FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE SEGURIDAD EN DISPOSITIVOS WEARABLES

AUTOR

ANGELO BRICHETTO RESHUAN

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE SEGURIDAD EN DISPOSITIVOS WEARABLES

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información.

Profesor Guía

MSc. Luis Santiago Criollo Caizaguano

Autor

Angelo Brichetto Reshuan

Año

2020

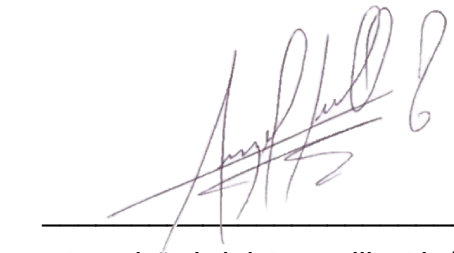
DECLARACIÓN PROFESOR GUÍA

"Declaro haber dirigido el trabajo, Análisis de seguridad en dispositivos wearables, a través de reuniones periódicas con el estudiante Angelo Brichetto Reshuan, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Luis Santiago Criollo Caizaguano
Master en Redes de Comunicaciones
CI: 1717112955

DECLARACIÓN PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, Análisis de seguridad en dispositivos wearables, del estudiante Angelo Brichetto Reshuan, en el semestre 202020, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".



Angel Gabriel Jaramillo Alcázar
Magister en Gerencia de Sistemas y en
Tecnologías de la Información
CI: 1715891964

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

"Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes."

Angelo Brichetto Reshuan

CI: 1804837472

AGRADECIMIENTOS

Al Ing. Luis Criollo, Ing. Angel Jaramillo, Ing. Iván Ortiz, Ing. William Villegas y a la Universidad de las Américas.

DEDICATORIA

A mi familia que me ha apoyado en todo momento a lo largo de mi vida.

RESUMEN

La tecnología vestible se ha convertido en un tema de investigación y análisis. Sin embargo, la importancia de la información que se transporta a través de estos dispositivos incentiva a individuos malintencionados a buscar maneras de atacarlos e interceptar dicha información con diferentes fines ilícitos que convierten a la seguridad de la información en una gran preocupación para los usuarios y fabricantes.

El propósito de este trabajo de titulación busca analizar a través de distintos parámetros basados en dos diferentes modelos encontrados tras una minuciosa investigación fundada en artículos científicos obtenidos de bases de datos científicas y fuentes confiables de la web, donde los autores demuestran su importancia y efectividad en el análisis de la seguridad informática. El primer modelo seleccionado fue el modelo DREAD, este analiza el Daño, Reproducibilidad, Explotabilidad, Afectación y Capacidad de Descubrimiento de cada ataque examinado. El segundo modelo elegido es el modelo STRIDE, este permite clasificar los ataques dentro de las principales categorías de amenazas como Suplantación de Identidad, Manipulación, Repudio, Divulgación de Información, Denegación de Servicio y Elevación de Privilegio.

El análisis realizado muestra a través de tablas y gráficos al ataque de Suplantación de Identidad como el que representa un mayor nivel de riesgo para los dispositivos vestibles. Por otro lado, la amenaza de divulgación de información termina siendo a la cual son más susceptibles estos dispositivos debido a que alberga la mayor cantidad de ataques analizados.

Finalmente, este trabajo de titulación busca demostrar a los usuarios a lo que están expuestos al utilizar dispositivos vestibles y estos puedan decidir de una manera más responsable al momento de adquirirlos. Además, brinda algunas recomendaciones de seguridad para que estos terminales que son utilizados por millones de personas diariamente puedan ser más seguros.

ABSTRACT

Wearable technology has become a subject of research and analysis. However, the importance of the information carried across these devices incentivizes malicious individuals to look for ways to attack them and intercept such information for various illicit purposes that make information security a major concern for users and manufacturers.

The purpose of this degree work seeks to analyze through different parameters based on two different models found after a thorough research based on scientific articles obtained from scientific databases and reliable sources of the web, where the authors demonstrate their importance and effectiveness in the analysis of computer security. The first model selected was the DREAD model, which analyzes the damage, reproducibility, exploitability, affectability, and Discovery Capability of each attack examined. The second model chosen is the STRIDE model, this allows to classify attacks within the main categories of threats such as Spoofing, Tampering, Repudiation, Disclosure of Information, Denial of Service and Elevation of Privilege.

The analysis performed shows through tables and charts the Phishing attack as the one that represents a higher level of risk for wearable devices. On the other hand, the threat of information disclosure ends up being to which these devices are most susceptible because it houses the most attacks analyzed.

Finally, this degree work seeks to demonstrate users what they are exposed to when using wearable devices, so they can decide in a more responsible way when purchasing them. In addition, it provides some safety recommendations so that these terminals that are used by millions of people daily can be safer.

ÍNDICE

1. CAPÍTULO I. INTRODUCCIÓN

La tecnología vestible provee al usuario servicios amigables y personalizados con múltiples sensores de información. Sin embargo, manejan información personal y sensible. Si esta data es utilizada por usuarios maliciosos, podría causar una gran cantidad de problemas sociales.

Dentro del aspecto de la seguridad, se han realizado análisis acerca de ejemplos reales de dispositivos vestibles como son los *Google Glasses*, dispositivos Fitbit y relojes inteligentes Samsung.

Según Ching y Singh (2016) los *Google Glasses* fueron los primeros dispositivos vestibles que dieron inicio al crecimiento de la tecnología vestible. Sin embargo, existe la preocupación acerca de la vulnerabilidad a la privacidad de quien las utiliza.

En el caso de los dispositivos Fitbit, cuyo dispositivo más conocido es la banda inteligente (*Smart fitness band*) que se utiliza en la muñeca. Este provee mediciones de actividad humana como número de pasos caminados, calidad de sueño, pulso, temperatura corporal, entre otros. Sin embargo, uno de los problemas más importantes encontrados en este dispositivo ha sido la falta de autenticación en el aspecto de monitoreo de datos, lo cual permite a cualquier atacante obtener la data de manera fácil sin que el usuario se dé cuenta.

Los dispositivos *Samsung Smartwatch* también contienen vulnerabilidades debido a que, según un estudio realizado por HP, Rawlinson (2015) afirma que el 100% de los dispositivos evaluados presentan diferentes puertas de ataque como autenticación débil, no contienen encripción, entre otras.

1.1 Objetivo General

- Analizar la seguridad de los dispositivos wearables.

1.2 Objetivos Específicos

- Definir la importancia de la seguridad de la información al trabajar con dispositivos wearables en redes wban.

- Estudiar la evolución de la seguridad en dispositivos vestibles.

- Determinar las principales amenazas de seguridad a las que los dispositivos wearables son vulnerables.

1.3 Alcance

El alcance de este trabajo de titulación es realizar un documento en el que se analice las vulnerabilidades de los dispositivos vestibles, los posibles ataques que estos pueden sufrir y mencionar algunas técnicas y métodos a los que se puede recurrir con el fin de tratar de proteger estos terminales para que la información que manejan se encuentre más segura.

Con este documento se busca que los usuarios obtengan más información de a lo que están expuestos al utilizar dispositivos vestibles y puedan realizar un balance de los pros y contras de los mismos al momento de adquirirlos. Además, se busca que las empresas fabricantes de estos terminales conozcan acerca de las vulnerabilidades que tienen sus terminales y se enfoquen en parcharlas con el objetivo de mantener más segura la información de sus clientes.

Para alcanzar el cumplimiento de lo mencionado anteriormente, se va a utilizar fuentes confiables entre la que se encuentran papers, publicaciones, artículos académicos, entre otros documentos que serán buscados utilizando las diferentes bases de datos científicas provistas por la biblioteca virtual de la Universidad de las Américas.

1.4 Justificación

El increíble y rápido crecimiento del número de dispositivos vestibles ha sido el incentivo del desarrollo de este trabajo de titulación. Nagamine (2019) menciona que según la IDC (*International Data Corporation*), solo en el primer cuarto de 2019 se vendieron 49.6 millones de unidades, lo que representa un 55.2% de lo vendido el año anterior.

Estos dispositivos son beneficiosos en diferentes ámbitos y especialmente generan bienestar general y comodidad en el usuario. Uno de estos aspectos y de los más importantes es la salud, permitiendo el seguimiento de datos médicos, comunicación con el médico e incluso inyección de ciertos medicamentos. En el aspecto del estado físico, permite monitorear frecuencias cardíacas calorías quemadas, entre otros datos. También facilitan la vida diaria del usuario al permitirle planificar su rutina diaria, grabar eventos importantes, etc.

Teniendo en cuenta esta información, es muy importante analizar la seguridad de estos dispositivos ya que los mismos manejan información muy personal y sensible de los usuarios como se mencionó antes, especialmente en el aspecto médico donde se encuentran datos de presión arterial, niveles de azúcar en la sangre, diagnósticos médicos, ritmo cardíaco, número de pasos caminados en un día, entre otros. Además, se manipula otra información como ubicaciones, rutinas diarias, etc. Toda esta información es muy importante y útil para el usuario, pero al caer en manos equivocadas pueden traer graves consecuencias negativas para los mismos usuarios y la sociedad debido a que pueden ser víctimas de ataques como inserción de datos, suplantación de identidad entre otros que al ser tan sensible la información manejada puede llevar desde la extorsión hasta a la muerte de un usuario.

Debido a todo lo mencionado anteriormente, es indispensable que los usuarios tengan un conocimiento de toda la información que manejan estos dispositivos y

todos los riesgos que estos representan para su privacidad, además de algunas posibles formas en que pueden tratar de proteger sus datos y así puedan tomar las respectivas medidas para que su información personal se encuentre menos vulnerable y tenga menos probabilidad de ser atacada.

2. CAPÍTULO II. MARCO TEÓRICO

A lo largo de este capítulo se desarrollará una descripción de los diferentes términos utilizados en el tema, características de los dispositivos vestibles y sus diferentes tipos, clasificación de las redes inalámbricas según su extensión, seguridad, tipos de atacantes, vulnerabilidades y amenazas.

2.1 Dispositivos Vestibles

2.1.1 Definición

Según Ching y Singh (2016) la tecnología vestible o también llamada *wearable*, es una tecnología para dispositivos que pueden ser utilizados en el cuerpo humano o vestidos como su nombre lo indica, ya sea una computadora incorporada en un accesorio o parte de un material utilizado en la vestimenta. Estos dispositivos pueden ser encontrados en diferentes formas, ya sean relojes, gafas, pulseras, joyería, entre otros.

Por su parte, el gerente de contenido y editorial de la firma Clutch asegura que los dispositivos vestibles son la tecnología de Internet de las cosas (IoT) más visible para el consumidor. IoT se refiere a dispositivos electrónicos que pueden conectarse a través de Internet. Así, los dispositivos vestibles vinculan a los usuarios al Internet de las cosas a través del contacto directo con su cuerpo. (Kemper, 2018)

2.1.2 Características

Los dispositivos vestibles son definidos por algunas características principales que son las siguientes:

- No restrictivos: Permite a los usuarios realizar otras actividades mientras utilizan estos dispositivos.
- Controlables: Tienen un sistema de respuesta que se encuentra siempre activo, por lo que el usuario puede controlarlo en cualquier momento.

- Atentos: Están siempre atentos a lo que sucede a su alrededor gracias a sus múltiples sensores.

- Observables: Pueden mantener la continua atención del usuario cuando este desee, recibiendo alertas, mensajes o recordatorios.

- Conectados: Se encuentran conectados a una red inalámbrica con el fin de que la información sea compartida en tiempo real.

Las aplicaciones que pueden trabajar con dispositivos vestibles se enfocan al campo del cuidado de la salud, aplicaciones industriales, entretenimiento y artes. Esta tecnología ofrece nuevas oportunidades de monitoreo continuo de la actividad humana a través de pequeños sensores embebidos. Además, provee eficiencia, servicio y productividad.

Sin embargo, Al-Muhtadi, Mickunas y Campbell (2001) aseguran que los dispositivos vestibles enfrentan continuos retos en cuestiones de consumo de energía, capacidad de comunicación, diseño y especialmente seguridad, esto debido a que su limitado ancho de banda y poder de procesamiento los lleva a proveer un menor nivel de seguridad en comparación a otros dispositivos de cómputo.

2.2 Tipos de Dispositivos Vestibles

A los dispositivos vestibles se los puede clasificar en base a su función, apariencia, proximidad al cuerpo humano, entre otros parámetros. Mardonova y Choi (2018) lo clasifican de acuerdo a sus características funcionales, capacidades y aplicaciones en la industria.

2.2.1 Relojes Inteligentes

Los relojes inteligentes son pequeños dispositivos computarizados cuya función es ser utilizados en la muñeca, tienen una funcionalidad expandida relacionada a la comunicación. La mayoría de los modelos comercializados en la actualidad se basan en un sistema operativo móvil. Algunos operan enlazados a un teléfono inteligente brindando una pantalla adicional que informa al usuario notificaciones como mensajes recibidos, llamadas, recordatorios de calendario, entre otras. Los fabricantes continúan desarrollando sus productos y tratando de añadir características, entre estas se encuentran sistemas de navegación GPS, marcos a prueba de agua, y sistemas de rastreo de actividad física y de salud. Al incorporar varios sensores en ellos, los relojes inteligentes se pueden utilizar para la captura y análisis de gestos realizados con las manos como fumar y algunas otras actividades. La figura 1 muestra un ejemplo de reloj inteligente, siendo este un Yamay 020.

Figura 1. Reloj Inteligente Yamay 020.
Tomado de (Amazon, 2020)

2.2.2 Gafas Inteligentes

Dentro de esta categoría, se hallan dispositivos utilizados con los ojos, entre los cuales se encuentran gafas de realidad virtual, realidad aumentada, realidad mixta y lentes de contacto inteligentes. A pesar de sus diferencias en funcionalidad y diseño, las gafas inteligentes pueden venir emparejadas a un *smartphone* con el fin de observar las imágenes obtenidas en la pantalla del teléfono o ser independientes, es decir necesitarán una conexión cableada con un dispositivo fuente. Las gafas inteligentes pueden tener pantallas monoculares, es decir para un solo ojo o binoculares para ambos. La figura 2 muestra unas gafas inteligentes DAQRI.

Figura 2. Gafas inteligentes DAQRI.
Tomado de (ComputerWorld, 2017)

2.2.3 Rastreadores de actividad

Estos dispositivos comúnmente conocidos como *fitness tracker* por su nombre en inglés se utilizan comúnmente en la muñeca, pecho u orejas y están diseñados para monitorear y rastrear actividades deportivas al aire libre y medir parámetros relacionados con la salud y el mantenimiento saludable del cuerpo como la velocidad y distancia recorrida, exhalación, velocidad del pulso y hábitos de sueño.

Mardonova y Choi (2018) aseguran que algunos estudios han concluido que algunos rastreadores funcionan correctamente en lugares cerrados y proveen resultados válidos, mientras otros funcionan de mejor manera en actividades al aire libre. Los investigadores sugieren que estos dispositivos proveen un mayor

control de su salud por parte de los usuarios lo que los motiva a aumentar su actividad física. Varios equipos de fútbol de Europa y Estados Unido utilizan estos dispositivos para cuantificar la actividad física de sus jugadores. La figura 3 muestra un rastreador de actividad LETSCOM.

Figura 3. Rastreador de actividad LETSCOM.
Tomado de (Amazon, 2020)

2.2.4 Vestimenta Inteligente

Este tipo de dispositivo vestible consiste en un conjunto de artículos inteligentes como camisetas, medias, pantalones, zapatos, cascos y gorras con un amplio rango de sensores y características que permiten monitorear la condición física de quien los viste.

Los dispositivos vestibles biométricos han captado la atención de los principales atletas de deportes como el golf, fútbol, atletismo, automovilismo, entre otros gracias a como estos se están beneficiando de la aplicación de los mismos para monitorear su actividad física durante los entrenamientos y así reducir la cantidad de lesiones mejorando el rendimiento del equipo. La vestimenta inteligente tiene la característica de ser altamente beneficiosa para los bomberos en sitios de construcción y transporte. La figura 4 muestra una camiseta inteligente DynaFeed.

Figura 4. Camiseta Inteligente DynaFeed.
Tomado de (HiConsumption, 2017)

2.2.5 Cámaras Vestibles

Las cámaras vestibles proveen un diseño amigable para el usuario, movilidad y flexibilidad que han significado gran interés para el consumidor. Un aspecto interesante de estos dispositivos es que son adecuados para la creación de fotos en tiempo real y videos en primera persona.

Existen dos tipos de cámaras vestibles, unas de ellas son pequeñas cámaras que pueden ser adjuntadas al cuerpo o vestimenta de su usuario incluso pueden ser utilizadas en los oídos, mientras que el otro tipo de estos dispositivos son cámaras grandes con kits de montaje que permiten ajustarlos en gorras o cascos. La figura 5 muestra una cámara vestible PatrolMaster 1296P.

Figura 5. PatrolMaster 1296P.
Tomado de (Amazon, 2020)

2.2.6 Equipo médico vestible

Un equipo médico vestible está formado por uno o varios biosensores que permiten monitorear una gran cantidad de información fisiológica y prevenir enfermedades al realizar diagnósticos previos, además de facilitar tratamientos y rehabilitación desde casa. Los dispositivos vestibles de cuidados de la salud son generalmente utilizados junto con otros dispositivos como monitores, relojes, vestimenta inteligente, entre otros cuyo objetivo también es mostrar y almacenar los datos referentes a la salud del paciente recopilados a través de sensores no invasivos instalados en el cuerpo del paciente como parches sensores de glucosa, presión arterial, entre otros. La figura 6 muestra un sensor de glucosa vestible.

Figura 6. Sensor de glucosa.
Tomado de (Time, 2017)

2.2.7 Joyería Inteligente

La joyería inteligente incluye productos como anillos, collares, aretes, entre otros. Al ser muy pequeños, estos dispositivos tienden a tener funciones específicas y limitadas en comparación con otros terminales como un reloj inteligente. Generalmente, la joyería inteligente está diseñada para alertar a los usuarios de notificaciones en su teléfono, rastrear señales fisiológicas, detección ambiental o autenticación de ingreso. Este tipo de productos son muy poco comunes y relativamente nuevos en el mercado vestible, en consecuencia, su información

técnica es limitada (Seneviratne et al., 2017). La figura 7 muestra la utilización de un anillo inteligente para la autenticación de ingreso.

Figura 7. Anillo Inteligente.
Tomado de (Flynt, 2019)

2.2.8 Tabla comparativa dispositivos vestibles

La tabla 1 mostrada a continuación, permite observar una comparación de los diferentes tipos de dispositivos vestibles y sus principales características.

Tabla 1.
Clasificación de dispositivos vestibles

TIPO	**PROPIEDADES**	**CAPACIDADES**	**APLICACIONES**
Relojes Inteligentes	-Bajo consumo de energía -Interfaz de usuario amigable	-Despliega información específica -Pagos -Rastreo de actividad -Comunicación -Navegación	-Negocios -Marketing -Deportes profesionales -Entrenamiento físico -Educación
Gafas Inteligentes	-Control por medio táctil, movimientos, voz -Bajo consumo de energía -Envía sonidos directo al oído	-Visualización -Interpretación del lenguaje -Comunicación -Coordinación de actividades	-Cirugía -Logística -Educación

Rastreadores de Actividad	-Alta exactitud -A prueba de agua -Peso liviano -Comunicación inalámbrica	-Salud fisiológica -Navegación -Rastreo de actividad física -Monitoreo de ritmo cardíaco	-Cuidado de la salud -Deporte profesional -Deporte aficionado
Vestimenta Inteligente	-No tiene pantalla -Información es obtenida por sensores corporales	-Monitoreo de ritmo cardíaco, actividades diarias, temperatura y posición corporal -Calentamiento o enfriamiento del cuerpo	-Deporte profesional -Medicina -Milicia -Logística
Cámaras Vestibles	-Captura de video y fotografías en primera persona -Pequeñas dimensiones -Visión nocturna -Empotramiento en ropa o cuerpo	-Captura fotografías y videos en primera persona -Streaming en vivo -Rastreo de actividad física	-Defensa -Salud -Industria -Educación
Dispositivos Médicos Vestibles	-Manejo del dolor -Monitoreo fisiológico -Monitoreo de glucosa -Monitoreo de sueño -Monitoreo de actividad cerebral	-Detección y monitoreo de enfermedades cardiovasculares, desordenes fisiológicos, enfermedades crónicas, diabetes	-Cirugía -Neurociencia -Dermatología -Rehabilitación
Joyería Inteligente	-Muy pequeños -Cómodos y agradables diseños -Bajo consumo de batería	-Monitoreo de señales fisiológicas -Alerta de notificaciones -Detección ambiental	-Medicina -Geolocalización -Ecología

2.3 Impacto de los dispositivos vestibles en la sociedad

2.3.1 Medicina

Zheng et al. (2014) mencionan que la creciente población, la imponencia de enfermedades crónicas y la aparición de enfermedades infecciosas son unos de los mayores retos para la sociedad actual. En la búsqueda de cubrir las necesidades del cuidado de la salud, principalmente la predicción y tratamiento de enfermedades graves, ha emergido la informática de la salud como un área multidisciplinaria de investigación que maneja la adquisición, transmisión, procesamiento, almacenamiento y uso de información médica.

La adquisición de información relacionada a la salud por medio de adquisición de datos discreta y tecnología vestible es considerado como la base para la informática de la salud. Los sensores pueden ser integrados en el cuerpo, vestimenta y accesorios del paciente, lo cual permite que la información sea tomada silenciosamente a lo largo del día a día. Además, pueden ser diseñados como tatuajes pegados al cuerpo o impresos directamente en la piel humana, esto permite un monitoreo a largo plazo.

Poon, Wong y Zhang (2006) indican que, observando la historia, la innovación y evolución de la tecnología es la medicina es ampliamente notable. Un ejemplo de ello es la toma de un electrocardiograma, donde la tecnología antigua utilizaba baldes de agua, voluminosos tubos de vacío, una mesa de trabajo y dispositivos con transistores, mientras que hoy en día se puede observar vestimenta y pequeños accesorios basados en dispositivos vestibles con circuitos integrados. Kim et al. (2011) corrobora que, en el futuro, esto probablemente evolucionará a dispositivos vestibles flexibles con electrónica de carbono de nanotubos.

Según Zheng et al. (2014) a pesar de que los dispositivos de medición fisiológica han sido usados ampliamente, algunas características únicas de los dispositivos vestibles han cambiado la forma en que estos eran utilizados debido a los

recientes avances en temas de adquisición de datos, networking y fusión de información. Primeramente, a través de la conectividad inalámbrica junto con la amplia infraestructura disponible de Internet, los dispositivos pueden proveer información en tiempo real y facilitar la intervención remota inmediata en casos de epilepsia o ataques cardíacos, particularmente en áreas rurales donde la intervención médica es escasa o nula.

Además, para la población saludable, el monitoreo discreto y vestible puede proveer información detallada sobre su salud a través de su teléfono celular o pantallas flexibles con la cuales puedan monitorear su bienestar, mismo que no solamente promueve un estilo de vida activo y saludable, también permite la detección de algún riesgo de salud y facilita la implementación de medidas preventivas en etapas primarias.

La figura 8 muestra un dispositivo vestible utilizado para la medición y proyección de datos médicos del usuario.

Figura 8. Dispositivos Vestibles en Medicina.
Tomado de (Healthcare IT Leaders, 2018)

2.3.2 Imagen Social

Según Yang, Yu, Zo y Choi (2015) el valor percibido por el usuario tiene una alta influencia en los consumidores potenciales de dispositivos vestibles. Su investigación halló que los beneficios percibidos representan una mayor influencia sobre el usuario que los potenciales riesgos porque muchos individuos ya han experimentado con varios dispositivos móviles innovadores como, por

ejemplo, teléfonos inteligentes, tabletas, entre otros y manejan suficiente información sobre ellos.

Yang et al. (2015) indican que la imagen social es un factor muy fuerte que afecta el valor percibido, dándole un mayor peso a los componentes beneficiosos. Al estar los dispositivos vestibles en su auge hoy en día, los consumidores esperan mejorar su imagen social al ser los primeros en comprarlos. Además, como estos dispositivos pueden incorporarse en vestimenta y accesorios, los hace más visibles ante el resto de las personas, permitiéndoles a sus portadores presumir estas innovaciones en el transcurso del día a día de sus vidas.

La imagen social tiene una alta relación con el atractivo visual, esto es consistente con algunos estudios previos que demuestran como los productos innovadores con un diseño lujoso e innovador permiten a sus dueños diferenciarse de otros (Park, Rabolt y Jeon, 2008; Tzou y Lu, 2009). Asimismo, revelaron que los clientes optan por el diseño como el factor más importante frente a otros aspectos como la operación y demás características en su agrado general hacia sus dispositivos móviles. La figura 9 muestra una representación de los dispositivos vestibles en la sociedad.

Figura 9. Dispositivos Vestibles en la Sociedad.
Tomado de (Wired, 2013)

2.3.3 Preferencias del consumidor

Según Yang et al. (2015), la utilidad del dispositivo se ha mostrado como un factor ligeramente más fuerte que el entretenimiento para los potenciales usuarios, mientras que para los usuarios actuales el factor más influyente es el entretenimiento brindado. Los investigadores señalan que los resultados de su estudio exponen la búsqueda de placer por parte de los usuarios reales al utilizar dispositivos vestibles, mientras que los usuarios potenciales los requieren más para propósitos utilitarios que por diversión. Por lo tanto, los autores creen que es importante asegurarse que no solo los usuarios actuales se sientan entretenidos, sino que los potenciales compradores perciban la utilidad de estos dispositivos y se motiven a adquirirlos.

La funcionalidad y compatibilidad influyen de manera positiva en la percepción de los usuarios. Según Davis (1989) las percepciones de utilidad de los sistemas tecnológicos han sido vinculadas tradicionalmente con la funcionalidad que ofrecen en la ayuda a los usuarios a alcanzar sus propósitos. Asimismo, los dispositivos vestibles que ofrecen aplicaciones móviles de alta calidad, acceso a internet de alta velocidad, retraso mínimo y una batería de larga duración tienen una mejor aceptación que los que ofrecen menor funcionalidad.

Los dispositivos vestibles tienen que trabajar de la mejor manera con los productos de tecnologías de la información del usuario, entre los que se encuentran sus teléfonos inteligentes, tabletas y computadoras, esto con el fin de una óptima sincronización y transferencia de información. Por ejemplo, la confiabilidad de la telemedicina depende en la exactitud de la información transferida desde el dispositivo vestible del paciente hacia las aplicaciones de diagnóstico o la computadora del doctor. (Davis, 1989). La figura 10 muestra la variedad de dispositivos vestibles existentes.

Figura 10. Variedad de Dispositivos Vestibles.
Tomado de (FitLyfe, 2019)

2.3.4 Industria

Yang et al (2015) consideran que los dispositivos vestibles pueden ser adquiridos por cualquier industria para propósitos de negocios. Los terminales del tipo reloj inteligente pueden reemplazar o complementar a los teléfonos y tabletas debido a que, a través de estos, los usuarios pueden recibir correo electrónico, mensajes de texto, y notificaciones sin tener que sacar del bolsillo o cartera sus teléfonos celulares.

Los dispositivos montados sobre la cabeza y de realidad virtual permiten a los médicos realizar cirugías mientras monitorean de manera simultánea los signos vitales de un paciente y así reaccionar a los cambios sin la necesidad de descuidar su vista del paciente.

Las universidades también pueden adquirir dispositivos vestibles en la búsqueda de mejorar su educación, brindando así a los alumnos experiencias simuladas de ambientes intensos como un quirófano, un campo atlético, o espacios al aire libre. Por lo tanto, los dispositivos vestibles tienen un gran campo de desarrollo en la industria debido a que permiten realizar las actividades empresariales de una manera más rápida y eficiente. (Yang et al, 2015). La figura 11 muestra la influencia de los dispositivos vestibles en la industria.

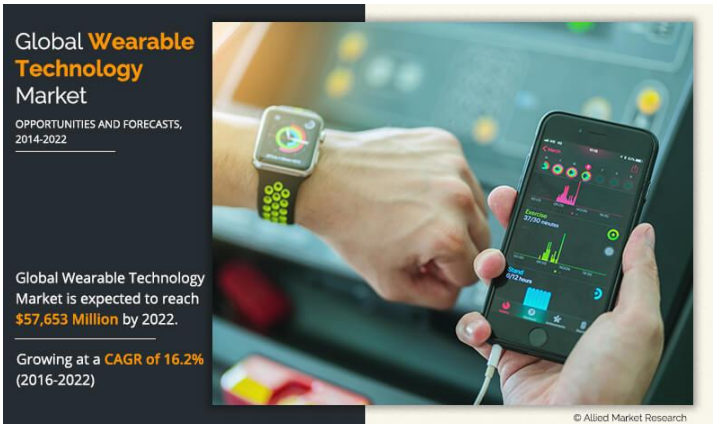


Figura 11. Dispositivos Vestibles en la Industria.
Tomado de (Allied Market Research, 2017)

2.3.5 Educación

Los dispositivos vestibles se pueden utilizar en el campo de la educación en algunos contextos como el aprendizaje auténtico, multimedia y cinestésico. La figura 12 muestra unas gafas inteligentes utilizadas para el aprendizaje.

Figura 12. Dispositivos Vestibles en la Educación.
Tomado de (WTVOX, 2018)

2.3.5.1 Aprendizaje Auténtico

Este tipo de aprendizaje se encuentra situado en el mismo contexto del mundo real en el que será aplicado (Heerington, Reeves, & Oliver, 2014). En otras palabras, permite a los estudiantes experimentar tareas integradas en

situaciones y contextos sociales y físicos del mundo real donde normalmente se encontrarían con ellas.

Un ejemplo de actividad auténtica donde intervienen los dispositivos vestibles se dio en el centro médico de la Universidad Estatal de Ohio donde un cirujano utilizó el dispositivo *Google Glass* para transmitir una cirugía en vivo a un grupo de estudiantes de medicina. (Centro Médico Wexner de la Universidad Estatal de Ohio, 2013). Los dispositivos vestibles permitieron a los estudiantes observar y aprender el procedimiento de una cirugía en primera persona desde el punto de vista de un experto. La figura 13 muestra el dispositivo vestible *Google Glass* utilizado en la mencionada cirugía.

Figura 13. Utilización de *Google Glass* para una clase de cirugía.
Tomado de (Weintraub, 2013)

2.3.5.2 Aprendizaje Multimedia

Según Mayer (2001) el aprendizaje multimedia se encarga de proveer instrucciones o presentar contenido que incluye texto, ya sea impreso o narrado, e imágenes como gráficos, cuadros y videos.

Los dispositivos vestibles pueden ser utilizados y representar una gran ayuda para el aprendizaje multimedia. Un ejemplo de lo mencionado se puede observar en un experimento realizado por el Grupo de Computación Contextual en el Instituto de Tecnología de Georgia en los Estados Unidos, allí se está llevando

a cabo el proyecto *Captioning on Glass* que busca ayudar a individuos que tienen dificultades para escuchar. El orador habla en el dispositivo móvil del individuo. En respuesta, el dispositivo *Google Glass* recibe la entrada del orador transcrita y la proyecta en su pantalla. Así, el individuo con dificultades auditivas recibe una transcripción en tiempo real de lo mencionado por el orador. (Grupo de Computación Contextual, 2014). La figura 14 muestra un usuario utilizando el dispositivo *Google Glass* como transcriptor.

Figura 14. *Google Glass* como transcriptor.
Tomado de (eLearning Bakery, 2019)

Según Sawaya (2015), a pesar de que este proyecto no engloba actividades de aprendizaje, es evidente que los *Google Glass* tienen el potencial de ser utilizados para el aprendizaje multimedia.

Otro ejemplo presenta Marner, Irlitti y Thomas (2013). Ellos han desarrollado una pantalla vestible que proyecta información virtual en un objeto físico y real, esto ha probado la efectividad del dispositivo en la mejora del rendimiento de los participantes en actividades de procedimiento comparado con una pantalla tradicional.

2.3.5.3 Aprendizaje Cinestésico

Los investigadores del Grupo de Computación Contextual del Instituto de Tecnología de Georgia desarrollaron un sistema háptico e inalámbrico de

instrucciones de piano que los usuarios lo utilizan como guante. Cada dedo de este guante está equipado con un pequeño motor de vibración que indica que nota musical se debe tocar. El objetivo de este proyecto busca el aprendizaje pasivo cinestésico, mismo que a pesar de no ser enseñado explícitamente, permite a los estudiantes interactuar físicamente con los estímulos necesarios. (Evans y Rick, 2014).

Huang et al. (2010) evaluaron la efectividad del guante y descubrieron que los usuarios que lo utilizaban lograron aprender una secuencia de notas de manera más precisa que los que no lo utilizaron.

La figura 15 muestra el guante antes descrito:

Figura 15. Guante utilizado para aprendizaje de piano.
Tomado de (Huang et al., 2010)

Todos estos ejemplos mencionados anteriormente, muestran el potencial de los dispositivos vestibles para las prácticas educacionales. El hecho de ser vestidos por los usuarios e integrados en sus contextos, proporciona las claves para comprender los fundamentos teóricos necesarios para el aprendizaje con dispositivos vestibles. (Sawaya, 2015).

2.4 Clasificación de redes inalámbricas según su extensión

Las redes inalámbricas se clasifican según su extensión de la siguiente manera:

2.4.1 Redes Inalámbricas de Área Metropolitana (WMAN - *Wireless Metropolitan Area Networks*)

Las redes inalámbricas de área metropolitana están basadas en el estándar IEEE 802.16, mejor conocido como WiMAX. Salazar (2017) indica que este estándar es una tecnología de comunicaciones que soporta una arquitectura punto-multipunto con el fin de proveer enlaces de alta velocidad a través de un área metropolitana. Esto permite a pequeñas redes de área local interconectarse y formar una red más amplia. De este modo es como se logra el enlace entre ciudades sin la necesidad de cableado.

2.4.2 Redes Inalámbricas de Área Extensa (WWAN - *Wireless Wide Area Networks*)

Las redes WWAN pueden extenderse más allá de los 50 kilómetros y generalmente utilizan frecuencias licenciadas. Este tipo de redes pueden ser desplegadas a través de áreas amplias como ciudades y países por medio de múltiples sistemas satelitales o sistemas de antenas ofrecidos por un proveedor de servicios de internet. (Salazar, 2017)

2.4.3 Redes Inalámbricas de Área Local (WLAN - *Wireless Local Area Networks*)

Según Salazar (2017) las redes inalámbricas de área local están diseñadas para proveer acceso inalámbrico en áreas de un rango de hasta 100 metros y se utilizan generalmente en escuelas, hogares, laboratorios de computación o ambientes de oficina.

2.4.4 Redes Inalámbricas de Área Personal (WPAN - *Wireless Personal Area Networks*)

Según Salazar (2017) las redes de área personal están basadas en el estándar IEEE 802.15. Estas permiten la comunicación en un rango muy corto de 10 metros aproximadamente. La conexión realizada a través de una red WPAN permite la implementación de soluciones pequeñas, baratas y eficientes para muchos dispositivos como un teléfono inteligente debido a que involucra una poca o nula infraestructura o conectividad directa fuera del enlace.

El autor menciona que estas redes se caracterizan por necesitar poca energía y una baja tasa de transferencia de bit y dependen de tecnologías como *Bluetooth*, ZigBee, IrDA o UWB. Desde el punto de vista de aplicación, *Bluetooth* se utiliza para la conexión de un mouse o teclado inalámbrico y auriculares de manos libres, IrDA en enlaces punto a punto entre dos dispositivos de transferencia de información simple y sincronización de archivos, ZigBee para el monitoreo y control inalámbrico de red y UWB se orienta a enlaces multimedia de gran ancho de banda. La figura 16 muestra el diagrama de una red WPAN.

Figura 16. Diagrama de red WPAN.
Tomado de (ICT Lounge, 2020)

2.4.5 Redes Inalámbricas de Área Corporal (WBAN - *Wireless Body Area Networks*)

Según Arefin, Ali y Haque (2017) es una red de varios sensores interconectados localizados dentro y/o fuera del cuerpo humano. Esto permite monitorear y recopilar diferente información del usuario. En las redes WBAN el usuario se puede movilizar utilizando los sensores sin ningún problema, el consumo de energía es muy bajo al igual que el costo de los mismos. Este tipo de redes utilizan tecnologías inalámbricas como *Bluetooth*, ZigBee, IEEE 802.15.6, WiFi de bajo consumo, NFC y LoRa.

2.4.5.1 Arquitectura de red WBAN

Arefin et al. (2017) clasifica a la arquitectura de una red WBAN en cuatro secciones, la primera sección consiste en varios nodos de sensores fisiológicos ubicados estratégicamente en el cuerpo humano, todos estos sensores son utilizados para monitorear continuamente el movimiento, parámetros vitales como ritmo cardíaco, presión sanguina, entre otros, además del ambiente que los rodea. Tradicionalmente, estos sensores se utilizan a través de cables, lo cual sería muy incómodo para el usuario llevar puestos todo el día, por lo tanto, las redes WBAN son una solución efectiva en el área, especialmente en casos de salud donde el paciente necesita ser monitoreado constantemente.

La segunda sección consiste en el nodo de coordinación, allí todo el sistema de sensores se conectará a un nodo conocido como la unidad central de control, esta unidad toma la responsabilidad de recolectar información de los sensores y transmitirlos a la siguiente sección. La tercera sección se encarga de la comunicación, actuando como *gateway* hacia el destino, en este punto, generalmente se utiliza un teléfono móvil que envíe la información hacia una red celular GSM/3G/4G, aunque también se puede utilizar un router o una computadora que se comunique vía correo electrónico o algún otro servicio por medio de *Ethernet*.

Finalmente, la cuarta sección es un centro de control que consiste en dispositivos finales como un teléfono móvil, un computador que monitorea la información y la almacena en una base de datos. La figura 17 muestra la arquitectura de una red WBAN.

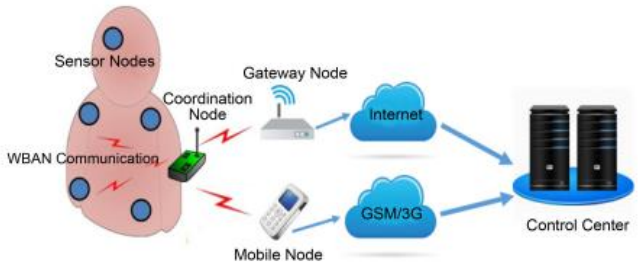


Figura 17. Arquitectura de Red WBAN.
Tomado de (Arefin et al., 2017)

2.4.5.2 Requerimientos de dispositivos utilizados en redes WBAN

Arefin et al. (2017) señalan que los sensores utilizados en las redes WBAN deben cumplir ciertos requerimientos que son los siguientes:

- Vestibilidad: Permitirá un monitoreo continuo no invasivo y discreto, los sensores deben ser ligeros y pequeños, estos factores generalmente se ven determinados por el tamaño y peso de las baterías, lo que es directamente proporcional a su capacidad.

- Fiabilidad: Una comunicación confiable es importante en las redes WBAN, por lo que el diseñador debería utilizar una técnica de comunicación que asegure la transmisión ininterrumpida y un óptimo rendimiento.

- Seguridad: Todos los sensores utilizados manejan información privada, por lo que se debe asegurar a privacidad de todos estos datos.

- Interoperabilidad: Los sensores deben permitir al usuario construir fácilmente una red WBAN robusta.

2.4.5.3 Estándares y Tecnologías en redes WBAN

Las redes WBAN necesitan de diferentes tipos de estándares y tecnología para su comunicación. Entre estos se encuentran *Bluetooth*, ZigBee, WiFi, IEEE 802.15.6, entre otros.

2.4.5.3.1 Bluetooth

Bluetooth es un estándar IEEE 802.15.1. Esta tecnología fue diseñada para la comunicación inalámbrica de corto alcance con el fin de construir una red con seguridad y bajo consumo de energía. *Bluetooth* opera en la banda de 2.4GHz. Generalmente, una red *Bluetooth* típica se puede construir utilizando un dispositivo en modo maestro y otros siete en modo esclavo, lo que le da la posibilidad a cada dispositivo de comunicarse con el otro simultáneamente. Además, existe otra topología donde se puede enlazar un dispositivo de una red *Bluetooth* como esclavo de otra. La figura 18 muestra la topología de esta red.

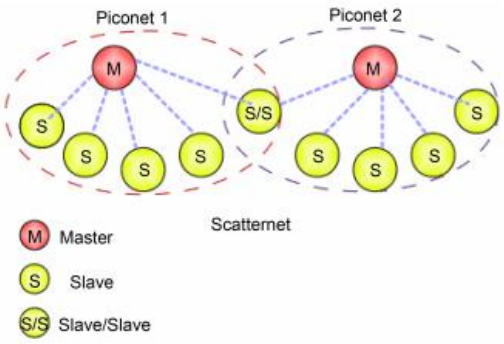


Figura 18. Topología de red B*luetooth*.
Tomado de (Arefin et al. 2017)

Un tema sólido en la literatura revisada es la vulnerabilidad de seguridad durante el emparejamiento del dispositivo vestible con la estación base. En este punto, el intercambio de información durante el emparejamiento es vulnerable, por

consiguiente, es importante comprender como funciona este proceso. Al momento de emparejarse por primera vez, *Bluetooth* emplea uno de los siguientes métodos de Emparejamiento Seguro Simple (SSP).

- Simplemente Funciona: Empareja automáticamente cuando es requerido sin interacción del usuario. Útil para la accesibilidad en IoT, pero es el menos seguro.

- Comparación Numérica: Al momento de intentar emparejarse por primera vez, el dispositivo vestible y el teléfono inteligente muestran una llave numérica idéntica de cuatro a seis dígitos. Si ambos concuerdan, el *smartphone* solicita al usuario que acepte la conexión.

- Llave Maestra: Consiste en que ambos dispositivos tienen una interfaz de usuario para ingresar un código de cuatro a seis dígitos. Uno o ambos dispositivos deben ingresar una llave maestra para que su emparejamiento sea exitoso. Según los autores, este método es el más seguro de los tres analizados. (Lotfy y Hale, 2016; Pieterse y Oliver, 2014)

A continuación, se definen otros procesos utilizados durante el emparejamiento en una comunicación *Bluetooth*:

- Perfil de Acceso Genérico (GAP): El dispositivo vestible define un protocolo de anuncio específico después del emparejamiento inicial durante instancias de conexión repetidas.

- Perfil de Atributo Genérico (GATT): Se trata de un entorno de servicio en la parte superior del protocolo de transporte elemental, llamado Protocolo de atributos, que establece el estándar de transferencia de datos mutuamente acordado.

- Ambos GAP y GATT operan en la banda de 2.4 GHz y transmiten a una velocidad de 1Mbps.

Lotfy y Hale (2016) mencionan que a pesar de que *Bluetooth Low Energy* (BLE) opera en las mismas frecuencias que otras tecnologías *Bluetooth*, este opera de diferente manera en las capas física y de enlace. BLE utiliza 40 canales, de los cuales tres son utilizados para el anuncio por dispositivos vestibles no conectados. Los restantes 37 canales son usados durante el perfil de atributo genérico (GATT) para la transmisión de data después del emparejamiento. La figura 19 muestra el proceso de emparejamiento de la tecnología BLE.

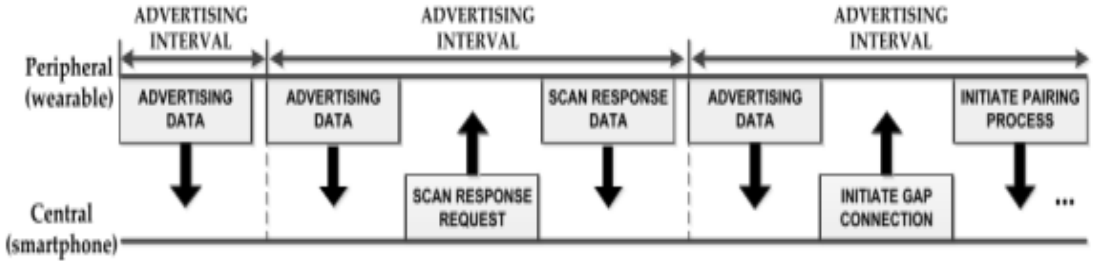


Figura 19. Proceso de emparejamiento *Bluetooth Low Energy*.
Tomado de (Lotfy y Hale, 2016)

2.4.5.3.2 ZigBee

ZigBee es una solución para telecomunicaciones inalámbricas estandarizada bajo el estándar IEEE 802.15.4, está diseñada para sensores y controles, apropiada para utilizarla en condiciones duras y aisladas. Una de sus principales características es el bajo consumo de energía.

La topología característica de *ZigBee* está compuesta por tres tipos de dispositivos o nodos que son un coordinador, un router y un dispositivo final. El coordinador maneja las funciones de administración de la red, el router las funciones de enrutamiento y los dispositivos finales son dispositivos alimentados de energía que se encuentran generalmente en modo standby y se muestran

activos para recolectar información. La figura 20 muestra la topología de una red *ZigBee*.

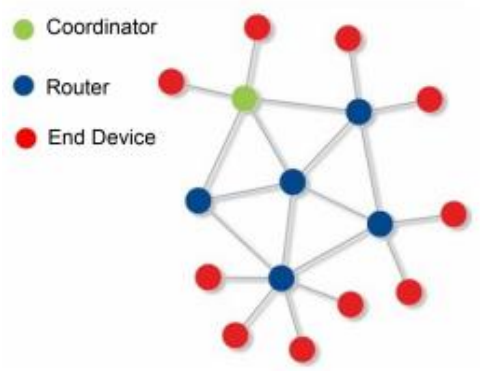


Figura 20. Topología de red *ZigBee*.
Tomado de (Arefin et al. 2017)

2.4.5.3.3 WiFi

WiFi es una tecnología para redes inalámbricas bajo el estándar IEEE 802.11 que opera en la banda de 2.4 GHz y 5 GHz en una cobertura de 100 metros. Esta tecnología permite a los nodos sensores y usuarios transferir datos directamente hacia el internet a través de un router WiFi básico, además puede ser utilizada para la adquisición de data a través de aplicaciones que permiten una comunicación directa entre los sensores y el teléfono inteligente o computador sin un router intermediario. No obstante, la desventaja de esta tecnología es su alto consumo de energía. (Arefin et al. 2017). La figura 21 muestra la topología de una red WiFi.

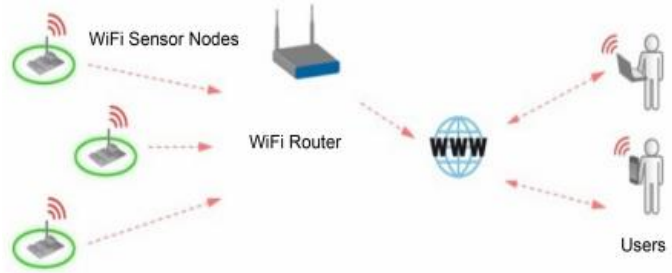


Figura 21. Topología WiFi.
Tomado de (Arefin et al. 2017)

2.4.5.3.4 IEEE 802.15.6 WBAN

El estándar 802.15.6 o también conocido como estándar WBAN provee varias aplicaciones médicas y no médicas, soporta comunicaciones dentro y alrededor del cuerpo humano. Esta comunicación puede ser utilizada para monitoreo de la salud, deportes, ambiente, entre otras aplicaciones.

Según Arefin et al. (2017) el estándar se encuentra dividido en otros tres estándares, cada uno utiliza diferentes bandas de frecuencias para la transmisión data con una tasa máxima de 10 Mbps. Banda estrecha (NB) opera en el rango de frecuencias de 400, 800, 900 MHz y 2.3, 2.4 GHz. Comunicaciones del cuerpo humano (HBC) opera en 50 MHz. Ultra banda ancha (UWB) opera entre 3.1 GHz y 10.6 GHz soportando un alto ancho de bando en comunicaciones de corto alcance. La figura 22 muestra la topología de una red WBAN.

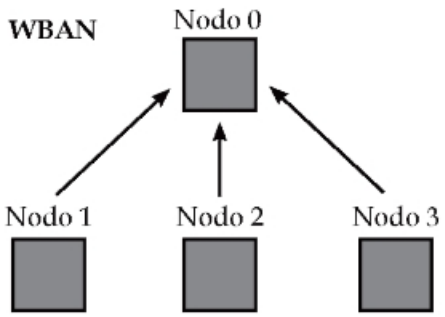


Figura 22. Topología red WBAN.
Tomado de (Tobón y Gaviria, 2012)

2.4.5.3.5 NFC (*Near Field Communication)*

NFC es una tecnología de comunicación inalámbrica de corto alcance cuya distancia es de alrededor de 4 pulgadas y opera en la frecuencia de 13.56 MHz a una velocidad de entre 160 kbps y 424 kbps. La combinación de NFC con dispositivos inteligentes permite el intercambio de información, descubrimiento

de servicios, señales de conexión, pagos electrónicos y venta de entradas. Se espera que a futuro reemplace a las tarjetas de crédito en pagos electrónicos (Eun, Lee y Oh, 2013). La figura 23 muestra la topología de una comunicación NFC.

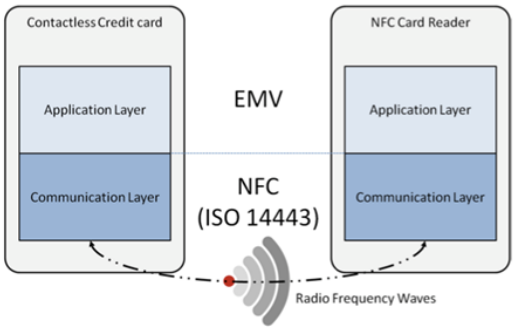


Figura 23. Topología de red NFC.
Tomado de (Acosta, 2014)

2.4.5.3.6 LoRa - LoRaWAN

La empresa Cat Sensors (2019) señala que LoRa es una tecnología inalámbrica altamente utilizada para conexiones en redes IoT donde se utilizan gran cantidad de dispositivos vestibles y sensores sin necesidad de corriente eléctrica de red. Esta tecnología utiliza una modulación denominada *Chirp Spread Spectrum* (CSS) que se emplea comúnmente en comunicaciones militares y espaciales.

Entre sus principales características se encuentran la alta tolerancia a interferencias, bajo consumo de batería, conexión punto a punto y su frecuencia de trabajo es de 868 MHz en Europa, 915 MHz en América y 433 MHz en Asia.

LoRa utiliza el protocolo de comunicación LoRaWAN para la comunicación entre sus dispositivos, este está compuesto de *gateways* que reciben y envían la información y nodos que son los dispositivos finales interconectados. La figura 24 muestra la topología de red LoRaWAN.

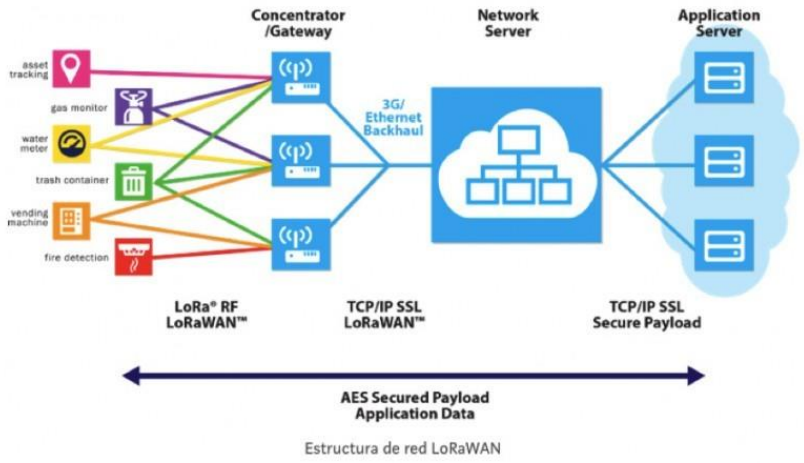


Figura 24. Topología de Red LoRaWAN.
Tomado de (Cat Sensors, 2019)

2.4.5.4 Aplicaciones de las redes WBAN

2.4.5.4.1 Medicina

En el campo de la medicina las redes WBAN son muy utilizadas, especialmente para la conectividad de dispositivos o sensores vestibles, esta tecnología mejora la eficiencia de las actividades e interacción entre médicos y pacientes, un ejemplo de ello es el monitoreo remoto del paciente, donde los sensores que pueden ser vestidos por el paciente implantados dentro del cuerpo del mismo, envían datos de diferentes órganos como el ritmo cardíaco, temperatura corporal, presión sanguínea, e incluso los movimiento del paciente. Toda la información recolectada es monitoreada y enviada a la unidad de control para su almacenamiento y al dispositivo del médico. Además, en caso de alguna emergencia, pueden emitir notificaciones y alertas o llamadas a emergencias o al teléfono del doctor en cualquier momento y lugar. La figura 25 muestra un reloj inteligente utilizado en la medicina para obtener el pulso cardíaco del usuario o paciente.

Figura 25. Tecnología Vestible WBAN en la Medicina.
Tomado de (Veredict, 2009)

2.4.5.4.2 Deportes

Las redes WBAN junto con dispositivos vestibles permiten monitorear efectivamente actividad fisiológica como temperatura, ritmo cardíaco, ritmo respiratorio, presión sanguínea, actividad física y postura de cualquier atleta en el campo de los deportes, de este modo los equipos deportivos pueden tomar decisiones más acertadas respecto a las actividades de los deportistas como decidir su adecuado plan de alimentación entrenamiento, entre otros y así mejorar su rendimiento en el campo. La figura 26 muestra chalecos inteligentes utilizados en el deporte.

Figura 26. Tecnología Vestible WBAN en el Deporte.
Tomado de (Catapult, 2020)

2.4.5.4.3 Milicia

Las oportunidades de la utilización de redes WBAN y dispositivos vestibles son numerosas. En un campo de batalla, se puede utilizar estos dispositivos para la comunicación entre soldados y enviar sus actividades de movimiento a un centro de control. Además, estos dispositivos permiten monitorear la condición de cada soldado, ubicación, ambiente, calidad del aire, radiación, condición física y médica, entre otros datos. Todos estos elementos pueden ser vestidos, implantados en el uniforme militar y la información transmitida a través de la red WBAN. La figura 27 muestra algunos dispositivos vestibles utilizados en la milicia.

Figura 27. Tecnología Vestible WBAN en Milicia.
Tomado de (Terahertz Technology, 2016)

2.4.5.4.4 Vida Cotidiana y Entretenimiento

Las redes WBAN permiten algunos servicios básicos como ayuda en la navegación mientras se camina, maneja o explora nuevas ciudades, entre otros beneficios como el monitoreo de bebes, activación remota del televisor, llamadas desde un dispositivo vestible como un reloj inteligente, reproducción de videos o música desde dispositivos portátiles en el televisor o equipo de música. La figura 28 muestra la utilización de un reloj inteligente en la vida diaria.

Figura 28. Tecnología vestible en la vida diaria.
Tomado de (Ingram, 2017)

2.4.5.4.5 Educación

Las redes WBAN son necesarias para la comunicación de los dispositivos vestibles utilizados en la educación como los *Google Glass*, guantes de aprendizaje de piano, entre otros con un teléfono inteligente. Esto permite que los datos enviados por los dispositivos vestibles puedan ser procesados por el teléfono y/o viceversa, es decir que el *smartphone* envíe datos como instrucciones o información a ser emitida en los dispositivos vestibles. La figura 29 muestra un dispositivo *Google Glass* utilizado para el aprendizaje.

Figura 29. Redes WBAN en la educación.
Tomado de (El País, 2015)

2.5 Seguridad en dispositivos vestibles

Para el ofrecimiento de las diferentes aplicaciones, los dispositivos vestibles dependen de protocolos de comunicación inalámbrica como se mencionó anteriormente. Desafortunadamente, ciertas características limitadas como batería, CPU, memoria y tamaño de los dispositivos limitan la implementación de medidas de seguridad avanzadas. (Seneviratne et al., 2017)

2.5.1 Vulnerabilidad

Según Cisco (2020) una vulnerabilidad de seguridad es una debilidad no intencionada en un producto que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad del dispositivo.

2.5.2 Amenaza

El Centro de Recursos de Seguridad Informática de los Estados Unidos CSRC (2020) define una amenaza o ciberamenaza como cualquier circunstancia o evento con el potencial de impactar adversamente las operaciones organizacionales o individuales a través de un sistema informático a través de acceso no autorizado, destrucción, modificación de información y/o denegación de servicio.

2.5.3 Riesgo

Cisco (2019) define al ciberriesgo como la exposición al daño o perdida resultante de violaciones o ataques a los sistemas informáticos. En el entorno operativos, otra definición es el potencial de pérdida o daño relacionado con la infraestructura técnica o el uso de tecnología dentro de la organización en general.

2.5.4 Propiedades de Seguridad

Chen et al. (2017) proponen cinco propiedades importantes para tomar en cuenta a la hora de analizar la seguridad informática, estos son integridad, confidencialidad, disponibilidad, autenticación y autorización. Además, Cryptomathic (2020) propone una propiedad adicional, el no repudio. Cada uno de estos parámetros son ampliados a continuación.

2.5.4.1 Confidencialidad

La confidencialidad asegura que la información sensible sea accedida únicamente por personas autorizadas y mantenida alejada de quienes no están autorizados a poseerla. La confidencialidad se implementa utilizando listas de control de acceso y encripción. De igual manera, es común categorizar la información en base a la extensión del daño que esta pueda sufrir al caer en manos malintencionadas. (Cisco, 2020)

2.5.4.2 Integridad

Según Cisco (2020), la integridad asegura que la información se encuentre en un formato verdadero y correcto para sus propósitos originales. El receptor debe tener únicamente la información que el autor pretende que reciba y puede ser editada únicamente por personas autorizadas y permanecer en su estado original el resto del tiempo. La integridad se implementa por medio de la utilización de mecanismos de seguridad como encripción y *hashing*.

2.5.4.3 Disponibilidad

Cisco (2020) indica que la disponibilidad busca asegurar que la información y los recursos se encuentren disponibles para quienes la necesiten. Para su implementación, se utilizan métodos como mantenimiento de hardware, parches de software y optimización de red. Adicionalmente, se utilizan procesos como la

redundancia, conmutación, RAID y clústeres de alta disponibilidad para mitigar consecuencias serias en caso de ocurrir problemas de hardware.

2.5.4.4 Autenticación

La autenticación se encarga de verificar y diferenciar las identidades que tienen permiso de acceder a las entidades. En los dispositivos vestibles, los protocolos de autenticación juegan un rol importante en la comunicación mutua entre entidades. (Chen et al., 2017)

2.5.4.5 Autorización

La autorización permite definir el proceso de concesión, denegación y restricción del acceso a las entidades. Su esquema se encarga de realizar diferentes operaciones conforme a las diferentes entidades. (Chen et al., 2017)

2.5.4.6 No Repudio

Según Cryptomathic (2020) el no repudio es la capacidad de asegurar que alguien no pueda negar la validez de algo. Este concepto se utiliza ampliamente en la seguridad de la información y se refiere a un servicio que provee pruebas del origen e integridad de la información. Es decir, el no repudio permite la identificación exitosa de quien envió y desde donde provino el mensaje, así como la autenticidad e integridad del mismo. Las firmas digitales combinadas con otras medidas ofrecen esta propiedad al momento de realizar transacciones en línea, donde es indispensable asegurar que una parte en un contrato o comunicación no pueda negar la autenticidad de su firma en un documento o envío de información.

2.5.5 Cibercrimen

Sabillon, Cano, Cavaller y Serra (2016) asegura que el cibercrimen no puede ser descrito como una definición singular, debe ser considerado como una colección de actividades ilegales donde un dispositivo digital o sistema de información es una herramienta, objetivo o una combinación de ambos. Estos actos se basan en el objeto material del delito y el modus operandi que afectará a la información y/o sistema. La expresión puede ser también conocida como crimen computacional, crimen electrónico o crimen digital.

2.5.6 Ciberatacantes o Hackers

El término hacker ha cambiado a través de las últimas décadas, la conceptualización de las actividades realizadas por este grupo de individuos es generalmente vista como oscura o malvada, operando en ambientes subterráneos y particularmente con intenciones de causar daño contra los sistemas de información de la sociedad. (Sabillon et al. 2016) Los motivos de estos individuos pueden ser desde diversión personal, reconocimiento hasta efectivamente el crimen.

2.5.6.1 Categorías de ciberatacantes

2.5.6.1.1 Sombrero Blanco

Este tipo de atacantes trabajan bajo las leyes de la ética, es decir no causar daño, generalmente son expertos en ciberseguridad.

2.5.6.1.2 Sobrero Gris

Este grupo lo conforman individuos de sombrero negro que han sido reformados y ahora trabajan como consultores de seguridad.

2.5.6.1.3 Sobrero Negro

Dentro de este grupo, se encuentran los motivados por el poder, enojo u odio. No tienen escrúpulos para robar o destruir la información de las redes que ellos han vulnerado.

2.5.6.2 Clases de ciberatacantes

Las siguientes clases de atacantes se encuentran dentro de las categorías de sombrero blanco y negro. Savillon et al. (2016) los clasifican de la siguiente manera:

2.5.6.2.1 Atacantes de Élite

Tienen el conocimientos y destrezas del más alto nivel. Este reconocimiento puede ser obtenido a través de un ataque famoso o longevidad en el área.

2.5.6.2.2 Niños de Guion (*Script Kiddies*)

Este subgrupo es el más despreciado dentro de la comunidad. Suelen ser los miembros menos capacitados y más jóvenes en utilizar herramientas creadas por hackers de élite.

2.5.6.2.3 Ciberterroristas

Estos individuos utilizan sus habilidades para intercambiar información relacionada al crimen, causar miedo y ruptura. Algunos de estos comparten virus a través de la red y otros amenazan y extorsionan personas electrónicamente.

2.5.6.2.4 Exempleados

Uno de los más peligrosos y menos publicitados. Este grupo cree que debió ser reconocido de mejor manera por su trabajo empresarial y busca tomar venganza por no haberlo recibido.

2.5.6.2.5 Desarrolladores de Virus

Este grupo tiende a explotar debilidades encontradas por otros atacantes, a través de la escritura de códigos a ser ejecutados en los dispositivos víctimas.

2.5.6.2.6 Hacktivistas

Su nombre deriva de la combinación de las palabras activismo y hacking. Unos de los subgrupos de atacantes que han crecido más rápidamente, su motivación consiste en ejecutar ataques de denegación de servicio con el fin de satisfacer sus agendas políticas, religiosas y sociales.

El consejo de consultores de comercio electrónico EC-Council (2014) ha creado una clasificación diferente donde se incluyen algunas otras clases de atacantes descritas a continuación.

2.5.6.2.7 Hackers Suicidas

Este grupo pretende causar daños en infraestructuras críticas por causas radicales y no temen ser arrestados y encarcelados. Tienen una alta relación con terroristas suicidas y son miembros activos de los grupos de ciberterrorismo.

2.5.6.2.8 Hackers Espías

Este grupo de atacantes son contratados por empresas con el objetivo de vulnerar y obtener secretos comerciales de los colaboradores de las empresas con las cuales compiten quien los contrató.

2.5.6.2.9 Hackers Patrocinados por el Estado

Estos atacantes son patrocinados por los gobiernos de estados para atacar las redes y sistemas de información de otros países.

2.5.6.2.10 Hackers Etiquetadores

Warren y Leitch (2009) han creado una categoría adicional que no ha sido considerada anteriormente, llamados hackers etiquetados. Estos individuos buscan desfigurar sitios web con la intención de dejar una etiqueta que es actualizada periódicamente para mostrar el score individual del atacante.

3 CAPÍTULO III. DESARROLLO

En el presente capítulo, se realizará un análisis de la seguridad y privacidad que involucra a los dispositivos vestibles. Además, se plantearán parámetros de análisis que permitirán alcanzar los objetivos de este documento que tiene como fin, identificar los principales riesgos y amenazas de seguridad y privacidad que representa la utilización de dichos dispositivos.

3.1 Metodología

Se realizará una investigación teórica utilizando los métodos inductivo y descriptivo con un enfoque integrado multimodal. La investigación teórica permite obtener conocimientos de diferente tipo basándose en conocimientos obtenidos de investigaciones previas. El método inductivo se basa en la

obtención de conclusiones partiendo desde la observación de los hechos, en este caso ataques previos a dispositivos vestibles. El método descriptivo establece una descripción completa de un evento o elemento, mostrando sus características principales. El enfoque integrado multimodal integra al enfoque cuantitativo que permite recolectar y analizar datos estadísticos de usuarios y dispositivos afectados junto con el enfoque cualitativo que ofrece una valoración cualitativa de las vulnerabilidades y ataques sufridos.

3.2 Parámetros por analizar

Los parámetros por analizar son la base fundamental del estudio que se realizará en el capítulo cuatro, por lo tanto, es indispensable explicar adecuadamente en qué consisten los mismos. Dichos parámetros se encuentran inmiscuidos dentro de dos modelos de análisis a través de los cuales se evaluarán varios tipos de ataques. Toda esta información se profundizará a continuación.

3.2.1 Modelo DREAD

Los autores Tseng, Wu y Lai (2019) plantean el modelo DREAD, mismo que sus siglas en inglés representan Daño, Reproducibilidad, Explotabilidad, Afectación y capacidad de Descubrimiento como se describe en la Tabla 2. Este modelo permite calcular el riesgo de cada amenaza. Los niveles de severidad son asignados a las amenazas de la siguiente manera:

- Bajo: 5 a 7
- Medio: 8 a 11
- Alto 12 a 15

Tabla 2.

Modelo DREAD

Amenaza	**Alto (3)**	**Medio (2)**	**Bajo (1)**
Daño	El atacante puede ignorar el mecanismo de protección del sistema de seguridad y obtener autorización del administrador para ejecutar programas arbitrariamente.	El atacante puede obtener información sensible del usuario.	El atacante puede obtener solo información general de identificación.
Reproducibilidad	El ataque puede ser realizado varias veces y ejecutado en cualquier momento sin restricción.	El ataque puede ser repetido únicamente en una situación particular o punto en el tiempo.	A pesar de existir vulnerabilidades de seguridad conocidas o la complejidad técnica sea muy alta, es difícil repetir el ataque.
Explotabilidad	Un atacante novato puede realizar el ataque directamente utilizando scripts o herramientas simples.	Un atacante con cierta experiencia puede realizar el ataque pero se requiere conocimiento técnico relevante.	Requiere la experiencia de un profesional en seguridad informática con un alto conocimiento del ataque.
Afectación	Todos los usuarios se ven afectados.	Solo se ven afectados algunos usuarios.	Afecta únicamente a un pequeño porcentaje de usuarios y puede ser recuperado rápidamente.

Descubrimiento	La información de la vulnerabilidad está definida por niveles de severidad, se encuentra expuesta públicamente y es fácil de implementar repetidamente.	La vulnerabilidad existe en un servicio que es raramente utilizado y su impacto es muy bajo que requiere información específica para identificarla.	El ataque a la vulnerabilidad es leve. Su implementación requiere condiciones específicas y es extremadamente difícil de detectar.

Tomado de: (Tseng et al., 2019, p.9)

3.2.1.1 Coeficiente Kappa

Con el fin de analizar los resultados obtenidos del modelo DREAD a través de encuestas a dos expertos, se considera necesario evaluar la concordancia entre sus valoraciones, para lo cual se utilizará el coeficiente Kappa.

Según la Sociedad Andaluza de Medicina Intensiva y Unidades Coronarias (2020), el coeficiente de Kappa propuesto por Jacob Cohen en 1960 se refiere a una medida estadística que permite comparar la concordancia observada por dos evaluadores en un grupo de datos, en comparación a lo que podría suceder por azar.

La ecuación utilizada para obtener el coeficiente Kappa (K) es la siguiente:

$$K = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)}$$

Donde, Pr (a) se refiere al acuerdo observado entre los evaluadores y Pr (e) es la probabilidad de acuerdo por azar. En caso de existir un completo acuerdo entre los dos evaluadores, el coeficiente K será igual a 1, caso contrario se acercará a 0 o incluso a valores negativos en una tabla 2 * 2. La tabla 3 muestra

la fuerza de acuerdo propuesta por Landis y Koch (1977) en base al coeficiente kappa.

Tabla 3.

Fuerza de Acuerdo Kappa

Coeficiente Kappa	**Fuerza de Acuerdo**
<0	Nula
0.0-0.2	Pobre
0.2-0.4	Débil
0.4-0.6	Moderada
0.6-0.8	Buena
0.8-1.0	Muy buena

Tomado de: (Landis y Koch, 1977)

3.2.2 Modelo STRIDE

Para identificar las amenazas, es necesario clasificarlas en las siguientes categorías mostradas en la Tabla 4. El proceso de identificación de amenazas utiliza el modelo STRIDE para clasificarlas y examinar sus aspectos de seguridad. El modelo STRIDE clasifica las amenazas de acuerdo con el objetivo y el propósito del ataque, lo que ayuda a desarrollar políticas de seguridad. (Tseng et al., 2019)

Tabla 4.

Modelo STRIDE

Amenaza	**Propiedad de Seguridad**	**Descripción**	**Acción**
Suplantación de Identidad	Autenticación	Acceso no autorizado al sistema utilizando una identidad ilegal o información errónea para engañar al sistema.	Esta amenaza utiliza las credenciales de otros usuarios legítimos para autenticarse en el sistema y acceder a la información.

Manipulación	Integridad	Modificación malintencionada no autorizada de la información para engañar al receptor.	Permite modificar la información a ser almacenada en bases de datos, sistemas de archivos o tráfico de red.
Repudio	No repudio	El usuario declara no haber y no poder realizar algún acción	El sistema no tiene la habilidad de rastrear las actividades del usuario
Divulgación de Información	Confidencialidad	La información es divulgada a usuarios no autorizados	Permite el acceso a archivos o data no autorizada en tránsito.
Denegación de Servicio	Disponibilidad	Deniega o interrumpe el acceso de los usuarios a las aplicaciones o servicios.	Deniega el acceso a usuarios válidos a bases de datos y aplicaciones temporalmente no disponibles.
Elevación de privilegio	Autorización	Usuarios con permisos limitados puede utilizar la aplicación para obtener permisos sin autorización.	Obtener permisos de acceso a los recursos con el fin de acceder o dañar la información.

Tomado de: (Tseng et al., 2019, p.10)

3.3 Tipos de Ataques

El mundo de los dispositivos vestibles representa un peligro para los usuarios debido al alto riesgo cibernético. Ellos están compartiendo masivamente información personal como por ejemplo ubicación, horarios, estado físico, estado de salud, preferencias, entre otros en sus diferentes dispositivos vestibles como relojes, bandas, sensores, etc. Así, se vuelven una gran atracción para los

hackers quienes buscan nuevas técnicas de ataque con el fin de obtener esa información y utilizarla a su conveniencia.

Los diferentes tipos de ataques a los dispositivos vestibles son el principal punto de análisis de este documento, por lo tanto, es importante entender su comportamiento. A continuación, se describirá cada uno de los tipos de ataques a los que se encuentran expuestos estos dispositivos.

3.3.1 Ataques por emparejamiento *Bluetooth*

El análisis de literatura identificó que existen varias clases de ataques en y alrededor del uso de la conectividad *Bluetooth*. Cusack et al. (2017) mencionan que para orientar su investigación y hacerla más realizable en el laboratorio, han seleccionado dos clases de ataques y cinco ataques específicos resaltados en azul en la figura 30.

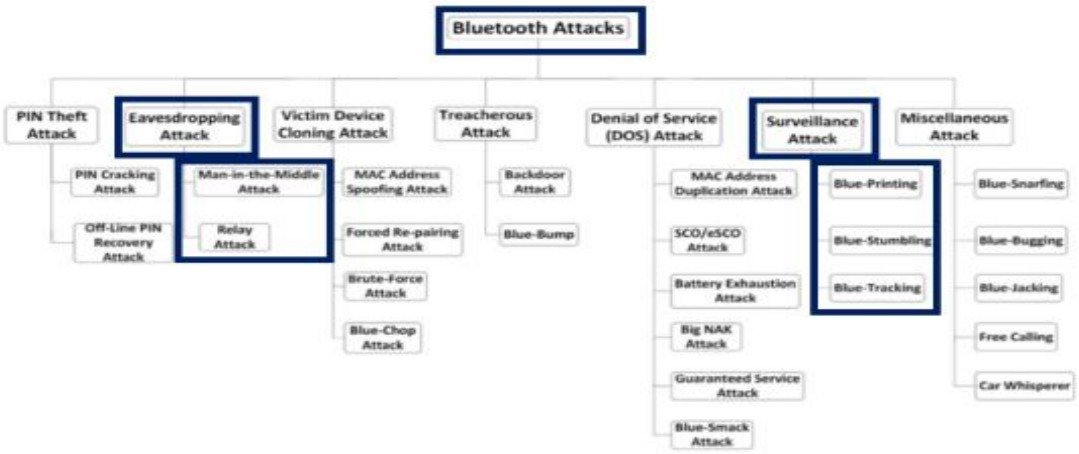


Figura 30. Clasificación de los ataques *Bluetooth*.
Tomado de (Hassan et al., 2017)

Los autores antes citados, señalan que el estudio de tres dispositivos vestibles elaborado por Lotfy y Hale (2016) determinó que la seguridad de las técnicas de emparejamiento tiene importantes grietas de seguridad y potenciales vulnerabilidades que incluyen ataques de hombre en el medio (*man in the*

middle), espionaje e inyección de paquetes. A través de estos tipos de ataques, los atacantes tienen la capacidad de espiar activamente dispositivos portátiles y hacer mal uso de la información.

Con respecto a los ataques de vigilancia, Cusack et al. (2017) los han clasificado de la siguiente manera:

- Impresión Azul (*Blue Printing*): Se refiere a la suplantación de direcciones MAC con el fin de ejecutar un ataque *man in the middle*.

- Tropiezo Azul (*Blue Stumbling*): Se trata de un ataque de re-emparejamiento forzado.

- Seguimiento Azul (*Blue Tracking*): Permite determinar la llave de encripción a través de fuerza bruta.

3.3.2 Inyección de Código

Según Farooq, Wasseem, Khairi y Mazhar (2015) este ataque introduce código malicioso en el sistema explotando errores de programación. La inyección de código puede ser utilizada para una gran variedad de propósitos, como por ejemplo para robar información, tomar control del sistema y en la propagación de gusanos. Los ataques más comunes de este tipo incluyen la inyección de *shell* y *scripts* HTML. Este tipo de ataque puede causar la pérdida del control de la aplicación y comprometer la privacidad del usuario.

3.3.3 Desbordamiento de búfer

Este ataque implica la violación de los límites del código o el búfer de datos al explotar las vulnerabilidades de la aplicación. Muchas aplicaciones operan con un diseño predefinido de memoria que contiene segmentos de código y datos. El atacante escribe una secuencia larga de datos en un área específica,

obteniendo como resultado un desbordamiento de la secuencia más allá de su región predefinida de residencia. El resultado puede ser la modificación de otros datos, la ejecución de código malicioso y la destrucción del flujo de control de la aplicación. (Zhu, Joseph y Sastry, 2011)

3.3.4 Manipulación de información sensible

Jia et al (2017) mencionan que este tipo de ataque hace referencia al acceso ilegal y manipulación de la información sensible manejada por los dispositivos vestibles, violando de este modo la privacidad del usuario. Fernandes, Jung y Prakash (2016) han analizado los eventos utilizados para la comunicación entre el dispositivo vestible y la aplicación. El dispositivo vestible envía información sensible a la aplicación mediante eventos, mismos que son utilizados por la aplicación para monitorear el dispositivo vestible. Sin embargo, a causa de la carencia de protección suficiente en el envío del evento, puede provocarse una filtración del mismo e incluso mayor daño al consumidor. Adicionalmente, a causa de la falta de protección adecuada de las entradas del usuario, la privacidad de este puede verse violada. (Nan et al., 2015)

3.3.5 Suplantación de Identidad (*Phishing*)

En este tipo de ataque, el atacante procura ser un usuario real o legítimo para obtener información sensible acerca de los usuarios, como por ejemplo las contraseñas. El medio común de este tipo de ataques es mediante el correo electrónico, donde la información sensible es adquirida por el atacante cuando el usuario abre el correo electrónico. (Farooq et al., 2015)

3.3.6 Autenticación y Autorización

El mecanismo de autenticación juega un rol importante en la protección de la seguridad y privacidad de los dispositivos. Los mecanismos actuales de autenticación no proveen una verificación adecuada. (Simmons et al., 2009). Por

ejemplo, las aplicaciones pueden descargar códigos maliciosos al momento de actualizarse y los atacantes utilizarla con el objetivo de controlar de manera remota el terminal. (Chang y Hwang, 2003). Además, Simmons et al. (2019) insinúa que mantener la configuración predeterminada es también parte del origen del problema de permitividad. Asimismo, cuando a un archivo y directorio se les proporciona permisos inapropiados, el atacante puede explotar la vulnerabilidad.

3.3.7 Inundación en la nube

Según Gruschka y Jensen (2010) este es una forma de ataque de denegación de servicio en la nube. Allí, los atacantes envían solicitudes constantemente a un servicio en la nube, agotando los recursos y afectando a la calidad del servicio. Además, cuando el sistema de *cloud* se da cuenta que la actual instancia no cumple los requisitos, lo transfiere a otros servidores e incrementa su carga de trabajo.

3.3.8 Inyección de *malware* en la nube

El atacante puede modificar la información, obtener control y ejecutar códigos maliciosos al inyectar una instancia de un servicio malicioso o máquina virtual en la nube (Padhy, Patra y Satapathy, 2011). En el artículo de Gruschka y Jensen (2010) se menciona que los atacantes copian y cargan la instancia de servicio de una víctima, pero con la diferencia que la instancia maliciosa responde a la petición cuando algún servicio solicita la instancia de la víctima. Como resultado, el atacante obtiene la información sensible del servicio.

3.3.9 Envoltura de firma

El sistema cloud utiliza la firma XML para garantizar la integridad del servicio. El atacante altera los mensajes escuchados sin invalidar la firma. (Jensen,

Schwenk, Gruschka y Iacono, 2009). De este modo, el atacante puede ejecutar comandos arbitrarios y operaciones como usuario legítimo.

3.3.10 Inyección SQL

La incorporación de sentencias SQL en los datos de entrada, permite a una aplicación mal diseñada convertirse en un blanco vulnerable a ataques (Zhang y Wang, 2009). Los atacantes usan sentencias SQL para operaciones de lectura, escritura y eliminación. Este tipo de ataque no solo permite la obtención de datos privados del usuario, sino también representa una amenaza para todo el sistema de la base de datos. Al momento en que las aplicaciones web son atacadas por inyección SQL, la página actual muestra resultados diferentes en comparación con la información verdadera. (Dorai y Kannan, 2011)

3.3.11 Denegación de Servicio (DoS)

Un ataque de denegación de servicio se logra llenando a la víctima con peticiones que generan una gran cantidad de tráfico. (Sastry, Sulthana y Vagdevi, 2013). Este tipo de ataque agota todos los recursos disponibles y permite que los mismos se vuelvan inaccesibles al usuario. Además, mucha información no encriptada puede ser filtrada. (Farroq et al., 2015). También, un ataque distribuido de denegación de servicio (DDoS) puede convertir varios dispositivos en una plataforma de ataque y ejecutar ataques DDoS hacia uno o más blancos.

3.3.12 Sybil

El ataque Sybil consiste en que un nodo atacante presenta múltiples identidades al nodo víctima, lo que permite al nodo afectado ejecutar una operación múltiples ocasiones, evitando así la redundancia. (Douceur, 2002). En las redes de dispositivos vestibles, al momento que el atacante tiene múltiples identidades, el

nodo víctima puede transmitir información a través del nodo comprometido hacia el atacante. (Sastry et al., 2013)

3.3.13 Sumidero (*Sinkhole*)

Según Farroq et al. (2015) el atacante utiliza un nodo comprometido para atraer el flujo de información de otros nodos cercanos. El sistema está engañado y considera que la información ha llegado a su destino. A su vez, Sastry et al. (2013) menciona que la información obtenida por el atacante una vez que este la obtiene puede operar arbitrariamente con ella.

3.3.14 Olfateo (*Sniffing*)

Los autores Welch y Lathrop (2003) consideran que los atacantes utilizan dispositivos y aplicaciones *sniffer* con el fin de obtener información de la red y extraer información valiosa para posteriormente ejecutar otro ataque.

3.3.15 Análisis de Tráfico

Babar, Stango, Prasad, Sen y Prasad (2011) mencionan que, para efectuar este ataque, los atacantes deducen el patrón y carga de la comunicación, para ello analizan el número y tamaño de los paquetes de información transmitida, a mayor número de paquetes analizados, mayor información valiosa disponible. Este tipo de ataque se puede aplicar para la encripción de paquetes. Según Welch y Lathrop (2003) se puede obtener tres tipos de información a través del análisis de tráfico. Primeramente, el atacante detecta la actividad en la red. En segundo lugar, procede a obtener la dirección MAC del punto de acceso inalámbrico. Finalmente, adquiere la información del protocolo utilizado en la transmisión.

3.3.16 Repetición (*Replay)*

Mitrokotsa, Rieback y Tanenbaum (2010) señalan que los atacantes obtienen información entre las partes comunicantes por medio de espionaje. Los mensajes recibidos se transmiten repetidamente entre las partes, causando el agotamiento de los recursos de comunicación. Asimismo, Ding, Li y Feng (2008) sugieren que en la tecnología RFID, este ataque ocurre en la comunicación entre el lector y el tag RFID, consumiendo recursos además de la base de datos.

3.3.17 Hombre en el Medio (*Man in the Middle*)

Este tipo de ataque es un ataque es un ataque de tiempo real, ocurre mientras se comunican dos nodos o dispositivos víctimas. El atacante oculta un nodo como un dispositivo genuino que se comunica con dos nodos víctima y obtiene la confianza de los dos dispositivos, esto le permite obtener la información de ambos. (Hossain, Fotouhi y Hasan, 2015)

3.3.18 Privación del sueño (*Sleep Deprivation*)

Según los autores Bhattasali, Chaki y Sanyal (2012) los dispositivos vestibles son limitados en el poder de su batería, por lo tanto, para alargar su tiempo de vida, es necesario que entren en estado de reposo cuando no están funcionando. Este tipo de ataque busca alterar este proceso, enviando constantemente información de control al dispositivo y manteniendo el nodo en un estado de trabajo.

4 CAPÍTULO IV. ANÁLISIS

Considerando lo desarrollado en el capítulo 2, donde se describió la información teórica y en el capítulo 3, donde se profundizó la investigación teórica con el fin de describir los principales parámetros a analizar acerca de la seguridad de los dispositivos vestibles, se procederá a crear tablas analíticas utilizando los

modelos DREAD y STRIDE descritos en el capítulo anterior para conceder al lector una visión más clara de las diferentes amenazas y ataques a las que se pueden ver expuestos al utilizar dispositivos vestibles, para que los mismos sean conscientes de estos aspectos al momento de adquirirlos. Además, se realizará el análisis de concordancia de los resultados obtenidos del modelo DREAD utilizando el coeficiente Kappa de Cohen. Finalmente, se procederá a crear una tabla en la cual se muestren algunas recomendaciones de seguridad frente a las amenazas analizadas.

Al existir diferentes tipos de ataques, con características y propósitos distintos, se procederá a realizar tablas separadas por los modelos de análisis, es decir se comparará los 18 ataques en base a los parámetros de análisis descritos en el capítulo 3. De este modo, se mostrarán tablas y gráficos fácilmente legibles e interpretables para el lector, lo que permitirá representar de manera más clara los resultados obtenidos.

4.1 Análisis Modelo DREAD

Las tablas 5 y 6 se basan en el modelo DREAD y muestran los resultados de la encuesta realizada a dos evaluadores con vasta experiencia en el tema de seguridad de la información, estas permitirán calcular el riesgo de cada ataque a través de parámetros como Daño (D), Reproducibilidad (R), Explotabilidad (E), Afectación (A) y Capacidad de Descubrimiento (D), donde se calificará cada aspecto en una escala de 1 a 3 para finalmente obtener un total en una escala de 5 a 15 que permitirá decidir el nivel de riesgo, siendo este bajo, medio o alto.

Tabla 5.

Análisis Modelo DREAD Evaluador 1

Ataque	**D**	**R**	**E**	**A**	**D**	**Total**	**Riesgo**
Emparejamiento Bluetooth	2	3	2	2	2	11	Medio
Inyección de Código	2	2	2	3	3	12	Alto
Desbordamiento de búfer	1	2	1	3	2	9	Medio

Manipulación de información sensible	3	3	3	3	2	14	Alto
Phishing	3	3	3	3	3	15	Alto
Autenticación y Autorización	2	2	2	3	1	10	Medio
Inundación en la nube	1	1	1	3	2	8	Medio
Inyección de *malware* en la nube	1	1	1	3	2	8	Medio
Envoltura de firma	1	1	1	1	1	5	Bajo
Inyección SQL	3	2	1	2	3	11	Medio
Denegación de Servicio	3	3	2	3	3	14	Alto
Sybil	2	2	2	2	1	9	Medio
Sinkhole	1	1	1	2	1	6	Bajo
Sniffing	2	3	2	2	2	11	Medio
Análisis de tráfico	2	3	2	2	2	11	Medio
Replay	1	1	1	2	1	6	Bajo
Man in the middle	1	1	1	2	2	7	Bajo
Sleep Deprivation	1	3	2	2	2	10	Medio

Adaptado de: (Tseng et al., 2019, p.9)

Tabla 6.

Análisis Modelo DREAD Evaluador 2

Ataque	**D**	**R**	**E**	**A**	**D**	**Total**	**Riesgo**
Emparejamiento Bluetooth	3	3	2	2	2	12	Alto
Inyección de Código	2	3	3	3	2	13	Alto
Desbordamiento de búfer	1	1	2	2	3	9	Medio
Manipulación de información sensible	3	3	2	3	3	14	Alto
Phishing	3	3	3	3	3	15	Alto
Autenticación y Autorización	2	2	2	2	1	9	Medio
Inundación en la nube	1	1	1	2	2	7	Bajo
Inyección de *malware* en la nube	1	1	1	3	2	8	Medio
Envoltura de firma	1	1	1	1	1	5	Bajo
Inyección SQL	3	2	2	2	3	12	Alto
Denegación de Servicio	3	3	2	3	2	13	Alto

Sybil	1	2	2	1	2	8	Medio
Sinkhole	1	1	2	1	1	6	Bajo
Sniffing	2	1	2	3	3	11	Medio
Análisis de tráfico	3	2	2	2	3	12	Alto
Replay	1	1	2	2	1	7	Bajo
Man in the middle	2	2	3	2	1	10	Medio
Sleep Deprivation	3	2	2	3	2	12	Alto

Adaptado de: (Tseng et al., 2019, p.9)

La figura 31 muestra gráficamente los resultados obtenidos a través del modelo DREAD. Es decir, se puede observar la calificación total de riesgo de cada evaluador para cada uno de los ataques analizados.

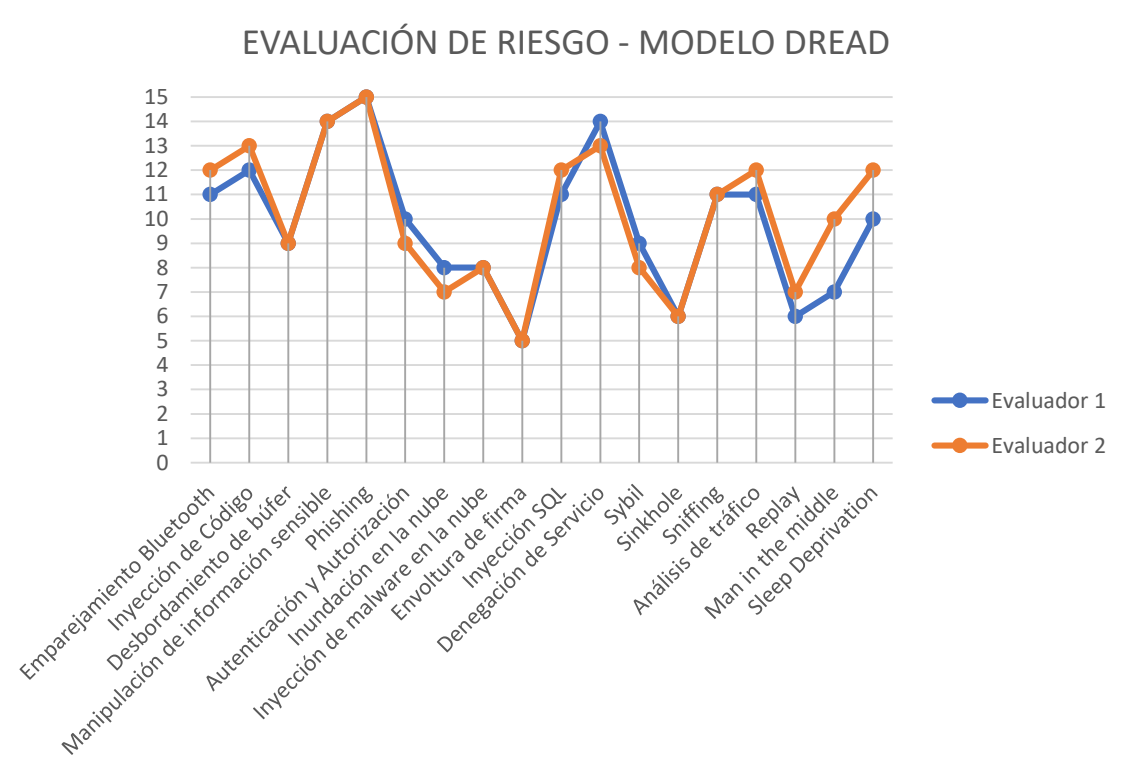


Figura 31. Estadísticas Modelo DREAD

Los resultados obtenidos muestran que el ataque más peligroso para los dispositivos vestibles es el ataque de *Phishing* o Suplantación de Identidad con la calificación de riesgo más alta, es decir 15. A través de este ataque, se puede

ignorar el mecanismo de protección del sistema, ejecutar código malicioso, modificar datos e incluso causar la pérdida del control de la aplicación y comprometer la privacidad del usuario. Además, puede ser realizado varias veces y en cualquier momento, incluso por un novato utilizando scripts o herramientas simples y fáciles de implementar que se encuentran expuestas públicamente en Internet, afectando de este modo a todos los usuarios del dispositivo víctima.

Por otro lado, el ataque menos riesgoso de los analizados es el ataque de envoltura de firma, este recibió una calificación de 5 por parte de ambos evaluadores, lo que lo ubica en el nivel de riesgo Bajo. A través de este ataque, se puede obtener solo información general de identificación, su complejidad técnica es alta y es difícil repetir el ataque. Además, se requiere la experiencia de un profesional con un alto conocimiento del ataque para ejecutarlo correctamente. Asimismo, la afectación sería únicamente a un pequeño porcentaje de usuarios y puede ser recuperado rápidamente.

4.1.1 Análisis de Concordancia Coeficiente Kappa

Una vez obtenidos los resultados de las encuestas realizadas a los expertos, se procede a evaluar la concordancia entre sus evaluaciones utilizando el coeficiente Kappa de Cohen. En la tabla 7 se observa la tabulación de los datos de concordancia entre los evaluadores.

Tabla 7.
Tabulación Datos Concordancia Coeficiente Kappa

	Evaluador 2			
Evaluador 1	Bajo	Medio	Alto	Total
Bajo	3	1	0	4
Medio	1	5	4	10
Alto	0	0	4	4
Total	4	6	8	18

Posteriormente, se han calculado las probabilidades de acuerdo observado y esperado como se muestra a continuación, obteniendo los resultados expuestos en la tabla 8.

$$\Pr(a) = \frac{3+5+4}{18} = 0.67$$

$$\Pr(e) = \frac{\frac{(4*4)+(10*6)+(4*8)}{18}}{18} = 0.33$$

Tabla 8. Cálculo de Probabilidades de Acuerdo

ACUERDO OBSERVADO Pr(a)	0.67
ACUERDO ESPERADO Pr(e)	0.33

Finalmente, se calculó el coeficiente de Kappa (K) obteniendo como resultado 0.5, esto quiere decir que la fuerza de acuerdo entre los dos evaluadores es moderada, reforzando los resultados obtenidos a través de las encuestas realizadas. Sin embargo, cabe destacar que los mismos pueden variar hasta cierto punto de acuerdo al criterio y experiencia de cada evaluador.

$$K = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)}$$

$$K = \frac{0.67 - 0.33}{1 - 0.33} = 0.5$$

4.2 Análisis Modelo STRIDE

La tabla mostrada a continuación se basa en el modelo STRIDE, este permitirá clasificar los ataques de acuerdo con el objetivo y el propósito del mismo, lo que ayudará a recomendar algunas políticas de seguridad. Esta tabla presentará una

equis (X) en la categoría o categorías a la que pertenezcan cada uno de los 18 ataques analizados. Las amenazas que se observan en las columnas de la tabla son: Suplantación de Identidad (S), Manipulación (T), Repudio (R), Divulgación de Información (I), Denegación de Servicio (D) y Elevación de Privilegio (E).

Tabla 9.

Análisis Modelo STRIDE

Ataque	**S**	**T**	**R**	**I**	**D**	**E**
Emparejamiento Bluetooth	X			X	X	X
Inyección de Código		X	X	X	X	X
Desbordamiento de búfer		X	X	X	X	X
Manipulación de información sensible		X		X		X
Phishing	X	X		X		
Autenticación y Autorización	X	X		X		X
Inundación en la nube					X	
Inyección de *malware* en la nube	X	X		X	X	X
Envoltura de firma	X	X	X	X		X
Inyección SQL		X		X	X	X
Denegación de Servicio				X	X	
Sybil	X			X	X	
Sinkhole	X	X		X		X
Sniffing			X			
Análisis de tráfico			X			
Replay	X			X	X	X
Man in the middle	X		X	X		
Sleep Deprivation					X	

La tabla 9 muestra como cada uno de los tipos de ataques analizados pueden pertenecer a más de una categoría de amenaza a las que son vulnerables los dispositivos vestibles. En este caso, se ha observado que la amenaza más importante a la que los dispositivos vestibles son vulnerables es la de divulgación de información, esta categoría vulnera una propiedad de seguridad muy

importante que es la confidencialidad de la información, divulgándola a usuarios no autorizados y permitiéndoles el acceso a archivos o data no autorizada. Se considera lo anterior porque por medio de 14 de los 18 diferentes tipos de ataques examinados, lo que representa el 77.78 %, se puede aprovechar las vulnerabilidades de los dispositivos vestibles y ejecutar dicha amenaza.

Por otro lado, la amenaza que puede ser menormente ejecutada por medio de los ataques analizados con el fin de vulnerar el dispositivo vestible es el repudio. Esto debido a que solo seis ataques, es decir un 33.33 % de la muestra pueden ejecutar esta amenaza vulnerando la propiedad de seguridad de no repudio, es decir que el usuario o dispositivo pueda renunciar a la responsabilidad de haber realizado alguna acción ya que los terminales a los que se conectan los dispositivos vestibles como los teléfonos inteligentes, tabletas o computadoras registran *logs* de las actividades del usuario y de comunicación entre terminales.

Sin embargo, es importante considerar las demás categorías de amenazas que se encuentran en un nivel parejo entre sí, la suplantación de identidad al igual que la manipulación de información cuentan con un total de 9 tipos de ataques (50 %) a través de los cuales pueden vulnerar las propiedades de seguridad de la autenticación e integridad respectivamente.

Además, las categorías de Denegación de Servicio y Elevación de Privilegios, amenazas que vulneran propiedades de seguridad como la disponibilidad y autorización respectivamente, presentan de igual forman un número alto de ataques a través de los cuales pueden aprovechar las vulnerabilidades de los dispositivos vestibles, siendo este un total de 10 tipos de ataques o 55.56 % de la muestra.

La figura 32 muestra de una manera gráfica la relación entre las categorías de amenazas y los diferentes tipos de ataques a través de los cuales los dispositivos vestibles pueden ser vulnerados. Es decir, permite observar a través de cuantos

tipos de ataques es posible ejecutar cada una de las categorías de amenazas analizadas.

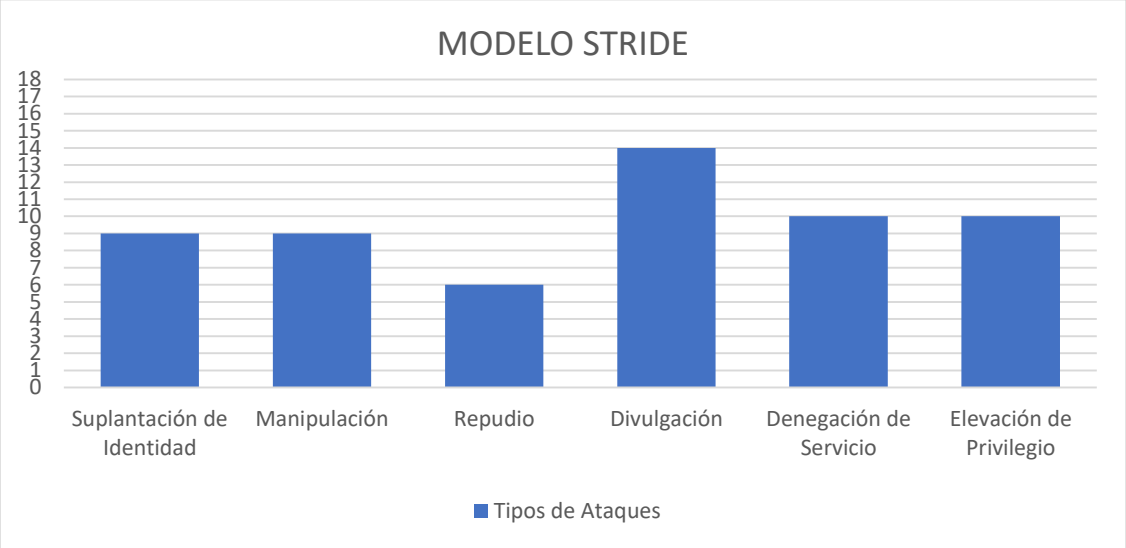


Figura 32. Estadísticas modelo STRIDE

4.3 Recomendaciones de Seguridad

Habiendo analizado cada uno de las amenazas, vulnerabilidades, riesgos y tipos de ataques de los que son víctimas los dispositivos vestibles, se procede a realizar recomendaciones de seguridad para que estos terminales que son utilizados por millones de usuarios diariamente y las redes a las que se conectan puedan ser más seguras. Las mencionadas recomendaciones se las observa en la tabla 10.

Tabla 10.

Medidas de Seguridad

Amenaza	**Contramedidas**
Suplantación de Identidad	No permitir que la información sensible sea transferida en texto plano.
	Impedir que las credenciales sean almacenadas en texto plano.
	Utilizar una autenticación más restrictiva.

Manipulación	Utilización de firmas digitales.
	Realizar comparaciones de códigos *hash*.
Repudio	Utilizar sistemas que registren *logs*.
	Utilizar firmas digitales.
Divulgación de Información	Utilizar algoritmos seguros de encriptación.
	No permitir que la información sensible sea transmitida en texto plano.
Denegación de Servicio	Utilizar control de ancho de banda o balanceo de carga para dispersar el flujo de información.
Elevación de privilegio	Seguir el principio de mínimos privilegios.

Adicionalmente, cabe mencionar que la información de identificación personal (PII) es información asignable a un factor específico del sistema humano y en algunas jurisdicciones tiene protección legal (Boyle y Panko, 2014). La transmisión de una dirección MAC fija, atada a la identidad de un individuo fallaría la prueba PII al crear una firma de usuario única. Cuando los dispositivos vestibles crean un riesgo sin notificación al usuario, la violación de la privacidad debe considerarse jurisdicción por jurisdicción. Por ejemplo, la Directiva de Protección de Datos Personales del Parlamento Europeo promulgada el 5 de mayo de 2016 e introducida por sus estados miembros en sus leyes nacionales hasta el 6 de mayo de 2018, extiende la definición de datos personales para incluir aquellos que pueden identificarse, directa o indirectamente (Parlamento Europeo, 2016). Una dirección MAC fija corre el riesgo de vigilancia invisible, violando este requerimiento.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La aparición de los dispositivos vestibles ha resultado en una gran cantidad de información sensible viajando a través del mundo digital. Así, toda esta data se encuentra expuesta al riesgo de violaciones injustificadas de privacidad, amenazando la vida de los usuarios y su seguridad. Por consiguiente, la protección de la privacidad de las personas se ha convertido en un gran reto en el desarrollo de la tecnología vestible.

La implementación y utilización de la tecnología vestible a través de redes WBAN empleando dispositivos sensores se han convertido en parte integral de la vida diaria y sus diferentes actividades. El creciente interés en estos dispositivos y redes ha generado preocupación sobre su seguridad y privacidad. En este documento se ha revisado y analizado utilizando el modelo DREAD, los diferentes ataques que los dispositivos vestibles pueden sufrir y el riesgo que esto conlleva. Así, se ha logrado confirmar la alta importancia que abarca la seguridad de la información al momento de trabajar con estos dispositivos.

La tecnología vestible a pesar de su rápido crecimiento se encuentra en una primera etapa de su generación y promete un gran futuro a nivel de su desarrollo. Asimismo, sus vulnerabilidades, amenazas y riesgos a los que se encuentran expuestos estos dispositivos, se hallan en una etapa inicial y de investigación que seguirá evolucionando al mismo o mayor ritmo que la tecnología. En consecuencia, este trabajo de investigación permite introducir una futura área de desarrollo en el ámbito de la evolución de la seguridad en la tecnología vestible.

El conocimiento de los usuarios acerca de las amenazas de seguridad y cuestiones de privacidad en el contexto de los dispositivos vestibles es muy importante debido a que un mayor conocimiento y entendimiento de las amenazas asociadas con estos dispositivos, permitirá al usuario tomar mejores

decisiones al momento de adquirirlos y utilizarlos. Con el fin de proveer al usuario dicha información, en esta investigación se ha utilizado el modelo STRIDE y demostrado la existencia de diferentes amenazas a las que están expuestas los dispositivos vestibles a través de varios tipos de ataques.

5.2 Recomendaciones

Evidentemente, los parámetros analizados en este documento son considerados por algunos científicos e investigadores como importantes. Sin embargo, cabe destacar que estos no son los únicos existentes. El lector debe ser capaz de analizarlos e interpretarlos según su criterio.

El desarrollo de la tecnología vestible ha traído grandes beneficios para la humanidad. Sin embargo, aunque sus beneficios son grandes, también hay que tener en cuenta sus implicaciones. Por lo tanto, se recomienda informarse ampliamente y sobre todo de fuentes confiables sobre los beneficios e implicaciones que conlleva el uso de esta tecnología y dispositivos.

El modo de uso de los dispositivos vestibles presenta algunas dificultades en su utilización para algunos usuarios, por consiguiente, es recomendable leer comprensivamente las indicaciones que brindan los manuales de usuario adjuntos en las páginas web oficiales del fabricante de cada dispositivo. Por su parte, esta buena práctica permite evitar una mala configuración que deje puertas abiertas a ataques informáticos hacia el dispositivo y su información.

Es importante tener en cuenta que la seguridad de los dispositivos vestibles en un futuro va a seguir evolucionando a la par de esta tecnología, es por ello, que se recomienda seguir informándose e investigando constantemente acerca del tema ya que permitirá ampliar el conocimiento y protegerse de mejor manera a la hora de utilizar estos dispositivos.

REFERENCIAS

Acosta, D. (2014). *¿Cómo funcionan las tarjetas de pago? Parte VI: Tarjetas contactless (RFID – NFC)*. Recuperado de: https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-vi-tarjetas-contactless-rfid-nfc/

Al-Muhtadi, J., Mickunas, D., Campbell, R. (2001). Wearable Security Services. *International Conference on Distributed Computing Systems Workshops.* doi: 10.1109/CDCS.2001.918716

Allied Market Research. (2017). *Wearable Technology Market Overview.* Recuperado de: https://www.alliedmarketresearch.com/wearable-technology-market

Amazon. (2020). *LETSCOM Fitness Tracker HR, Reloj de seguimiento de actividad con monitor de frecuencia cardíaca, resistente al agua, pulsera inteligente de fitness con contador de pasos, contador de calorías, podómetro, para niños, mujeres y hombres, Android iOS.* Recuperado de: https://www.amazon.com/-/es/seguimiento-actividad-frecuencia-resistente-inteligente/dp/B07GCM9N72

Amazon. (2020). *PatrolMaster 1296P Cámara de cuerpo UHD con audio (64 GB), pantalla de 2 pulgadas, visión nocturna, impermeable, a prueba de golpes, cámara desgastada con diseño compacto, cámara de policía para hacer cumplir la ley.* Recuperado de: https://www.amazon.com/-/es/PatrolMaster-pantalla-pulgadas-impermeable-desgastada/dp/B07T8YPMRT?ref_=s9_apbd_otopr_hd_bw_bAy3NYR&pf_rd_r=PN6VJF3X25679Y0A9T1G&pf_rd_p=6b996aec-772e-5c69-b472-5ca68d8a2ed5&pf_rd_s=merchandised-search-10&pf_rd_t=BROWSE&pf_rd_i=10048714011

Amazon. (2020). *YAMAY - Reloj inteligente para Android y iOS Phone IP68 resistente al agua, con monitor de ritmo cardíaco, monitor de sueño, reloj inteligente compatible con iPhone Samsung, reloj para hombres y mujeres.* Recuperado de: https://www.amazon.com/YAMAY-Waterproof-Pedometer-Smartwatch-Compatible/dp/B07SK1SF81

Arefin, T., Ali, M., Haque, F. (2017). Wireless Body Area Network: An Overview and Various Applications. *Journal of Computer and Communications, 5*(7), 53-64. doi: 10.4236/jcc.2017.57006

Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011*, 1–5. doi: 10.1109/WIRELESSVITAE.2011.5940923

Bhattasali, T., Chaki, R., Sanyal. S. (2012). Sleep deprivation attack detection in wireless sensor network. *International Journal of Computer Applications, 40*(15), 19-25. doi: 10.5120/5056-7374

Boyle, R. J., & Panko, R. R. (2014). *Corporate computer security*. Essex, Inglaterra: Prentice Hall Press

Catapult. (2020). *Cardiff city partner with catapult to measure player performance through wearable technology*. Recuperado de: https://staging-v2.catapultsports.com/blog/cardiff-city-catapult-performance-wearable-technology

Cat Sensors. (2019). *Tecnología LoRa y LoRaWAN.* Recuperado el 07 de junio de 2020 de: https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan

Centro de Recursos de Seguridad Informática de los Estados Unidos CSRC. (2020). *Threat*. Recuperado el 14 de abril de 2020 de: https://csrc.nist.gov/glossary/term/threat

Centro Médico Wexner de la Universidad Estatal de Ohio. (2013). *Point of view surgery shown via Google Glass*. Recuperado de: http://www.osuwmc.multimedianewsroom.tv

Chang, C., Hwang, K. (2003). *Some forgery attacks on a remote user authentication scheme using smart cards, 14*(3), 289–294

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., Jin, Y. (2018). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*. doi: 10.1007/s41635-017-0029-7.

Ching, K., Singh, M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications (IJNSA), 8*(3). doi: 10.5121/ijnsa.2016.8302

Cisco. (2020). *Security Vulnerability Policy*. Recuperado el 14 de abril de 2020 de: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

Cisco. (2019). *The Evolution of Industrial Cybersecurity and Cyber Risk White Paper*. Recuperado el 14 de abril de: https://www.cisco.com/c/en/us/solutions/collateral/industry-solutions/whitepaper-c11-742528.html

ComputerWorld. (2017). *The future of smart glasses comes into focus*. Recuperado de: https://www.computerworld.com/article/3236493/the-future-of-smart-glasses-comes-into-focus.html

Cryptomathic. (2020). *What is non-repudiation?* Recuperado el 17 de mayo de 2020 de: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation

Cusack, B., Antony, B., Ward, G., Mody, S. (2017). Assessment of security vulnerabilities in wearable devices. *Australian Information Security Management Conference*. doi: 10.4225/75/5a84e6c295b44

Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security Analysis of Wearable Fitness Devices (Fitbit). Massachusetts Institute of Technology, 2014, 1-14.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340. doi: 10.2307/249008

Dimov, D. (2013). *Privacy Implications of Google Glass*. Recuperado el 14 de abril de 2020 de: https://resources.infosecinstitute.com/privacy-implications-of-google-glass/

Ding, Z., Li J., Feng, B. (2008). A taxonomy model of RFID security threats. *11th IEEE International Conference on Communication Technology. ICCT, 2008*, 765–768. doi: 10.1109/ICCT.2008.4716242

D'Mello, O., Gelin, M. Khelil, F., Sürek, R., Chi, H. (2018). Wearable IoT Security and Privacy: A Review from Technology and Policy Perspective. *Future Network Systems and Security*, 162-177. doi: 10.1007/978-3-319-94421-0_13.

Dorai, R., Kannan, V. (2011). SQL injection—database attack revolution and prevention. *J Int'l Com L & Tech, 6* (4), 224.

Douceur, J. (2002). The Sybil attack. *International Workshop on Peer-to-Peer Systems, 2429*, 251–260. doi: 10.1007/3-540-45748-8_24

eLearning Bakery. (2019). *Accessing content with Google Glasses*. Recuperado de: http://elearningbakery.com/accessing-content-with-google-glasses/#sthash.Jr9LBS8q.dpbs

El País. (2015). *Google Glass "es celeste"*. Recuperado de: https://www.elpais.com.uy/vida-actual/google-glass-celeste.html

Eun, H., Lee, H., Oh, H. (2013). Conditional privacy preserving security protocol for NFC applications. *IEEE Transactions on Consumer Electronics, 59*(1), 153-160. doi: 10.1109/TCE.2013.6490254

Evans, M. A., & Rick, J. (2014). Supporting learning with interactive surfaces and spaces. En J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of research on educational communications and technology, 4*, 689–701. New York, NY: Springer. doi: 10.1007/978-1-4614-3185-5_55

Fajardo, A., Rangel, F. (2016). A taxonomy for learning, teaching, and assessing wireless body area networks. *IEEE 7th Latin American Symposium on Circuits & Systems*, 179-182. Florianopolis. doi: 10.1109/LASCAS.2016.7451039

Farooq, M., Waseem, M., Khairi, A., Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*, 1-6. doi: 10.5120/19547-1280.

Fernandes, E., Jung, J., Prakash, A. (2016). Security analysis of emerging smart home applications. *IEEE Symposium on Security and Privacy (SP),* 636–654. doi: 10.1109/SP.2016.44

FitLyfe. (2019). *Wearable devices at work*. Recuperado de: https://www.gofitlyfe.com/blog/wearable-devices-5-data-driven-tips-for-healthy-holiday-habits/

Flynt, J. (2019). *6 Best Smart Jewelry Pieces of 2019.* Recuperado de: https://3dinsider.com/smart-jewelry/

Geek University. (2019). *Confidentiality, Integrity, and Availability (CIA) triad*. Recuperado el 14 de abril de 2020 de: https://geek-university.com/ccna-security/confidentiality-integrity-and-availability-cia-triad/

Ghoreishizadeh, S.S., et al. (2014). A lightweight Cryptographic system for implantable biosensors. *Biomedical Circuits and Systems Conference.* IEEE

Grassi, M. (2014). *How to capture Bluetooth packets on Android 4.4*. Recuperado de: https://www.nowsecure.com/blog/2014/02/07/bluetooth-packet-capture-on- android-4-4/

Grupo de Computación Contextual. (2014). *Captioning on Glass (COG).* Recuperado de: https://www.research.cc.gatech.edu

Gruschka, N., Jensen, M. (2010) Attack surfaces: a taxonomy for attacks on cloud services. *IEEE 3rd International Conference on Cloud Computing (CLOUD)*, 276–279. doi: 10.1109/CLOUD.2010.23

Guo, F. (2015). *Securing Wearable Devices*. Recuperado de: http://www.leiphone.com/news/201511/cMxCXDonsugGN892.html

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2017). Security threats in Bluetooth technology. *Computers & Security, 74*. doi: 10.1016/j.cose.2017.03.008.

Healthcare IT Leaders. (2018). *How Wearables Are Changing the Healthcare Industry*. Recuperado de: https://www.healthcareitleaders.com/blog/how-wearables-are-changing-the-healthcare-industry/

Herrington, J., Reeves, T. C., & Oliver, R. (2014). Authentic learning environments. En J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of research on educational communications and technology, 4*, 401–412. New York, NY: Springer. doi: 10.1007/978-1-4614-3185-5_32

HiConsumption. (2017). *DynaFeed Smart Shirt*. Recuperado de: https://hiconsumption.com/dynafeed-smart-shirt/

Hossain, M., Fotouhi, M., Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. *IEEE World Congress on Services*, 21–28. doi: 10.1109/SERVICES.2015.12

Huang, K., Starner, T., Do, E., Weinberg, G., Kohlsdorf, D., Ahlrichs, C., & Leibrandt, R. (2010). Mobile music touch: mobile tactile stimulation for passive learning. En *Proceedings of the SIGCHI conference on human factors in computing systems*, 791–800. Conferencia llevada a cabo en el Grupo de interés especial sobre la interacción computadora-humano, Atlanta, GA. doi: 10.1145/1753326.1753443

ICT Lounge. (2020). *The different types of Networks*. Recuperado de: https://www.ictlounge.com/html/types_of_networks.htm

Ingram. (2017). *How to Design a Wearable Technology Policy for Businesses*. Recuperado de: https://imaginenext.ingrammicro.com/networking-and-security/how-to-design-a-wearable-technology-policy-for-businesses

Jensen, M., Schwenk, J., Gruschka, N., Iacono, LL. (2009). On technical security issues in cloud computing. *IEEE International Conference on Cloud Computing*, 109–116. doi: 10.1109/CLOUD.2009.60

Jia, Y., Chen Q., Wang, S., Rahmati, A., Fernandes, E., Mao, Z., Prakash, A. (2017). ContexIoT: towards providing contextual integrity to appified IoT platforms. *Proceedings of the 21st Network and Distributed System Security Symposium*. doi: 10.14722/ndss.2017.23051

Kim, D., Lu, N., Ma, R., Kim, Y., Kim, R., Wang, S., Wu, J., Won, S., Tao, H., Islam, A., Yu, K., Kim, T., Chowdhury, R., Ying, M., Xu, L., Li, M., Chung, H., Keum, H., McCormick, M., Liu, P., Zhang, Y., Omenetto, F., Huang, Y., Coleman, T., Rogers, J. (2011). Epidemial Electronics. *Science, 333*(6044), 838-843. doi: 10.1126/science.1206157

Kemper, G. (2018). *Do Wearable Devices Connect People to the Internet of Things?* Recuperado el 07 de junio de 2020 de: https://clutch.co/it-services/resources/wearables-connect-internet-of-things-technology

Landis, J., Koch, G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*, 159-74.

Lotfy, K., Hale, M. L. (2016). Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things. *2016 IEEE International Conference on Mobile Services*. doi:10.1109/MobServ.2016.15

Mardonova, M., Choi, Y. (2018). Review of Wearable Device Technology and Its Applications to the Mining Industry. *Energies, 11*(3), 547. Doi: 10.3390/en11030547

Marner, M. R., Irlitti, A., & Thomas, B. H. (2013). Improving procedural task performance with augmented reality annotations. *Science and technology proceedings of the 2013 IEEE international symposium on mixed and augmented reality.* Simposio llevado a cabo en el Instituto de Ingenieros Eléctricos y Electrónicos, Adelaida, Australia. doi: 10.1109/ISMAR.2013.6671762

Mayer, R. E. (2001). *Multimedia learning*. New York, NY: Cambridge University Press.

Mitrokotsa, A., Rieback, M., Tanenbaum, A. (2010). Classification of RFID attacks. *2nd International Workshop on RFID Technology - Concepts, Applications, Challenges*.

Nagamine, K. (2019). *Ongoing Demand Fuels a Strong Growth Trajectory for Wearable Devices in Q1 2019 with Wrist-Worn and Ear-Worn Leading the Market, According to IDC*. Recuperado de: https://www.idc.com/getdoc.jsp?containerId=prUS45115019

Nan, Y., Yang, M., Yang, Z., Zhou, S., Gu, G., Wang, X. (2015). UIPicker: user-input privacy identification in mobile applications. *USENIX Security Symposium*, 993–1008.

Padhy, R., Patra, M., Satapathy, S. (2011) Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS), 1*(2), 136–146.

Park, H., Rabolt, N., Jeon, K. (2008). Purchasing global luxury brands among young Korean consumers. *Journal of Fashion Marketing and Management, 12*(2), 244-259. doi: 10.1108/13612020810874917

Parlamento Europeo. (2016). *Directive (EU) 2016/680*. Recuperado el 20 de abril de 2020 de: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

Pieterse, H., & Olivier, M. S. (2014). Bluetooth Command and Control channel. *Computers & Security, 45*, 75-83. doi: 10.1016/j.cose.2014.05.007

Poon, C., Wong, Y., Zhang, Y. (2006). M-Health: The development of cuff-less and wearable blood pressure meters for use in body sensor networks. *IEEE/NLM Life Science Systems and Applications Workshop*, 1-2. doi: 10.1109/LSSA.2006.250377

Rawlinson K. (2015). *HP Study Reveals Smartwatches Vulnerable to Attack*. Recuperado de: http://www8.hp.com/us/en/hp-news/pressrelease.html?id=2037386#.Vi18G7crLIU

Sabillon, R., Cano, J., Cavaller, V., Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176.

Safavi, S., Z. Shukur. (2014). Improving google glass security and privacy by changing the physical and software structure. *Life Science Journal, 11*(5), 109-117.

Salazar, J. (2017). *Wireless Networks*. Universidad Técnica de Praga, Praga, República Checa.

Sastry, A., Sulthana, S., Vagdevi, S. (2013). Security threats in wireless sensor networks in each layer. *Int. J. Advanced Networking and Applications, 4*(4), 1657-1661.

Sawaya S. (2015). Wearable Devices in Education. En P. Redmond, J. Lock, P.A Danaher (eds), *Educational Innovations and Contemporary Technologies*. Palgrave Macmillan, Londres. doi: 10.1057/9781137468611_3

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A. (2017). A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys & Tutorials, 19*(4), 2573-2620. doi: 10.1109/COMST.2017.2731979

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q. (2009). *AVOIDIT: a cyber-attack taxonomy*

Sociedad Andaluza de Medicina Intensiva y Unidades Coronarias. (2020). *Kappa de Cohen.* Recuperado de: http://www.samiuc.es/estadisticas-variables-binarias/medidas-de-concordancia/kappa-de-cohen/#:~:text=Kappa%20de%20Cohen%20(%CE%BA),que%20podr%C3%ADaocurrir%20por%20mero%20azar.&text=Si%20K%20es%20cero%2C%20ello,que%20ocurrir%C3%ADa%20por%20puro%20azar.

Terahertz Technology. (2016). *Terahertz -One of "5 Technologies Transforming the Defense and Aerospace Industries".* Recuperado de: https://terahertztechnology.blogspot.com/2016/11/terahertz-one-of-5-technologies.html

Time. (2017). *Why Perfectly Healthy People Are Using Diabetes Monitors.* Recuperado de: https://time.com/4703099/continuous-glucose-monitor-blood-sugar-diabetes/

Tobón, D., Gaviria, N. (2012). *Análisis de métricas de calidad de servicio para la configuración del protocolo CSMA/CA en redes de sensores inalámbricas de área corporal.* Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-34612012000100007

Tseng, T., Wu, C., Lai, F. (2019). Threat Analysis for Wearable Health Devices and Environment Monitoring Internet of Things Integration System. *IEEE Access, 7*, 144983-144994. doi: 10.1109/ACCESS.2019.2946081

Tzou, R., Lu, H. (2009). Exploring the emotional, aesthetic, and ergonomic facets of innovative product on fashion technology acceptance model. *Behaviour & Information Technology, 28*, 311-322. doi: 10.1080/01449290701763454

Veredict. (2019). *Wearable technology in healthcare: What are the leading tech themes driving change?* Recuperado de: https://www.medicaldevice-network.com/comment/wearable-technology-in-healthcare-what-are-the-leading-tech-themes-driving-change/

Warren, M., Leitch, S. (2009). Hacker Taggers: A new type of hackers. *Information Systems Frontiers, 12*, 425-431. doi: 10.1007/s10796-009-9203-y

Weintraub, S. (2013). *Doctor uses Google Glass to share surgery with colleagues/students across town*. Recuperado de: https://9to5google.com/2013/08/27/doctor-uses-google-glass-to-share-surgery-with-colleaguesstudents-across-town/

Welch, D., Lathrop, S. (2003). Wireless security threat taxonomy. *IEEE Systems, Man and Cybernetics Society and Information Assurance Workshop, 2003*, 76–83. doi: 10.1109/SMCSIA.2003.1232404

Wired. (2013). *Why Wearable Tech Will Be as Big as the Smartphone*. Recuperado de: https://www.wired.com/2013/12/wearable-computers/

WTVOX. (2018). *Wearable Tech Education – Top 10 Changes For Years To Come*. Recuperado de: https://wtvox.com/fashion-innovation/wearable-tech-education/

Yang, H., Yu, J., Zo, H., Choi, M. (2015). User acceptance of wearable devices: An extended perspective of perceived value. *Telematics and Informatics*. doi: 10.1016/j.tele.2015.08.007

Zhang, Q., Wang, X. (2009). SQL injections through back-end of RFID system. *International Symposium on Computer Network and Multimedia Technology*, 1–4. doi: 10.1109/CNMT.2009.5374533

Zheng, Y., Ding, X., Poon, C., Lo, B., Zhang, H., Zhou, X., Yang, G., Zhao, N., Zhang, Y. (2014). Unobtrusive Sensing and Wearable Devices for Health Informatics. *IEEE Transactions on Biomedical Engineering, 61*(5), 1538-1554. doi: 10.1109/TBME.2014.2309951

Zhu, B., Joseph, A., Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. *International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011*, 380-388. doi: 10.1109/iThings/CPSCom.2011.34

ANEXOS

Glosario de Términos

Estándar: Se refiere a un conjunto de normas utilizadas de manera general en un ámbito determinado y de forma repetida, lo cual permite lograr un orden determinado.

Hashing: Se refiere al proceso de encripción a través de fórmulas matemáticas conocidas como funciones *hash*.

IEEE: *Institute of Electrical and Electronics Engineers.* Es una asociación mundial de Ingenieros que se dedica al desarrollo de normas y estándares enfocadas al área técnica.

IrDA: *Infrared Data Association*. Se refiere al uso de la luz infrarroja como medio de comunicación.

Log: Se refiere a la grabación en un archivo o base de datos de manera secuencial de todos los eventos que afectan a un proceso específico.

Modelo: Hace referencia a aquello que es tomado como referencia en la búsqueda de producir algo igual o similar.

RFID: *Radio Frequency Identification.* Es a una forma de comunicación inalámbrica a través de ondas de radio entre un lector y un emisor. Su propósito es transmitir la identidad de un objeto. Se compone de una etiqueta, un lector y un sistema de procesamiento de datos.

Wearable: Se refiere a los dispositivos electrónicos incorporados o portados en alguna parte del cuerpo humano que interactúan continuamente con el usuario y otros dispositivos con el fin de cumplir una o varias funciones específicas.