solera-Cotanilla et al., 2022). Un elemento con mayor capacidad de computación (por ejemplo, un *smartphone*) hace de intermediario (*hub*, configurador, etcétera) entre el *wearable* y los servidores externos. La tecnología de comunicación más común entre estos dispositivos es BLE.

Figura 2

Escenario de pruebas



Nota. Reproducido de "Análisis de problemas de seguridad y privacidad en *wearables* usados por menores" (p. 211), por S. Solera-Cotanilla et al., 2022, en *Actas de las VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022).*

En ese sentido, en el escenario se observan tres áreas de comunicación potenciales de análisis: (i) la primera, centrada en la interacción usuario-dispositivo conectado; (ii) la segunda, entre el *wearable* y el *hub* de comunicación; (iii) y la tercera, entre el *hub* de comunicación y los servidores externos o aplicaciones de terceros. En este trabajo, no analizaremos el caso de las conexiones móviles *Long-Term Evolution* (LTE) entre el *hub* de comunicación (por ejemplo, un *smartphone*) y los servidores externos.

6. CONCLUSIONES

Se ha hecho una revisión de los artículos más relevantes para el fin de esta investigación, el cual es conocer qué y cómo se usan los dispositivos *wearables*, así como los riesgos a los que están expuestos los usuarios, tanto niños como adultos, y cómo pueden verse afectados. Al conocer las vulnerabilidades de los principales dispositivos *wearables* mediante metodología de riesgos, se pueden reconocer los riesgos y demás. En futuros trabajos se podrían proponer nuevas metodologías y alternativas a la gestión de riesgos.

REFERENCIAS

Almusaylim, Z. A., & Zaman, N. (2018). A review on smart home present state and challenges: Linked to context-awareness Internet of Things (IoT). *Wireless Network*, *25*, 3193-3204. https://doi.org/10.1007/s11276-018-1712-5

Altawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*, *4*, 959-979. https://doi.org/10.1109/access.2016.2521727

Argentina Cibersegura. (2020). *¿Qué es la privacidad en internet?* https://www.argentinacibersegura.org/admin/resources/files/consejos/33/Gu%C3%ADa_sobre_Privacidad.pdf

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32. https://doi.org/10.1080/1364557032000119616

Cyr, B., Horn, W., Miao, D., & Specter, M. A. (2014). Security analysis of wearable fitness devices (Fitbit). *Massachusetts Institute of Technology*, *1*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082016/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf

Dziubinski, K., & Bandai, M. (2020). Your neighbor knows what you're doing: Defending smart home IoT device traffic from privacy LAN attacks. En L. Barolli, F. Amato, F. Moscato, T. Enokido & M. Takizawa (Eds.), *Web, Artificial Intelligence and Network Applications. WAINA 2020* (pp. 526-534). Springer. https://doi.org/10.1007/978-3-030-44038-1_48

Feal, Á., Calciati, P., Vallina-Rodriguez, N., Troncoso, C., & Gorla, A. (2020). Angel or devil? A privacy study of mobile parental control apps. *Proceedings on Privacy Enhancing Technologies*, *2*, 314-335. https://doi.org/10.2478/popets-2020-0029

Fernández-Caramés, T., & Fraga-Lamas, P. (2018). Towards the internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles. *Electronics*, *7*(12), 405. https://doi.org/10.3390/electronics7120405

Girma, A. (2018). Analysis of security vulnerability and analytics of Internet of Things (IOT) platform. En S. Latifi (Ed.), *Information Technology - New Generations. 15th International Conference on Information Technology* (pp. 101-104). Springer. https://doi.org/10.1007/978-3-319-77028-4_16

González, C. A. (2020). *Introducción a la minería de datos.* Universidad de Valladolid.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi. org/10.1016/j. future.2013.01.010

Hale, M. L., Lotfy, K., Gamble, R. F., Walter, C., & Lin, J. (2019). Developing a platform to evaluate and assess the security of wearable devices. *Digital Communications and Networks*, *5*(3), 147-159. https://doi.org/10.1016/j.dcan.2018.10.009

Hui, S., Wang, Z., Hou, X., Wang, X., Wang, H., Li, Y., & Jin, D. (2021). Systematically quantifying IoT privacy leakage in mobile networks. *IEEE Internet of Things Journal*, *8*(9), 7115-7125. DOI: 10.1109/JIOT.2020.3038639

ISACA Madrid Chapter. (2010). *Certified in Risk and Information Systems Control (CRISC)*.

Klopfenstein, L. C., Delpriori, S., Aldini, A., & Bogliolo, A. (2019). "Worth one minute": An anonymous rewarding platform for crowd-sensing systems. *Journal of Communications and Networks*, *21*(5), 509-520. https://doi.org/10.1109/ jcn.2019.000051

Laricchia, F. (2022). *Wearables unit shipments worldwide by vendor from 1st quarter 2014 to 4th quarter 2021.* Statista.

Lee, Y., Yang, W., & Kwon, T. (2018). Data transfusion: Pairing wearable devices and its implication on security for Internet of Things. *IEEE Access*, *6*, 48994-49006. https://doi.org/10.1109/access.2018.2859046

Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security analysis of IoT devices by using mobile computing: A systematic literature review. *IEEE Access*, *8*, 120331-120350. https://doi.org/10.1109/access.2020.3006358

Nmap. (2022). *Free security scanner for network exploration and security audits*. https:// nmap.org/

OpenVAS. (2022). *A framework for vulnerability scanning and vulnerability management*. http://openvas.org/

Organización Internacional de Normalización. (2015). *Sistemas de gestión de calidad (ISO 9000:2015)*. https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-4:v1:es

Organización Internacional de Normalización. (2018). *Gestión del riesgo (ISO 31000:2018)*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Peters, M. D., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015). Guidance for conducting systematic scoping reviews. *International Journal of Evidence-Based Healthcare*, *13*(3), 141-146. https://doi.org/10.1097/XEB.0000000000000050

Reardon, J., Feal, Á., Wijesekera, P., Elazari, A., Vallina-Rodriguez, N., & Egelman, S. (2019). *50 ways to leak your data: An exploration of apps' circumvention of the android permissions system.* USENIX. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., ... Seneviratne, A. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, *19*(4), 2573-2620. https://doi.org/10.1109/comst.2017.2731979

Solera-Cotanilla, S., Fúster, J., Pérez, J., Palacios, R., Vega-Barbas, M., Álvarez-Campana, M., & López, G. (2022). Análisis de problemas de seguridad y privacidad en *wearables* usados por menores. En *Actas de las VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022)* (pp. 209-215). https://www.researchgate.net/publication/361972187_Analisis_de_Problemas_de_Seguridad_y_Privacidad_en_Wearables_Usados_por_Menores

Spil, T. A. M., Romijnders, V., Sundaram, D., Wickramasinghe, N., & Kijl, B. (2021). Are serious games too serious? Diffusion of wearable technologies and the creation of a diffusion of serious games model. *International Journal of Information Management*, *58*. https://doi.org/10.1016/j.ijinfomgt.2020.102202

Tomaz, A. E. B., Nascimento, J. C. D., Hafid, A. S., & De Souza, J. N. (2020). Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. *IEEE Access*, *8*, 204441-204458. https://doi.org/10.1109/access.2020.3036811

Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing*, *22*, 345-364. https://doi.org/10.1007/s00779-017-1068-3

Tseng, T. W., Wu, C. T., & Lai, F. (2019). Threat analysis for wearable health devices and environment monitoring Internet of Things integration system. *IEEE Access*, *7*, 144983-144994. https://doi.org/10.1109/access.2019.2946081

Udoh, E. S., & Alkharashi, A. (2016). Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. En *2016 Future Technologies Conference (FTC)* (pp. 926-931). https://doi.org/10.1109/ftc.2016.7821714

Wireshark. (2022). *A network protocol analyzer*. https://www.wireshark.org/

Wells, S. (2019, 17 de julio). *How Fitbits, other bluetooth devices make us vulnerable to tracking*. The Brink. https://www.bu.edu/articles/2019/fitbit-bluetooth-vulnerability/

Wu, M., & Luo, J. (2019). *Wearable technology applications in healthcare: A literature review*. HIMSS. https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review

Xue, Y. (2019). A review on intelligent wearables: Uses and risks. *Human Behavior and Emerging Technologies*, *1*(4), 287-294. https://doi.org/10.1002/hbe2.173