Maestría en

# CIBERSEGURIDAD

**Trabajo previo a la obtención de título de**
**Magíster en Ciberseguridad**


**AUTOR/ES:**

Gabriela Alexandra Montenegro Martínez

Paula Vanessa Mosquera Morales

Omar Enrique Pilay Díaz

Stefano Andrés Rodríguez Mosquera

**TUTOR/ES:**

Alejandro Cortés

Iván Reyes Chacón


**TEMA:**

Auditoría de ciberseguridad para el análisis de identificación de vulnerabilidades en dispositivo medidor de glucosa


Quito - Ecuador

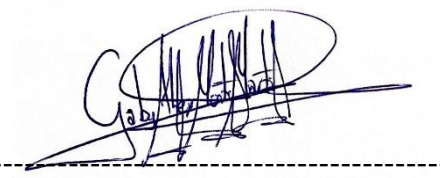
Julio – 2025


REINVENTEMOS EL FUTURO

**Certificación de autoría**

Nosotros, **Gabriela Alexandra Montenegro Martínez, Paula Vanessa Mosquera Morales, Omar Enrique Pilay Díaz, Stefano Andrés Rodríguez Mosquera,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



---

**Firma del graduando**
**Gabriela Alexandra Montenegro Martínez**

---

**Firma del graduando**
**Paula Vanessa Mosquera Morales**

---

**Firma del graduando**
**Omar Enrique Pilay Díaz**

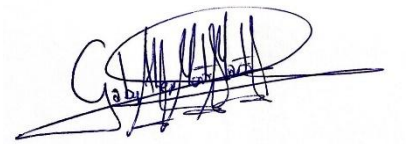
---

**Firma del graduando**
**Stefano Andrés Rodríguez Mosquera**

**Autorización de Derechos de Propiedad Intelectual**

Nosotros, **Gabriela Alexandra Montenegro Martínez, Paula Vanessa Mosquera Morales, Omar Enrique Pilay Díaz, Stefano Andrés Rodríguez Mosquera**, en calidad de autores del trabajo de investigación titulado ***Auditoría de ciberseguridad para el análisis de identificación de vulnerabilidades en dispositivo medidor de glucosa***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (Julio 2025)

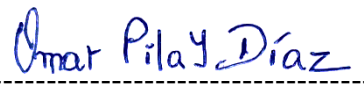


---

**Firma del graduando**
**Gabriela Alexandra Montenegro Martínez**

---

**Firma del graduando**
**Paula Vanessa Mosquera Morales**



---

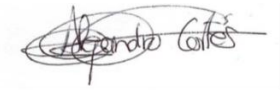
**Firma del graduando**
**Omar Enrique Pilay Díaz**

---

**Firma del graduando**
**Stefano Andrés Rodríguez Mosquera**

**Aprobación de dirección y coordinación del programa**

Nosotros, **Alejandro Cortés e Iván Reyes,** declaramos que los graduandos: **Gabriela Alexandra Montenegro Martínez, Paula Vanessa Mosquera Morales, Omar Enrique Pilay Díaz, Stefano Andrés Rodríguez Mosquera** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés L.
Maestría en Ciberseguridad

Iván Reyes Ch.
Maestría en Ciberseguridad

# DEDICATORIA

Dedicamos este trabajo a nuestras familias quienes, con su amor incondicional, comprensión y apoyo constante, han sido el motor que nos impulsó incluso en los momentos más retadores.

Este logro también va dedicado a quienes, con su ejemplo, nos inspiraron a seguir el camino del conocimiento y la ética profesional.

# AGRADECIMIENTOS

Expresamos nuestro más sincero agradecimiento a la Universidad Internacional del Ecuador (UIDE) y al cuerpo académico de la Maestría en Ciberseguridad, por brindarnos las herramientas, conocimientos y orientación necesarios para el desarrollo de esta investigación.

Agradecemos también a nuestros compañeros de cohorte, por las discusiones, aportes y momentos compartidos que enriquecieron tanto el aprendizaje como la experiencia personal.

Finalmente, a nuestras familias y amigos, por su apoyo incondicional, su paciencia y su fé en nuestras capacidades.

# RESUMEN

La presente investigación aborda el análisis de seguridad informática aplicado a dispositivos médicos de monitoreo de glucosa con conectividad inalámbrica, específicamente aquellos que utilizan tecnología Bluetooth Low Energy (BLE). Se llevaron a cabo dos experimentos controlados con los modelos ACCU-CHEK Instant y ACCU-CHEK Guide, aplicando una metodología basada en principios del hacking ético. Las pruebas incluyeron diferentes fases como el reconocimiento del entorno, identificación de servicios disponibles, simulación de ataques conocidos y análisis estático de la aplicación móvil vinculada (mySugr).

A pesar de las limitaciones impuestas por el uso de hardware genérico, no se detectaron vulnerabilidades críticas que comprometieran la privacidad o funcionalidad de los dispositivos analizados. Por el contrario, se evidenciaron medidas de protección adecuadas tanto en los dispositivos como en el software asociado. Por lo que se concluye que, si bien estos equipos presentan mecanismos defensivos efectivos, futuras auditorías con herramientas más avanzadas podrían revelar aspectos técnicos adicionales. Finalmente, se plantean recomendaciones dirigidas tanto a usuarios como a desarrolladores, con el fin de promover entornos de atención médica más seguros en el contexto de dispositivos IoT.

Palabras Claves:
Ciberseguridad, dispositivos médicos, auditoría, Bluetooth Low Energy, hacking ético, IoT.

# ABSTRACT

This research focuses on the cybersecurity evaluation of wireless medical devices used for blood glucose monitoring, particularly those that rely on Bluetooth Low Energy (BLE) connectivity. Two controlled experiments were conducted using the ACCU-CHEK Instant and ACCU-CHEK Guide models, applying ethical hacking techniques to assess their vulnerability. The approach included reconnaissance, service enumeration, simulated exploit attempts, and static analysis of the associated mobile app (mySugr).

Despite using non-specialized hardware, the investigation did not uncover critical flaws affecting the devices' integrity or data protection. On the contrary, security features implemented in both the hardware and the mobile application were found to be robust. The study highlights the importance of continuous security assessments and recommends further testing with advanced tools. Suggestions are also provided for both end users and developers to strengthen defenses in the context of connected medical technologies.

Keywords:
Cybersecurity, medical devices, audit, Bluetooth Low Energy, ethical hacking, IoT.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# CAPITULO 1:

## 1. INTRODUCCIÓN

La conocida revolución digital en la actualidad ha transformado todos los aspectos en lo cotidiano y demás campos e industrias alrededor del mundo. Uno de los campos en el que se ha visto un cambio relativamente específico y tan importante es el denominado sector de la salud. Gracias a la tecnología de gran ayuda, como lo es el Internet de las cosas conocida por sus siglas en inglés IoT (Internet of Things) ha renovado la atención sanitaria. Con los dispositivos médicos conectados a la red, los profesionales de la salud tienen la facilidad de poder diagnosticar, monitorear y brindar una atención médica oportuna al paciente (Vaca y Valle, 2024).

Con el avance de la tecnología también aumentan las amenazas cibernéticas con estrategias cada vez más sofisticadas. Debido a que los sistemas de salud almacenan grandes cantidades de información (datos sensibles), estos son un blanco de vital importancia para los ciberdelincuentes.

Las principales causas de ciberataques provienen de las vulnerabilidades en dispositivos médicos IoT que están conectados a Internet, como lo son los marcapasos, monitoreo de signos vitales (monitores de presión arterial y glucosa, entre otros) y las bombas de insulina, mismos dispositivos tienen a ser explotadas sus vulnerabilidades por los ciberdelincuentes con el fin de reunir información (riesgo de privacidad de datos) o a su vez modificar datos (causar daños) (Cervera y Goussens, 2024).

En este trabajo de investigación se plantea realizar una auditoría de seguridad informática en dispositivo médico IoT medidor de glucosa, empleando técnicas y heramientas de ciberseguridad para identificar las posibles vulnerabilidades de dicho dispositivo que puedan comprometer su integridad.

En el capítulo 1, se define el proyecto, se detallan los objetivos de como se realiza la propuesta, se da su respectiva justificación y por ultimo se explica el alcance de la investigación. En el capítulo 2, se detallan estudios relacionados con la investigación y se justifica de manera teórica el proyecto. En el capíulo 3, se expone la metodología utilizada en la investigación y se explica con detalle la propuesta del trabajo (análisis de factibilidad y fases de un ataque hacker). En el capítulo 4, se pone en funcionamiento la auditoría de ciberseguridad realizada al dispositivo IoT médico medior de glucosa, además del análisis de resultados y las medidas de mitigación. Finalmente, en el capítulo 5, se dan las conclusiones y recomendaciones del protecto.

### 1.1. Definición del Proyecto

Este proyecto tiene como propósito llevar a cabo una evaluación detallada de la seguridad informática en un dispositivo medidor de glucosa con conectividad IoT, orientada a la detección de posibles vulnerabilidades que puedan comprometer su integridad. En un entorno donde los avances tecnológicos han transformado la atención médica y la gestión de datos sensibles, garantizar la protección de estos dispositivos resulta cada vez más prioritario.

El análisis consistirá en aplicar métodos de auditoría de ciberseguridad específicos para identificar debilidades en la arquitectura y el funcionamiento del dispositivo. Se busca exponer brechas que podrían ser explotadas por agentes maliciosos, afectando tanto la privacidad de los pacientes como la estabilidad de los sistemas en los equipos.

Con base en los resultados obtenidos, se plantearán estrategias de mitigación y fortalecimiento de la seguridad, enfocadas en prevenir accesos no autorizados y manipulación de información médica crítica. Este trabajo aspira a generar conciencia en la comunidad médica y en los fabricantes sobre la importancia de integrar políticas de ciberseguridad robustas en el desarrollo y la implementación de tecnologías sanitarias, contribuyendo así a crear un entorno clínico más seguro y confiable.

### 1.2. Justificación e importancia del trabajo de investigación

El avance de la tecnología digital ha transformado radicalmente el sector de la salud, impulsando la adopción de dispositivos médicos inteligentes que facilitan el monitoreo y control de diversas condiciones clínicas. Sin embargo, esta modernización ha traído consigo nuevos desafíos en materia de ciberseguridad, especialmente para dispositivos que integran tecnologías IoT, como los medidores de glucosa.

El incremento en el número de dispositivos interconectados ha expandido la superficie de ataque disponible para los ciberdelincuentes, quienes buscan explotar vulnerabilidades para obtener acceso a información confidencial o alterar el funcionamiento de equipos médicos. En este contexto, el presente proyecto resulta relevante ya que aborda la necesidad crítica de garantizar la protección de los datos de los pacientes y de preservar la integridad funcional de los dispositivos médicos.

Mediante el desarrollo de la auditoría de ciberseguridad se pretende realizar un análisis identificando las posibles vulnerabilidades que el dispositivo medidor de glucosa llegase a tener. Esta investigación no solo contribuye al fortalecimiento de la seguridad en dispositivos de uso sanitario, sino que también proporciona un marco de referencia para el

diseño de políticas de ciberseguridad orientadas al sector salud. La detección temprana de riesgos permitirá reducir la exposición de los sistemas hospitalarios a amenazas, mejorando la confianza de los usuarios en el uso de tecnologías digitales para el manejo de enfermedades crónicas.

Además, este estudio tiene un impacto más allá del ámbito técnico, al fomentar una cultura de prevención en seguridad informática entre fabricantes, profesionales sanitarios y responsables de infraestructura hospitalaria, colaborando así en la construcción de entornos clínicos más seguros y resilientes frente a amenazas emergentes.

## 1.3. Alcance

Este proyecto de investigación se centrará en la evaluación de las vulnerabilidades de un dispositivo medidor de glucosa que opera bajo un entorno de Internet de las Cosas (IoT). A través de la aplicación de técnicas de auditoría de ciberseguridad, se buscará identificar posibles brechas que comprometan la confidencialidad, integridad y disponibilidad de los datos generados y transmitidos por el dispositivo.

El análisis se limitará al estudio de dos modelos específicos de medidores de glucosa, evaluando su exposición a amenazas comunes en entornos IoT, así como su capacidad de resistir ataques dirigidos. No se contemplará la intervención sobre otros dispositivos médicos ni la implementación directa de soluciones de seguridad en ambientes hospitalarios.

Al finalizar el estudio, se emitirán recomendaciones específicas orientadas a mitigar los riesgos detectados, con el objetivo de fortalecer las capacidades de protección del dispositivo evaluado. De esta manera, se contribuirá a establecer prácticas de seguridad más robustas que puedan ser aplicadas en futuras investigaciones o desarrollos tecnológicos en el ámbito médico.

## 1.4. Objetivos

### 1.4.1. Objetivo General

Realizar un análisis de ciberseguridad sobre un dispositivo médico IoT medidor de glucosa, a fin de identificar vulnerabilidades y proponer medidas que fortalezcan su protección frente a amenazas cibernéticas.

### 1.4.2. Objetivos Específicos

- Aplicar técnicas de hacking ético para detectar vulnerabilidades y poder comprometer la seguridad del dispositivo medidor de glucosa.
- Investigar sobre las herramientas en Kali Linux que conllevan a realizar con éxito ataques comunes de Bluetooth dirigidos a comprometer los datos transmitidos por el dispositivo glucómetro y vulnerar la integridad de este.
- Evaluar el impacto potencial de las vulnerabilidades halladas en la privacidad de los datos médicos y en la integridad del dispositivo.
- Formular recomendaciones prácticas de seguridad orientadas a minimizar los riesgos identificados.

# CAPITULO 2:

## 2. REVISIÓN DE LITERATURA

### 2.1. Estado del Arte

En este apartado se darán a conocer investigaciones sobre los peligros que conllevan el uso de la tecnología IoT en el sector salud sin la ciberseguridad de la mano. Además, de estudios relevantes relacionadas con el análisis de identificación de posibles vulnerabilidades en dispositivo médico IoT, que pueden llegar a afectar a la privacidad, integridad y disponibilidad de los datos de los pacientes, y hasta comprometer los sistemas de la institución hospitalaria.

Según Oliveira (2024), el aumento de Internet de las cosas (de las siglas en inglés IoT) es un hito tan relevante en el crecimiento tecnológico en la actualidad, y brinda una conectividad satisfactoria entre dispositivos físicos y sistemas informáticos. El uso de esta tecnología es implementado en muchos campos, uno de ellos en el sector salud, como lo es la atención médica. Este campo antes mencionado se beneficia de las posibilidades innovadoras en termino de calidad de vida. Sin embargo, es preocupante en tema de seguridad informática el gran crecimiento de estos dispositivos conectados, recopilando gran cantidad de información para su posterior transmisión de los datos aumenta el riesgo de ataques que pueden llegar a explotar por parte de ciberdelincuentes y personas malintencionadas.

En la sección de artículos, la Administración de Alimentos y Medicamentos de Estados Unidos (FDA) menciona que los dispositivos médicos (marcapasos, bombas de insulina y demás dispositivos) son cada vez más modernos. La mayoría de estos dispositivos contienen software y se pueden conectar a internet, a las redes de la institución hospitalaria, al teléfono celular u otros dispositivos para compartir información. Por eso es de vital importancia que se garantice la ciberseguridad de los dispositivos IoT médicos. Los avances de esta tecnología son aplicados a los dispositivos médicos debido a que estos avances permiten brindar una atención médica oportuna. Se sabe que las personas que sufren de diabetes tienen nuevas alternativas para llevar el control de sus niveles de glucosa en la sangre, dado que varios dispositivos médicos medidores de glucosa y bombas de insulina logran comunicarse entre sí. Las instituciones hospitalarias buscan ser más eficiente en la mejora a la atención a los pacientes, y están utilizando más dispositivos que estén conectados a la red para compartir datos. La FDA indica que, si un dispositivo médico posee software y conexión por cable o conexión inalámbrica, es importante prestar la debida atención a

cualquier problema que se presente, teniendo en cuenta que estos problemas pueden volverse vulnerable a ciberataques (Food and Drug Administration, 2022).

Un caso relevante sucedió en el año 2019, en donde la Administración de Alimentos y Medicamentos (FDA) de Estados Unidos ordenó el retiro del mercado de señaladas bombas de insulina Medtronic MiniMed teniendo en cuenta a ciertos riesgos de ciberseguridad. La FDA dio como recomendación a las personas que utilizasen estos modelos de bombas de insulinas cambiasen a modelos que contengan seguridad adicional contra estos mismos riesgos. Se conoce que hasta el momento no se han reportado incidentes de daños de salud a pacientes ocasionados por esta vulnerabilidad de ciberseguridad, pero el retiro de este dispositivo llama la atención la necesidad de embestir las vulnerabilidades de seguridad en los dispositivos IoT médicos para el perseverar la seguridad del paciente y garantizar la integridad de los datos (Oliveira, 2024).

Cartwright (2023), en su investigación el elefante en la habitación: la ciberseguridad en la atención médica detalla como la ciberseguridad ha experimentado un crecimiento de los ciberataques y la exposición de la Información Médica Protegida (por sus siglas en inglés PHI). Además, la adopción en auge de los dispositivos IoT y sobre todo el impacto que representó la pandemia de COVID-19 han sido la causa de amenaza que representa el sector salud para los ciberataques. En el espacio sanitario en general, se ha producido un crecimiento a diario sobre el uso de dispositivos cableados e inalámbricos en la atención médica de la mayoría de los pacientes. El Internet de las cosas Médicas (IoMT), como ventiladores, máquinas de anestesia, bombas de infusión, marcapasos y una gran variedad de dispositivos de monitorización, conectados a la red un hospital, supone una nueva oportunidad para que personas malintencionadas pueda acceder a los sistemas hospitalarios de la institución. Ya sea con fines económicos, políticos o simplemente atacar a los sistemas y causar una monitorización errónea de los pacientes, y la modificación en la configuración de los dispositivos IoMT.

Saltzstein (2020), en su artículo denominado tecnología inalámbrica Bluetooth Ciberseguridad y dispositivos tecnológicos para la diabetes detalla el uso de dispositivos para la diabetes, con énfasis atención en la ciberseguridad. Los dispositivos médicos son ampliamente utilizados en el sector hospitalario, pero han hecho una transición del sector hospitalario al familiar y al del usuario final o consumidor. Estos dispositivos han demostrado tener capacidad para la mejora en la movilidad y mejorar la calidad de vida en el tratamiento de la diabetes. Algunos dispositivos, como las bombas de insulina y los medidores de glucosa

fueron diseñados con tecnología Bluetooth para la conexión entre sí o como puerta de enlace. Esta tecnología de conexión inalámbrica permite transmitir los datos del medidor de glucosa a aplicaciones móviles inteligentes que se emplean para generar estadísticas y alertas para el usuario y sus cuidadores. Los datos contienen valores variantes tanto para el atacante como para el usuario final. Al interceptar un solo valor de medición de glucosa de un dispositivo no tiene mucha relevancia sin tener información del paciente. En cambio, si la misma medición de glucosa es utilizada para establecer la dosis de insulina y el atacante logra modificar los datos, el resultado final podría ser fatal para el usuario. Por esta razón los fabricantes de estos dispositivos y sistemas deben de realizar un análisis previo y ver el valor de los activos, para luego ser implementadas las soluciones y medidas de ciberseguridad oportunas para todo el sistema que los incluye.

En sección de artículos, la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) mencionan vulnerabilidades encontradas en el equipo “kit de inicio del sistema de monitoreo de glucosa en sangre Dario Health USB-C (aplicación para Android)”. El estándar Sistema de Puntuación de Vulnerabilidades Comunes (CVSS), en su versión 4 le asigna una puntuación de 8.7, considerado un riego alto. La evaluación de riesgos detalla que la explotación exitosa de estas vulnerabilidades podrían ser blanco fácil de un atacante puesto que el mismo puede exhibir la información, inyectar código, manipular datos o a su vez lograr secuencias de comandos entre sitios (XSS), lo que implicaría un compromiso de sesión completa por parte del atacante. Entre las vulnerabilidades encontradas están la exposición de la información privada del usuario a un actor no autorizado, neutralización inadecuada en la salida de los registros, almacenamiento de datos sensibles del usuario en un mecanismo sin el debido control de acceso, la falta de cifrado facilita la transmisión de información sensible en texto claro, la aplicación del proveedor es vulnerable a ataques XSS (secuencias de comandos entre sitios), no contar con política de cookies sin la marca “HttpOnly” permitiendo comprometer información sensible durante la navegación y políticas incompatibles en el servidor del proveedor, lo que podría generar una funcionalidad insegura, comprometiendo información sensible (Cybersecurity and Infrastructure Security Agency, 2025).

## 2.2. Marco Teórico

### 2.2.1. El Internet de las Cosas Médicas (IoMT): Fundamentos, Beneficios y Aplicaciones

El internet de las Cosas Medicas (IoMT) representa una convergencia entre la tecnología de sensores, la conectividad inalámbrica y los sistemas de información médica, permitiendo la recopilación, transmisión y el análisis de datos clínicos en tiempo real. Esta interconexión facilita una atención sanitaria más eficiente y personalizada, al integrar dispositivos médicos con plataformas digitales que respaldan la toma de decisiones clínicas (Iberia, 2021).

**Fundamentos del IoMT**

IoMT se basa en la integración de dispositivos médicos equipados con sensores y capacidades de comunicación, que permite la monitorización continua de parámetros fisiológicos. Estos dispositivos recopilan datos y estos son transmitidos a través de redes seguras a sistemas de almacenamiento y análisis, donde los profesionales de la salud pueden acceder a información actualizada para el seguimiento y tratamiento de los pacientes (Ghubaish et al., 2023).

La arquitectura del IoMT generalmente comprende tres capas: la capa de percepción, esta incluye los sensores y los dispositivos de recopilación de datos; la capa de red, que se encarga de la transmisión de datos; y la capa de aplicación, donde se procesan y analizan los datos para proporcionar servicios médicos (Si-Ahmed et al., 2022).

**Beneficios del IoMT**

Como parte de la infraestructura de telemedicina más extensa, IoMT ofrece varias ventajas las cuales se mencionan a continuación (Lutkevich y DelVecchio, 2023):

- **Sistemas de monitorización de pacientes:** El usar IoMT va a permitir la monitorización continua de la salud del paciente que posea alguna enfermedad crónica, facilitando a los profesionales de la salud (médicos) en el control con respecto a la información sobre las condiciones de vida del paciente, misma que influye en la atención del paciente.
- **Accesibilidad:** Con IoMT los pacientes tendrán mayor acceso a los servicios de salud. Gracias al uso de IoMT, los pacientes tienen más opciones a los diferentes servicios de salud y pueden acceder a ellos cuando los requieran por medio de una aplicación de telesalud.
- **Control de costos:** La monitorización remota de pacientes (de sus siglas en

inglés, RPM) y la telesalud ahorran los costos que en primera instancia implica que el paciente acuda de manea física al centro de salud. El contar con un procesamiento más rápido de los datos de salud comprende el ahorro de tiempo y dinero a los proveedores, permitiéndoles enfocar sus recursos en las áreas que más lo necesiten.

- **Experiencia mejorada del paciente:** Con IoMT se minimizan las visitas del paciente de manera presencial debido al uso de nuevas tecnologías que facilitan el autoservicio del paciente. Entre las tecnologías de autoservicio se encuentran los dispositivos wearables de consumo. Estos dispositivos ofrecen a los pacientes acceso a datos que de manera tradicional habrían tenido que obtener de un profesional de la salud (médico).
- **Precisión:** Se proporcionan más datos, lo que permite a los profesionales de la salud (médicos clínicos) conseguir información de manera más precisa sobre el estado de salud de los pacientes. Un claro ejemplo de esto es un tensiómetro con IoMT, dado que estos dispositivos médicos pueden proporcionar lecturas de presión arterial y frecuencia cardiaca de algunos días, permitiendo un diagnóstico más preciso, al contrario de los datos de una sola consulta médica.
- **Logística:** Los dispositivos IoMT son utilizados para la supervisión de los equipos en centros sanitarios, con el fin de enviar alertas cuando surgen problemas de mantenimiento u otros problemas que lleguen a afectarlos. Además, son utilizados como rastreadores para dar seguimiento a los pacientes y a los medicamentos en las instalaciones de los centros médicos, reduciendo las confusiones y los errores.

**Aplicaciones del IoMT**

Las aplicaciones del IoMT son diversas y abarcan múltiples áreas de la atención medica:

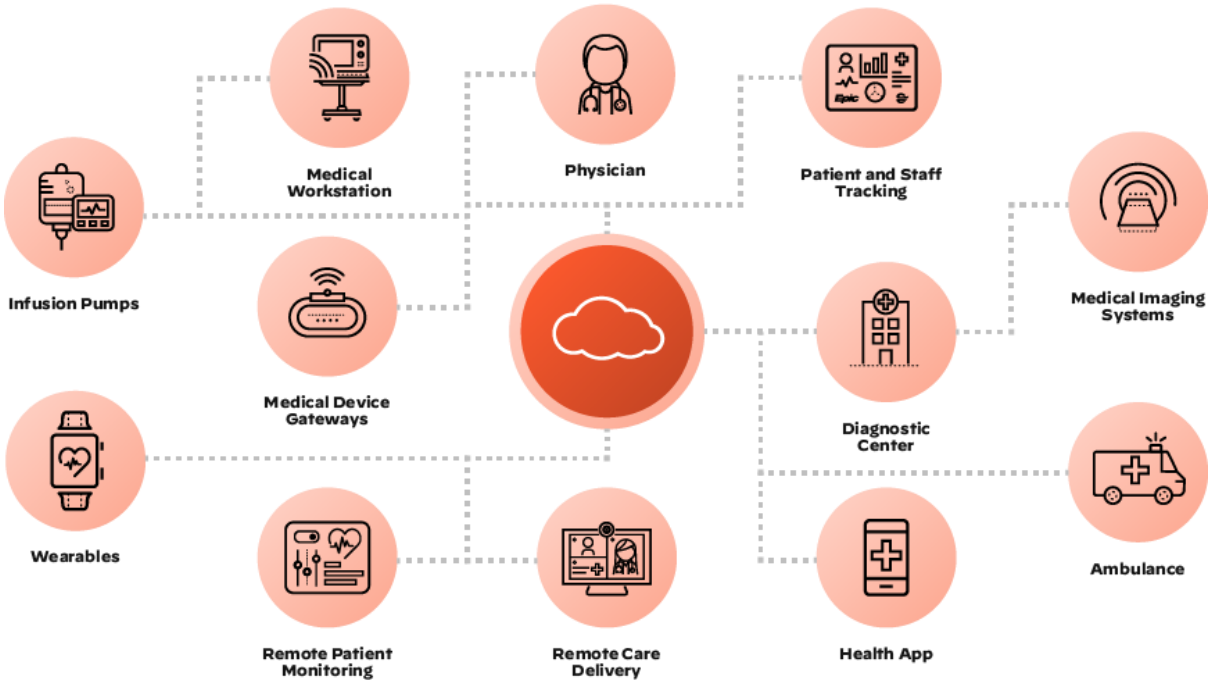
- **Monitorización remota de pacientes:** Permite el seguimiento continuo de pacientes con enfermedades crónicas, reduciendo la necesidad de visitas presenciales y facilitando intervenciones tempranas ante cambios en los parámetros de salud (Dzamesi y Elsayed, 2025).
- **Gestión de enfermedades crónicas:** Con el ejemplo de la diabetes mellitus

tipo 1, el IoMT facilita la monitorización continua de la glucosa y la administración automatizada de insulina, mejorando el control glucémico y la calidad de vida de los pacientes (Campo, 2023).

- **Telemedicina:** La integración de dispositivos IoMT con plataformas de telemedicina permite consultas médicas a distancia, aumentando el acceso a servicios de salud en áreas remotas o con limitaciones de movilidad.
- **Cirugías asistidas por robots:** La combinación del IoMT con tecnologías robóticas ha dado lugar a procedimientos quirúrgicos más precisos y menos invasivos, al proporcionar datos en tiempo real y asistencia durante las intervenciones (Ghubaish et al., 2023).

**Figura 1**

*Aplicaciones de IoMT*




*Nota*. Podemos ver algunos ejemplos de dispositivos y aplicaciones de IoMT. Adaptado de *Aplicaciones de IoMT* [Fotografía], Palo Alto Networks, s.f., https://www.paloaltonetworks.co.uk/cyberpedia/what-is-iomt-security#iot

### 2.2.2. Principios de la Auditoría de Seguridad en Dispositivos IoT

La adopción masiva de tecnologías IoT ha traído consigo una expansión significativa en la superficie de ataque de los entornos digitales. Esto es especialmente crítico en el sector médico, donde los dispositivos conectados manejan información sensible y pueden influir

directamente en la salud de los pacientes. En este contexto, la auditoría de seguridad en dispositivos IoT representa una herramienta fundamental para identificar riesgos, verificar la integridad de la arquitectura tecnológica y recomendar acciones de mitigación efectivas (Majumdar et al., 2021).

## Fundamentos de la Auditoria de Seguridad en IoT

La auditoría de seguridad en IoT implica un proceso técnico y metodológico orientado a la evaluación sistemática de los dispositivos, sus configuraciones, y los servicios que ofrecen. A diferencia de otros entornos, los dispositivos IoT suelen operar con recursos limitados (baja capacidad de cómputo, memoria reducida y ausencia de sistemas operativos tradicionales), lo que requiere un enfoque especializado para la identificación de vulnerabilidades (Majumdar et al., 2021).

Una auditoría eficaz debe considerar las capas físicas, de red y de aplicación del sistema IoT. Además, debe incluir el análisis de vectores de ataque, como el acceso físico no autorizado, la interceptación de datos en tránsito, la suplantación de identidad de dispositivos y la manipulación de firmware.

## Etapas de la Auditoría de Seguridad en IoT

Una metodología estructurada puede dividirse en las siguientes fases (Targolic, 2021):

1. **Identificación de activos:** Registro detallado de los dispositivos conectados, funciones y su nivel de exposición.
2. **Análisis de riesgos:** Evaluación del impacto potencial de una amenaza sobre la operación o los datos del dispositivo.
3. **Revisión de configuraciones:** Validación de parámetros de red, autenticación, cifrado y accesos.
4. **Pruebas técnicas:** Ejecución de escaneos de puertos, sniffing de red, fuzzing, o análisis de firmware.
5. **Monitoreo de comportamiento:** Revisión de logs, patrones de tráfico y eventos anómalos.
6. **Informe de resultados:** Documentación clara de hallazgos, riesgos y recomendaciones priorizadas.

**Buenas Prácticas y Estándares**

Existen marcos normativos que respaldan la auditoría de dispositivos IoT. Entre los más relevantes están:

- **NIST IR 8259:** Define perfiles de seguridad para fabricantes de dispositivos IoT.
- **OWASP IoT Top 10:** Enumera los riesgos más comunes en entornos IoT, tales como configuraciones inseguras, interfaces vulnerables y ausencia de actualizaciones seguras (Foudation, 2022).
- **ISO/IEC 27030:** Proporciona directrices de ciberseguridad específicas para IoT.

Entre las buenas prácticas recomendadas se encuentran:

- El uso de credenciales únicas y fuertes.
- La segmentación de red y filtrado de tráfico.
- La actualización periódica del firmware.
- La eliminación de servicios innecesarios expuestos por los dispositivos.

### 2.2.3. Seguridad del IoT

El fin del proyecto de Internet de las cosas (IoT) de OWASP es ayudar a los fabricantes, desarrolladoras y consumidores a entender de mejor manera sobre los problemas de seguridad asociados con la IoT, y a su vez permitir que los usuarios tomen mejores decisiones de seguridad al momento de crear, implementar o evaluar tecnologías de Internet de las cosas (IoT).

A continuación, se detallan en una sola lista de 10 ítems, sobre riesgos, amenazas y vulnerabilidades, que se deben tener en cuenta al momento del desarrollo de proyectos IoT, que se deben evitar en la seguridad del IoT (Open Web Application Security Project [OWASP], 2019):

1. **Contraseñas débiles, adivinables y codificadas:** Este aspecto implica el uso de credenciales forzadas de manera fácil, disponibles públicamente o que las mismas no se pueden alterar, que incluyen puertas traseras en el firmware o a su vez del software cliente que otorgan acceso no autorizado a los servidores o al sistema.
2. **Servicios de red inseguros:** En este apartado se encuentran los servicios de

red innecesarios (servicios de red que no se utilizan en el dispositivo) o inseguros que se ejecutan en el mismo dispositivo. Los más peligrosos son los que se encuentran expuestos a Internet, llegando a ser explotados por personas con grado de conocimiento en la materia o personas malintencionadas, que pueden llegar a comprometer la confidencialidad (información vista por otra persona no autorizada), integridad (información modificada) y disponibilidad (no disponibilidad de la información) de la información, además de permitir el control remoto no autorizado.

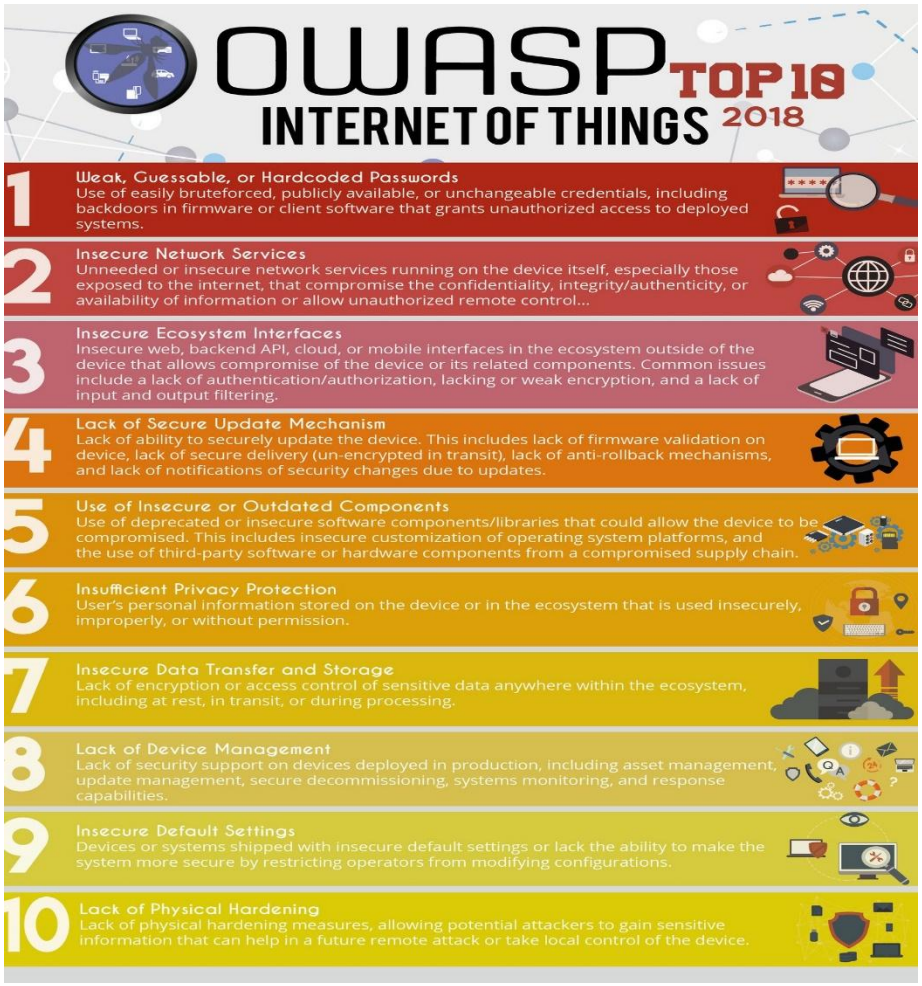
3. **Interfaces de ecosistema inseguras:** Las cuales se encuentran interfaces web, API de backeund, la nube o móviles inseguras en el entorno fuera del dispositivo que puede llegar a ser comprometido o sus componentes relacionados. Entre los problemas más comunes se encuentra la falta de autenticación/autorización, el cifrado deficiente y la falta de filtrado en la entrada y salida.
4. **Falta de un mecanismo de actualización seguro:** Consiste en la falta de capacidad para la correcta actualización del dispositivo de forma segura. Misma incluye la falta de validación del firmware en el dispositivo, falta de entrega segura (tránsito sin cifrar), falta de mecanismos antirretroceso y la falta de avisos ante algún cambio de seguridad en vista de actualizaciones.
5. **Uso de componentes inseguros u obsoletos:** El uso de componentes y/o bibliotecas de software obsoletos e inseguros que pueden llegar al punto de verse comprometido. Como puede ser las plataformas del sistema operativo dado a la personalización insegura, y el uso de elementos de software o hardware de terceros de una cadena de suministro aumenta el riesgo de ser vulnerable a un ataque.
6. **Protección insuficiente de la privacidad:** La información sensible del usuario es almacenada en el dispositivo o en el ecosistema que es utilizada de manera insegura, indebida o sin permiso.
7. **Transferencia y almacenamiento de datos inseguros:** La falta de cifrado o el control de acceso a datos confidenciales del usuario en cualquier parte dentro del entorno, incluidos el estado en reposo, en tránsito o durante el procesamiento.
8. **Falta de administración de dispositivos:** La falta de soporte de seguridad en

los dispositivos efectuados durante la producción, comprendida la gestión de activos, las actualizaciones, el desmantelamiento seguro y el control de sistemas.

9. **Configuración predeterminada insegura:** Los dispositivos desde fábrica o sistemas finalizados son enviados con las configuraciones predeterminadas o que no tienen la capacidad de hacer que el sistema sea más seguro al limitar que el personal que manejan estas utilidades modifiquen las configuraciones que vienen predeterminadas por el proveedor, ocasionado que estos componentes sean más inseguros.
10. **Falta de endurecimiento físico:** La falta de medidas de endurecimiento físico permite que los atacantes puedan obtener información sensible mediante posibles ataques futuros como ataque remoto o tener el control total del dispositivo.

**Figura 2**

*OWASP Top 10 IoT*



*Nota*. Top 10 sobre las vulnerabilidades más comunes según OWASP. Adaptado de *OWASP Top 10 IoT* [Fotografía], OWASP, 2019, https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

### 2.2.4. Tecnologías de Comunicación en Dispositivos Médicos: Enfoque en Bluetooth Low Energy

La integración de tecnologías inalámbricas en dispositivos médicos ha transformado la atención sanitaria, permitiendo una monitorización continua y remota de pacientes. Entre estas tecnologías, Bluetooth Low Energy (BLE) se destaca por su bajo consumo energético y su capacidad para mantener conexiones estables, características esenciales para dispositivos médicos que requieren operaciones prolongadas sin recargas frecuentes (Terzidis et al., 2023).

#### Características de BLE en el Ámbito Médico

BLE opera en la banda de 2.4 GHz y está diseñado para aplicaciones que requieren transferencias de datos de baja velocidad, pero con alta eficiencia energética. Esto lo convierte en una opción ideal para dispositivos médicos como monitores de glucosa, marcapasos y sensores de actividad, donde la duración de la batería y la fiabilidad de la conexión son críticas (Peña, 2023).

#### Vulnerabilidades y Desafíos de Seguridad

A pesar de sus ventajas, BLE presenta desafíos significativos en términos de seguridad. Investigaciones han identificado vulnerabilidades como ataques de intermediario (MITM), suplantación de identidad y ataques de denegación de servicio (DoS), que pueden comprometer la integridad y confidencialidad de los datos médicos transmitidos (Terzidis et al., 2023).

Un estudio de caso reveló que ciertos dispositivos médicos basados en BLE eran susceptibles a ataques que permitían a un atacante remoto manipular los niveles de intensidad de un electroestimulador, lo que podría tener consecuencias graves para el paciente (Lakshminaryanan y Nota, 2023).

#### Medidas de Mitigación y Buenas Prácticas

Para abordar estas vulnerabilidades, se recomiendan las siguientes medidas:

- **Autenticación y Emparejamiento Seguro:** Implementar métodos de emparejamiento seguros, como el uso de claves de autenticación y códigos de confirmación, para prevenir accesos no autorizados (Peña, 2023).
- **Cifrado de Datos:** Utilizar algoritmos de cifrado robustos, como AES-128, para proteger la información transmitida entre dispositivos (Terzidis et al., 2023).
- **Actualizaciones de Firmware:** Mantener los dispositivos actualizados con los últimos parches de seguridad proporcionados por los fabricantes para corregir vulnerabilidades conocidas (Lakshminaryanan y Nota, 2023).
- **Monitoreo y Detección de Anomalías:** Implementar sistemas de monitoreo que detecten comportamientos inusuales en la comunicación BLE, lo que podría indicar un intento de ataque (Shukla, 2024).

### 2.2.5. Gestión de Vulnerabilidades en IoMT: Estándares y Modelos de Evaluación

La gestión de vulnerabilidades en dispositivos del Internet de las Cosas Médicas (IoMT) es un proceso sistemático orientado a identificar, analizar, priorizar y mitigar las debilidades de seguridad presentes en los dispositivos médicos conectados a redes digitales. Dado que estos equipos recopilan, procesan y transmiten información clínica sensible, su exposición a ciberamenazas representa un riesgo elevado tanto para la privacidad del paciente como para la operación de los servicios médicos.

Una de las herramientas más aceptadas internacionalmente para la clasificación de estas vulnerabilidades es el Common Vulnerability Scoring System (CVSS), cuya versión más reciente, la 4.0, incorpora criterios mejorados de evaluación según el impacto del fallo, la dificultad de explotación y el contexto operativo del dispositivo (FIRST, 2023). Esta puntuación permite establecer la criticidad de una vulnerabilidad mediante un sistema estandarizado y facilita a los responsables de seguridad tomar decisiones informadas sobre las medidas correctivas a implementar.

Además del CVSS, se emplean marcos normativos como la ISO/IEC 27005, que establece los principios para la gestión de riesgos en sistemas de información, y la NIST SP 800-30, enfocada en la evaluación cualitativa y cuantitativa de amenazas

tecnológicas (NIST, 2022). Estas guías recomiendan realizar evaluaciones periódicas que incluyan análisis de vulnerabilidades, auditorías técnicas y pruebas de penetración en dispositivos IoMT, considerando su especificidad en entornos clínicos.

También es esencial aplicar principios de seguridad desde el diseño, siguiendo el enfoque "security by design", que implica proteger el software, firmware y hardware desde las primeras fases del desarrollo. Estrategias como la actualización segura de firmware, la segmentación de red para aislar dispositivos críticos, el cifrado de datos en tránsito y en reposo, y la autenticación robusta forman parte de una arquitectura de seguridad integral.

Finalmente, la integración de herramientas automáticas de escaneo junto con la supervisión activa de los sistemas, el monitoreo de logs y la aplicación de inteligencia de amenazas ayudan a detectar anomalías y responder ante incidentes. Esto requiere una cultura institucional orientada a la ciberseguridad, con roles claramente definidos y políticas de respuesta efectivas.

### 2.2.6. Seguridad en Aplicaciones Móviles Asociadas a Dispositivos Médicos

Las aplicaciones móviles que interactúan con dispositivos médicos desempeñan un papel crucial en la atención digital, ya que permiten a los usuarios monitorear variables fisiológicas, recibir alertas y compartir datos clínicos con los profesionales de salud. Sin embargo, su conectividad constante a redes públicas, su presencia en dispositivos personales y el manejo de datos sensibles las convierten en uno de los puntos más vulnerables del ecosistema IoMT.

Diversos estudios han evidenciado que muchas aplicaciones de salud carecen de mecanismos adecuados de protección de datos. Entre los errores comunes se encuentran el uso de protocolos de comunicación inseguros (como HTTP en lugar de HTTPS), la ausencia de cifrado en el almacenamiento local de datos, y la exposición de información sensible a través de logs o notificaciones del sistema (Aljedaani y Babar, 2023). Estas debilidades pueden permitir que un atacante intercepte, modifique o suplante datos críticos, afectando decisiones médicas y poniendo en riesgo la vida del paciente.

Para abordar estos riesgos, el marco de referencia más utilizado es el OWASP Mobile Security Testing Guide (MSTG), que ofrece una serie de controles de seguridad para garantizar la protección de las aplicaciones móviles. Entre estos controles se incluyen: cifrado de extremo a extremo para la transmisión de datos, validación de entradas para prevenir

inyecciones, uso de almacenamiento seguro del sistema operativo (Android Keystore o iOS Secure Enclave), y autenticación multifactor (OWASP, 2023).

Además, las aplicaciones deben implementar control de accesos basado en roles (RBAC), políticas estrictas de gestión de sesiones y protección contra secuestro de cookies mediante la aplicación de banderas como HttpOnly, Secure y SameSite. También se recomienda la revisión continua del código fuente y las dependencias externas, ya que bibliotecas de terceros pueden introducir vulnerabilidades inadvertidas. En el contexto legal, legislaciones como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) en Estados Unidos, establecen exigencias claras respecto a la confidencialidad, integridad y disponibilidad de la información médica, aplicables también a las plataformas móviles. Cumplir con estos marcos regulatorios no solo previene sanciones, sino que refuerza la confianza del paciente en la tecnología.

En suma, la seguridad en aplicaciones móviles médicas debe abordarse de forma holística, desde el desarrollo hasta la distribución y actualización. La falta de una gestión adecuada puede exponer tanto al paciente como a las instituciones médicas a amenazas cibernéticas con consecuencias potencialmente graves.

### 2.2.7. Arquitectura de Seguridad en Dispositivos Médicos IoT

El desarrollo y la integración de dispositivos médicos inteligentes en el ecosistema del Internet de las Cosas Médicas (IoMT) han generado una transformación significativa en la atención sanitaria. Sin embargo, esta conectividad expone a dichos dispositivos a riesgos de ciberseguridad cada vez más sofisticados. Frente a esta realidad, la arquitectura de seguridad se vuelve un componente crítico, ya que define las bases técnicas, organizativas y procedimentales que garantizan la protección de los datos médicos y el correcto funcionamiento de los equipos (Fernández y Fraga, 2018).

Una arquitectura de seguridad en dispositivos IoMT debe concebirse de manera defensiva en profundidad, lo que implica la implementación de múltiples capas de protección, desde el hardware hasta la nube, con el objetivo de reducir la superficie de ataque y mitigar los riesgos en cada nivel del sistema (Sicari et al., 2015 ).

**Capa de seguridad física y del firmware**

Esta capa protege el dispositivo ante manipulaciones físicas o ataques de hardware. Se emplean mecanismos como el arranque seguro (Secure Boot), la protección de memoria no volátil (e.g., EEPROM con cifrado) y la verificación de integridad del firmware. Además, se recomienda implementar un sistema de actualizaciones firmadas digitalmente para prevenir la instalación de código malicioso (Yaqoob et al., 2022).

**Capa de comunicación y red**

Dado que muchos dispositivos médicos se conectan a través de Bluetooth Low Energy (BLE), Wi-Fi o redes móviles, es esencial cifrar toda comunicación entre nodos. El uso de protocolos seguros como TLS/SSL sobre TCP/IP, o el cifrado AES-CCM en BLE, permite evitar la interceptación de datos o ataques de intermediario (MITM). Asimismo, se debe autenticar cualquier dispositivo que intente emparejarse, y validar los certificados digitales de los servidores con los que interactúe el sistema (Farahani, 2021).

**Capa de autenticación, autorización y gestión de identidades (IAM)**

La gestión de identidades es vital para controlar el acceso a funciones críticas del dispositivo y a los datos del paciente. Se recomienda el uso de autenticación multifactor (MFA) para los usuarios finales y mecanismos de autorización basados en roles (RBAC) o atributos (ABAC), permitiendo así limitar las acciones que cada entidad puede ejecutar (Chatterjee et al., 2019). Esta capa también incluye el control de sesiones, detección de accesos anómalos y revocación de credenciales comprometidas.

**Capa de monitoreo y gestión de vulnerabilidades**

Los dispositivos IoMT deben incorporar capacidades de monitoreo de seguridad, como registros de eventos (logs), detección de anomalías en el comportamiento, y notificaciones de incidentes. Igualmente, deben contar con sistemas de actualización OTA (Over-The-Air) que garanticen la instalación segura de parches frente a nuevas vulnerabilidades. Esta capa es fundamental para mantener la confianza en el dispositivo una vez desplegado en el entorno hospitalario o domiciliario (Yaqoob et al., 2022).

**Capa de cumplimiento normativo y privacidad por diseño**

La arquitectura de seguridad debe cumplir con normativas como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley HIPAA en Estados Unidos. Estas regulaciones obligan al desarrollador a incorporar principios de privacidad desde el diseño, tales como la minimización de datos, la anonimización o seudonimización, y la transparencia frente al usuario (Radanliev et al., 2019). La trazabilidad de acciones, la posibilidad de auditar el sistema y los mecanismos de consentimiento informado también forman parte de esta capa.

Una arquitectura de seguridad efectiva en el IoMT no puede abordarse de manera aislada. Requiere una visión integral que contemple el dispositivo, la aplicación móvil, la infraestructura de backend, y los flujos de datos entre cada componente. Además, debe existir una coordinación multidisciplinaria entre ingenieros biomédicos, desarrolladores de software, expertos en seguridad informática y personal médico, lo que plantea un desafío técnico, ético y organizacional.

### 2.2.8. Amenazas de Seguridad Comunes en el Entorno IoMT

Actualmente en el sector de la salud se ha visto un crecimiento notable de ciberataques, preferiblemente por falta de madurez en materia de ciberseguridad, ocasionando una alta rentabilidad obtenidas por los atacantes (S2 Grupo, 2024).

Cada vez más las instituciones sanitarias utilizan el Internet de las cosas médicas (IoMT) para llevar un mejor control a los pacientes de forma eficaz y precisa.

El incremento del IoMT conlleva un aumento significativo de vulnerabilidades, que llevan a crear situaciones para que estos sean atacados. El problema viene cuando estos dispositivos médicos no están protegidos, poniendo en riesgo a los pacientes y llega hasta realizar daño a la infraestructura de una institución sanitaria.

Por tal razón, se van a mencionar los tipos de ataques comunes dirigidos a los dispositivos IoMT (PDI Technologies, s.f.):

- **Canal lateral:** Este tipo de ataque se beneficia de la fuga de información, demostrando ser potente y eficaz. En el sector salud, los atacantes podrían hacer uso de técnicas de canal lateral para el robo de información de los pacientes mediante el monitoreo de la actividad electromagnética a dispositivos médicos determinados.

- **Clonación de etiquetas:** El atacante realiza la acción del duplicado de los datos conseguidos a través del ataque de canal lateral de forma exitosa y utiliza la información para tener acceso a datos no autorizados (información personal de los pacientes). Los atacantes pueden clonar con facilidad las RFID (dispositivo con tecnología de identificación por radiofrecuencia).
- **Dispositivos de manipulación:** Un atacante puede hallar la manera de manipular físicamente los sensores para la detención o manipulación de forma parcial o total su funcionalidad, aplicando técnicas de explotación de vulnerabilidades del firmware para instalar un programa maligno (malware) para su posterior toma de control del dispositivo.
- **Rastreo de sensores:** Aplicativos como la monitorización de pacientes por medio de sensores GPS, la detección de caídas o a su vez la gestión de sillas de ruedas, los sensores enviarán la ubicación del paciente al profesional de la salud (médico) o al centro encargado de monitorear al paciente en caso de una emergencia. Una vez localizados, los atacantes logran acceder a estos dispositivos y a la ubicación del paciente, a sus datos privados o se puede dar el caso de enviar datos erróneos.
- **Escuchas clandestinas:** El dispositivo inteligente al ser localizado por el atacante, el mismo puede interceptar los datos inalámbricos que son transmitidos mediante dispositivos hardware. Como es el caso de los signos vitales de un paciente que consiguen ser interceptados durante la transmisión, ocasionando al uso inadecuado de esos datos.
- **Repetición:** El atacante reutiliza el mensaje de autenticación preliminarmente intercambiado entre los usuarios legítimos. Este tipo se da ataque se da ante la falta de mecanismos de comunicación seguros.
- **Man-in-the-middle:** En este tipo de ataque el hacker consigue acceder a los datos y logra reproducir y alterar de manera secreta las comunicaciones de ambas partes, debido a que los dispositivos de detección IoMT tienen por práctica enviar y recibir datos (lecturas del paciente), la alteración de esta información podría causar un tratamiento incorrecto (como el caso de una dosis excesiva de medicamentos o resultados falsos).
- **Acceso no autorizado:** El atacante se encarga de instalar una puerta trasera de

enlace no autenticada (falsificada) siempre y cuando se encuentre dentro del radio de la red inalámbrica para que esta permita el acceso a un usuario. De igual manera el hacker logra interceptar ese tráfico sin ser descubierto.

- **Denegación de servicio (DoS):** La gestión de este ataque es la de cargar a los dispositivos inteligentes con muchas solicitudes de servicio, ocasionado la interrupción del servicio y su disponibilidad. Además, los atacantes pueden tomar el control de los dispositivos IoMT mediante el ataque botnet (conjunto de red de robots informáticos automáticos) sin que el propietario tenga el más mínimo conocimiento.
- **Falsificación de solicitud entre sitios (CSRF):** El objetivo del ataque es la de engañar al usuario final para que funcione en una aplicación vulnerable sin el conocimiento del mismo usuario. Si no se realiza la configuración correctamente el entorno web de la capa del dispositivo IoMT se vuelve vulnerable a ataques CSRF.
- **Secuestro de sesión:** Este tipo de ataque actúa en los dispositivos inteligentes que administran la conexión de sesión a nivel de entorno web, estas interfaces web se vuelven vulnerables al ataque de secuestro de sesión, permitiendo que el atacante logre tener el control de los datos de la sesión del usuario.
- **Scripting entre sitios (XSS):** Este ataque se genera a través de la inyección de scripts cuyo fin es la de evadir los controles de acceso por medio de páginas web. Por ejemplo, se encuentran los dispositivos IoT conectados a la nube, su aplicativo web es vulnerable a estos ataques XSS.
- **Inyección SQL:** En este ataque el hacker se encarga de efectuar sentencias SQL maliciosas con el fin de evitar las medidas de seguridad del dispositivo donde se puede llegar a comprometer los datos privados del paciente o a su vez la modificación de estos datos sensibles.
- **Secuestro de cuentas:** Se da el secuestro de cuentas donde el atacante lo realiza interceptando la comunicación entre los elementos de IoMT a la espera de la autenticación del usuario final. El mayor problema de estos ataques se da en dispositivos con vulnerabilidades sin parchear.
- **Ransomware:** Mediante este ataque los hackers cifran los datos privados de un paciente (historiales clínicos) y son reservados a cambio de dinero. Por

primera instancia esta amenaza se puede dar en una sola máquina, hasta llegar a comprometer toda la red. Este ataque logra tener éxito con tan solo denegando el acceso a dispositivos IoMT en funcionamiento, poniendo en peligro la seguridad del paciente.

- **Fuerza bruta:** Existe escasa protección para eludir este tipo de ataques en dispositivos IoT. Este tipo de ataques se considera el modo más fácil en que los hackers consiguen ganar acceso a un servidor y a los mismos dispositivos IoT.

### 2.2.9. Requisitos Regulatorios y Normativos para Dispositivos Médicos Conectados

El desarrollo y uso de dispositivos médicos conectados está regulado por diversas normativas que buscan garantizar tanto la seguridad del paciente como la protección de los datos clínicos que estos dispositivos generan. En este contexto, los marcos regulatorios no solo se enfocan en el desempeño clínico, sino también en los aspectos relacionados con la ciberseguridad y la privacidad.

En Europa, uno de los principales marcos normativos es el Reglamento (UE) 2017/745 sobre los productos sanitarios (MDR), que exige que los dispositivos incorporen medidas de protección frente a accesos no autorizados y que gestionen adecuadamente los riesgos de software. Este reglamento considera el software como parte integral del dispositivo médico, por lo que debe evaluarse en función de su capacidad para resistir amenazas tecnológicas (European Union, 2017).

En Estados Unidos, la Administración de Alimentos y Medicamentos (FDA) ha emitido diversas guías que abordan la ciberseguridad en dispositivos médicos. Entre ellas destaca la "Premarket Cybersecurity Guidance" (2023), que establece que los fabricantes deben identificar amenazas potenciales, evaluar sus riesgos y desarrollar controles de mitigación antes de lanzar el producto al mercado. También se exige que los dispositivos incluyan mecanismos de actualización de software seguros y que se documenten los planes de respuesta ante incidentes (FDA, 2023).

A nivel global, normas como la ISO/IEC 81001-1 y la ISO/IEC 27001 ofrecen lineamientos específicos para la gestión de la seguridad de la información en entornos clínicos y tecnológicos. La primera se centra en los requisitos de seguridad de los sistemas de

salud digital, mientras que la segunda define un sistema de gestión de seguridad de la información que puede ser aplicado por organizaciones del sector salud (ISO, 2022).

Además, el cumplimiento del Reglamento General de Protección de Datos (GDPR) es obligatorio para los dispositivos que procesen datos personales dentro del territorio europeo. Este reglamento establece principios como la minimización de datos, la transparencia, el consentimiento explícito y el derecho del usuario a la portabilidad y eliminación de su información (European Parliament, 2016).

Cumplir con estas normativas no solo garantiza la legalidad del producto en los mercados internacionales, sino que también fortalece la confianza de los pacientes y profesionales médicos en el uso de tecnologías conectadas. Por ello, los fabricantes deben incorporar equipos multidisciplinarios que incluyan ingenieros biomédicos, expertos legales y profesionales de ciberseguridad para asegurar que cada dispositivo cumpla con los estándares más exigentes.

### 2.2.10. Buenas Prácticas para el Desarrollo Seguro de Aplicaciones Médicas

Dada la sensibilidad de los datos de salud las buenas prácticas para el desarrollo seguro de aplicaciones médicas son un factor de alta importancia por lo cual se vuelve indispensable adoptar prácticas que garanticen la confidencialidad, integridad y disponibilidad de la información. A continuación, se describen las principales buenas prácticas respaldadas por estándares internacionales.

#### Cumplimiento normativo desde el diseño

Las aplicaciones médicas deben ser diseñadas con enfoque en la privacidad y la seguridad desde su etapa inicial. Esto incluye la adopción de marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) en Europa, la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) en Estados Unidos y normas técnicas como la ISO/IEC 82304-1, que establece los requisitos generales de seguridad para software de salud (International Organization for Standardization, 2020).

#### Cifrado de datos

Toda la información médica debe ser cifrada desde el momento en el que se comienza a almacenar. Para ello, se recomienda el uso del protocolo TLS 1.2 o superior, y algoritmos de cifrado como AES-256 (National Institute of Standards and Technology, 2020). Esto evita

que los datos sean interceptados o accedidos de manera indebida, incluso si se produce una vulneración del sistema.

**Gestión de autenticación y control de acceso**

El uso de autenticación multifactor (MFA) fortalece significativamente la protección contra accesos no autorizados. Además, se debe implementar el principio del mínimo privilegio, asegurando que cada usuario solo tenga acceso a los datos y funcionalidades que necesita (Health Level Seven International, 2023). También es crucial mantener registros de auditoría para detectar comportamientos anómalos o posibles brechas.

**Pruebas de seguridad continuas**

La seguridad debe ser validada de forma continua mediante pruebas automatizadas y manuales. Esto incluye análisis estáticos de código (SAST), pruebas dinámicas (DAST) y pruebas de penetración para detectar vulnerabilidades antes de que puedan ser explotadas (OWASP Foundation, 2023). Integrar estas prácticas en el ciclo de desarrollo permite una detección temprana de errores críticos.

**Manejo seguro de errores y registros**

Los mensajes de error no deben revelar información sensible sobre la infraestructura del sistema o la lógica del negocio. Asimismo, los archivos de registro (logs) deben ser protegidos frente a alteraciones y accesos no autorizados, ya que pueden contener información clave sobre el comportamiento de la aplicación (SANS Institute, 2019).

**Protección de APIs**

Las interfaces de programación de aplicaciones (APIs) deben estar adecuadamente protegidas, utilizando mecanismos como OAuth 2.0, tokens JWT y validación de entradas para prevenir ataques de inyección, cross-site scripting (XSS) y otras amenazas comunes (Microsoft, 2023). Dado que las APIs permiten el intercambio de datos con sistemas externos, su seguridad es crítica.

Todas estas recomendaciones respaldadas por estándares internacionales y normativas legales no solo mejoran la calidad del desarrollo de aplicaciones, sino que también reduce riesgos legales y reputacionales para las organizaciones del sector salud.

### 2.2.11. Principales Prácticas de Seguridad de IoMT

Se va a detallar las mejores prácticas recomendadas de seguridad que hacen uso de los servicios en pleno desarrollo de IoT y las entidades médicas con la finalidad de salvaguardar la infraestructura y la información privada del IoT (Zhuravel, 2023).

- **Inventario de activos:** Para resguardar correctamente el entorno de IoMT, se necesitar conocer que se está protegiendo. Se recomienda crear un inventario que cuente con todos los dispositivos IoMT. No solo se debe proteger dispositivos médicos como bombas de insulina y los marcapasos, sino también elementos de toda la infraestructura de red.

  Para que el trabajo sea exitoso se debe realizar tareas en la actualización del inventario de manera frecuente, y así poder tener conocimiento de todos los dispositivos conectados a la red. Esta actividad es de vital importancia para la supervisión y gestión de forma eficaz los riesgos de seguridad.
- **Política de contraseñas seguras:** Para una óptima atención médica es importante consolidar la seguridad del IoT a través de una buena política de contraseñas robusta. Para ello se debe asegurar que todos los sistemas y dispositivos de la red de IoMT manejen contraseñas únicas y seguras. Se debe establecer una contraseña robusta se debe contar con diferentes caracteres (números, caracteres especiales y letras) y una longitud mayor de ocho caracteres, evitando nombres comunes y predeterminados, para no ser objetivo del atacante. Además, se debe realizar cambios periódicos de manera obligatoria de las contraseñas.
- **Autenticación multifactor:** Este método de autenticación multifactor (MFA) es una favorable medida de seguridad que agrega una capa extra de protección a los sistemas y dispositivos de IoMT. Se necesita que los usuarios tengan dos o más componentes de verificación (contraseña, tarjeta inteligente, una aplicación móvil, huella dactilar o escaneo de retina). Al implementar esta medida de seguridad se logra disminuir significativamente el riesgo de acceso no autorizado inclusive si una contraseña fuese comprometida.
- **Segmentación de la red:** Esto implica fraccionar la red IoMT en distintos segmentos pequeños y aislados. Cada segmento debe operar con sus medidas de seguridad y sus propios controles de acceso.

Al tener implementado la segmentación de red se puede contrarrestar las brechas de seguridad, evitando el movimiento lateral de los hackers y a su vez reducir el impacto de una vulneración de un segmento en específico, mejorando la seguridad de toda la red y proteger los sistemas y datos sensibles de salud.

- **Actualizaciones de parches de seguridad:** Realizar la actividad de actualizar de manera periódica el software y el firmware de los dispositivos IoMT además de la infraestructura de red es concluyente para abordar las vulnerabilidades y los fallos de seguridad. Se debe realizar la gestión de seguimiento de los avisos de seguridad de los dispositivos IoMT y efectuar los parches para aminorar los posibles riesgos.

# CAPITULO 3:

# 3. DESARROLLO

## 3.1. Desarrollo del Trabajo

El presente proyecto tiene como propósito auditar la ciberseguridad de dispositivos médicos que forman parte del ecosistema del Internet de las Cosas Médicas (IoMT), particularmente aquellos diseñados para el monitoreo de glucosa en pacientes con diabetes. Se seleccionaron dos modelos comerciales ampliamente utilizados: el ACCU-CHEK Instant y el ACCU-CHEK Guide debido a su popularidad y capacidad de conectividad mediante Bluetooth Low Energy (BLE). Estos dispositivos interactúan con la aplicación móvil mySugr, que permite a los pacientes visualizar, gestionar y compartir sus datos clínicos con profesionales sanitarios.

Dado el tipo de tecnología que emplean y el entorno sensible donde se utilizan, este tipo de dispositivos se convierten en blancos potenciales de ataques cibernéticos. Su análisis permite no solo evidenciar brechas técnicas, sino también reforzar las buenas prácticas en el diseño e implementación de soluciones médicas conectadas (Terzidis et al., 2023).

### 3.1.1. Metodología empleada

El presente trabajo empleó una metodología adaptada a auditorías de ciberseguridad en entornos IoMT, con un enfoque práctico y sistemático basado en el modelo de hacking ético. Esta aproximación resulta idónea para identificar vulnerabilidades en dispositivos que operan bajo el protocolo Bluetooth Low Energy (BLE), dado que considera tanto el comportamiento técnico del hardware como los posibles vectores de explotación en las capas de comunicación y aplicación (Majumdar et al., 2021):

El procedimiento se estructuró en cinco fases adaptadas de la metodología clásica de pentesting, siguiendo los lineamientos éticos recomendados por organizaciones como OWASP (2022) y NIST (2022):

- **Reconocimiento:** En esta primera etapa se llevó a cabo la identificación de los dispositivos mediante escaneo Bluetooth. Se obtuvieron parámetros como nombre del dispositivo, dirección MAC y estado de emparejamiento. Herramientas como hcitool y bluetoothctl fueron utilizadas para listar y monitorizar dispositivos cercanos.
- **Escaneo:** A continuación, se intentó enumerar servicios activos mediante

herramientas como sdptool y btmon, con el fin de descubrir canales abiertos o servicios mal configurados. Este paso permitió establecer que el dispositivo ACCU-CHEK Instant no publica servicios SDP visibles, lo que indica un diseño de seguridad más riguroso, mientras que el canal móvil presentaba más superficie de ataque.

- **Ganar acceso:** Se simularon ataques controlados utilizando herramientas como BlueSnarfer, BlueBugging y Crackle. Si bien no se logró obtener datos o acceso directo, estos intentos permitieron validar la robustez del cifrado implementado. Por ejemplo, Crackle no logró descifrar la clave de emparejamiento debido a que no fue posible capturar correctamente los paquetes de inicio BLE, lo que coincide con estudios recientes sobre los desafíos técnicos del análisis BLE con adaptadores comerciales (Shukla, 2024).
- **Persistencia:** Se evaluó la posibilidad de establecer accesos no autorizados de forma sostenida. Este análisis incluyó el intento de reutilizar claves de emparejamiento, comprobar reconexiones automáticas y examinar si existían respuestas del sistema ante conexiones anómalas.
- **Encubrimiento:** Finalmente, se analizó la capacidad del sistema para registrar los accesos o intentos de intrusión. No se detectaron mecanismos visibles de logging local o alertas en la aplicación vinculada, lo que podría representar un área de mejora en futuras actualizaciones del firmware o de la app.

### 3.1.2. Entorno de pruebas y recursos utilizados

Para garantizar la validez técnica del análisis, se configuró un entorno de laboratorio controlado compuesto por:

- **Sistema operativo:** Kali Linux, ejecutado en VirtualBox con configuración de red aislada.
- **Adaptador Bluetooth:** TP-Link UB500 USB, compatible con BLE.
- **Dispositivos físicos:** ACCU-CHEK Instant y ACCU-CHEK Guide.
- **Aplicación móvil:** mySugr para Android, en versión .apk descargada de forma directa para análisis estático.
- **Herramientas utilizadas:** bluetoothctl, sdptool, btmon, BlueSnarfer, rfcomm,

Crackle, apktool, jadx, Wireshark, hcitool, Crunch.

Este conjunto de herramientas permitió realizar una auditoría básica sin comprometer la integridad de los dispositivos ni la privacidad de los usuarios

### 3.1.3. Análisis de la aplicación móvil

El análisis forense de la app mySugr se llevó a cabo descompilando el APK con apktool y jadx. En el archivo AndroidManifest.xml se identificaron permisos relevantes como:

- **BLUETOOTH y BLUETOOTH_CONNECT:** fundamentales para el emparejamiento BLE.
- **ACCESS_FINE_LOCATION:** exigido por el sistema Android para permitir escaneo BLE.
- **READ_EXTERNAL_STORAGE:** cuya presencia puede representar un riesgo si se abusa de él por otras apps.

Aunque no se detectaron vulnerabilidades críticas ni componentes exportados de forma insegura, se recomienda que los desarrolladores realicen auditorías periódicas del código y de las bibliotecas externas utilizadas, tal como sugiere OWASP (2022).

### 3.1.4. Limitaciones encontradas

Pese al éxito metodológico, se identificaron varias limitaciones técnicas que condicionaron el alcance del análisis:

- Los adaptadores Bluetooth convencionales no permiten captura completa del tráfico cifrado BLE (Terzidis, Mouratidis & Kalloniatis, 2023).
- Algunas herramientas como BlueBorne ya no están activamente mantenidas, lo que dificulta su ejecución en entornos modernos.
- El análisis de tráfico BLE cifrado en tiempo real requiere hardware especializado como el Ubertooth One o el nRF52840 Dongle.

Estas limitaciones no invalidaron los resultados, pero sí sugieren que para futuras investigaciones se utilicen recursos de nivel profesional que permitan acceder a capas más profundas del protocolo.

### 3.1.5. Enfoque ético y normativo

Todas las actividades se realizaron bajo el principio del hacking ético, respetando los límites legales y garantizando que ninguna prueba vulnerara información real o afectara la funcionalidad de los dispositivos. Se observó el marco de controles propuesto por el NIST SP 800-53 Rev. 5 (NIST, 2022) y las directrices de seguridad establecidas en el OWASP IoT Top 10 (OWASP, 2022). Esta práctica no solo protege a los fabricantes y usuarios, sino que también refuerza el compromiso del auditor con la responsabilidad social y profesional.

## 3.2. Propuesta del Trabajo

Varios dispositivos medidores de glucosa están diseñados con la tecnología inalámbrica Bluetooth para establecer una conexión entre un dispositivo móvil, comúnmente con un teléfono inteligente. De este modo se recepta la información obtenida del medidor de glucosa, para su posterior visualización en la aplicación móvil, y así poder monitorear y llevar el control de diabetes del paciente.

Para el presente proyecto de investigación se propone realizar dos pruebas de laboratorio practico, con el fin de hallar posibles vulnerabilidades en los dispositivos medidores de glucosa. El primer laboratorio se lo practicará con el modelo ACCU-CHEK Instant y el segundo laboratorio con el modelo ACCU-CHEK Guide. Cabe mencionar que ambas pruebas se las realizará en un entorno controlado para auditar la seguridad de ambos dispositivos medidor de glucosa.

### 3.2.1. Análisis de factibilidad

El presente proyecto plantea la realización de pruebas prácticas de laboratorio sobre dos dispositivos médicos de tipo IoT: el ACCU-CHEK Instant y el ACCU-CHEK Guide. La propuesta técnica es viable, ya que se cuenta con la posibilidad de adquirir ambos modelos en el mercado comercial, sin restricciones legales ni técnicas que limiten su análisis. El entorno experimental se configurará con herramientas y recursos informáticos de fácil acceso, como una computadora con el sistema operativo Kali Linux y un adaptador Bluetooth USB. Adicionalmente, se emplearán utilidades incluidas en dicha distribución (como hcitool, bluetoothctl, entre otras), ampliamente utilizadas en auditorías de seguridad inalámbrica.

El diseño experimental considera un entorno controlado para evitar interferencias externas y garantizar la repetibilidad de las pruebas. La metodología adoptada sigue las fases tradicionales del hacking ético (reconocimiento, análisis de vulnerabilidades, explotación

controlada y documentación), lo que proporciona un marco técnico confiable y validado por la comunidad de ciberseguridad.

El proyecto se considera económicamente factible, ya que los recursos necesarios no representan una carga significativa. La adquisición de los dispositivos a analizar, junto con los adaptadores Bluetooth y otros materiales complementarios, implica un gasto moderado. Por otro lado, la utilización de software libre y de código abierto como Kali Linux y sus herramientas reduce considerablemente los costos operativos, eliminando la necesidad de licencias comerciales.

Asimismo, el hecho de que el estudio no requiere la contratación de personal adicional ni la implementación de infraestructura compleja permite su ejecución con recursos limitados, ajustándose a presupuestos académicos o de investigación básica.

El enfoque del estudio se alinea con los principios del hacking ético y la ciberseguridad responsable. Al no involucrar datos de pacientes ni intervenir en entornos clínicos reales, el proyecto evita comprometer la privacidad o integridad de usuarios finales. Las pruebas se ejecutarán únicamente sobre los dispositivos en cuestión, respetando su integridad física y sin modificar su funcionalidad de forma permanente.

La investigación tiene un propósito académico y preventivo, orientado a evidenciar posibles brechas de seguridad para fortalecer futuras soluciones. Siempre que se respeten los derechos de autor y se dé el debido reconocimiento al fabricante, no se prevén conflictos legales derivados del estudio.

Desde el punto de vista académico, el tema abordado posee alta relevancia, considerando el creciente uso de tecnologías IoT en el sector salud. La investigación propuesta puede aportar conocimientos útiles sobre la seguridad de dispositivos médicos conectados, un campo que ha captado el interés de investigadores y reguladores por igual.

Existen antecedentes bibliográficos y técnicos sobre vulnerabilidades en dispositivos Bluetooth y sistemas IoT, lo cual proporciona una base teórica sólida para el desarrollo del trabajo. Los resultados del estudio podrían servir como referencia para futuras investigaciones o como insumo para propuestas de mejora en el diseño seguro de este tipo de equipos.

A pesar de su factibilidad general, el proyecto no está exento de riesgos. Entre ellos se encuentra la posible falta de acceso al firmware o documentación técnica detallada de los dispositivos, lo cual podría limitar el análisis en profundidad. Sin embargo, esta limitación

puede mitigarse mediante técnicas de ingeniería inversa no invasiva y monitoreo del tráfico de datos por Bluetooth.

También se contempla la posibilidad de obtener resultados no concluyentes debido a falsos positivos o errores de interpretación. Para ello, se aplicará una validación cruzada con diversas herramientas y métodos, reduciendo el margen de error.

La investigación propuesta se considera factible desde los ámbitos técnico, económico, legal y académico. Los recursos requeridos son accesibles, la metodología se basa en prácticas reconocidas en el campo de la ciberseguridad, y el impacto potencial del estudio es significativo. Por lo tanto, se concluye que el proyecto es viable y representa una contribución válida al análisis de seguridad en dispositivos médicos IoT.

### 3.2.2. Fases de un ataque hacker

Se explican las cinco fases importantes para llevar a cabo con éxito el ataque. La persona que realiza el ataque de forma ética va a comprender como piensa una persona malintencionada o un hacker de manera que sirva de ayuda, conociendo la estrategia del ataque, para tomar medidas y mitigar el riesgo de seguridad.

- **Reconocimiento:** En esta fase se realiza el estudio previo que un atacante realiza hacia su objetivo. Se extrae toda la información posible (sistema operativo, dirección IP, aplicaciones, entre otros.) que sirva de ayuda al atacante para planear el ataque.
- **Escaneo:** Una vez obtenida toda la información de la fase anterior, el atacante debe analizar la información que le sirva e identificar las características, para luego hallar vulnerabilidades. Esta fase es importante enfocarse en los puertos puesto que es clave para un ataque.
- **Ganar acceso:** En esta fase el hacker deberá aplicar la estrategia planeada, una vez encontrada las vulnerabilidades en la fase anterior. El atacante deberá poner en marcha sus habilidades y el uso de herramientas para el tipo de ataque que desea realizar. Entre los ataques más conocidos se encuentran el secuestro de sesión. Esta fase es crucial dado que el atacante o hacker podrá ver el alcance exitoso que pueda tener su penetración.
- **Mantener el acceso:** Es la fase en la que el atacante deberá mantener el acceso que gano en el sistema manejando diversas herramientas como es el caso de los sniffers (usados para capturar el tráfico en la red). En esta fase

debe iniciar sesiones telnet y FTP.

El hacker debe permanecer indetectable para el objetivo debido a que, si no quiere ser descubierto, este debe hacer uso de ataques de programas maliciosos (Backdoor y Troyanos) para su persistencia en el sistema informático y así ganar accesos con altos niveles de privilegio, como lo es un administrados.

- **Cubrir las huellas:** En esta fase el atacante deberá hacer uso de herramientas para evitar que sea descubierto por los administradores del sistema, para cuando el administrador realice análisis de tráfico, este pueda ver los registros de acceso de un usuario desconocido (Mamani, 2013).

# CAPITULO 4

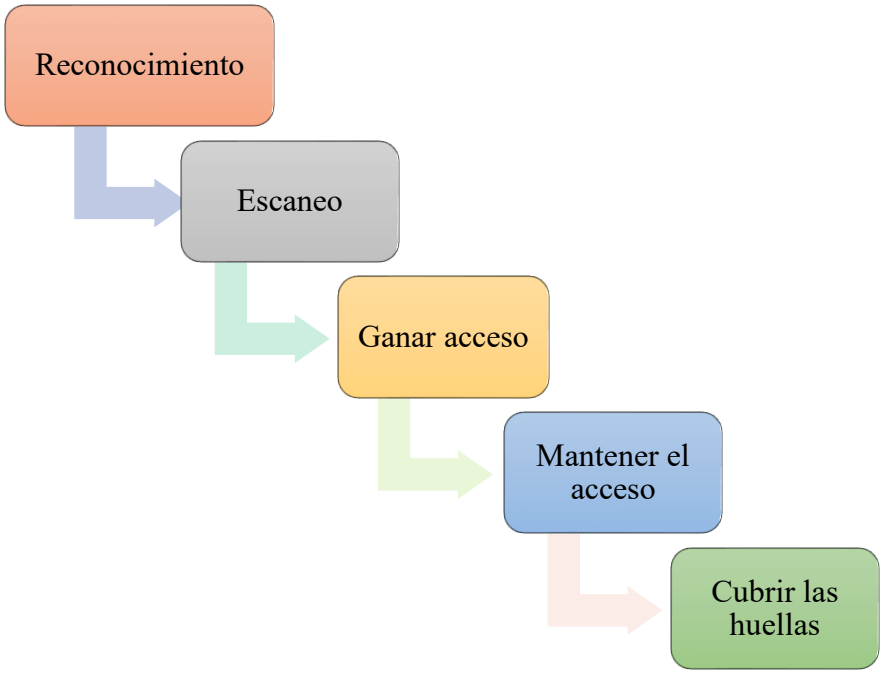
## 4. ANÁLISIS DE RESULTADOS

### 4.1. Pruebas de Concepto

En esta parte del proyecto se implementará las distintas fases de hacking ético aplicadas a hackeo de dispositivo medidor de glucosa con tecnología Bluetooth, aplicando el modelo clásico o cascada dado que es un proceso secuencial y cada fase se deberá completar antes de pasar a la siguiente. El modelo en cascada utilizado en la presente investigación se incorpora en la Figura 3.

**Figura 3**

*Modelo en cascada fases de hacking*




*Nota*. Fases de hacking ético que se aplicará a hackeo de Bluetooth.

#### 4.1.1. Escenario 1: prueba de laboratorio practico

En este escenario se va a aplicar auditoría de seguridad para el dispositivo IoT médico medidor de glucosa, especialmente el modelo ACCU-CHEK Instant, con el objetivo de identificar posibles vulnerabilidades del dispositivo. Cabe mencionar que todo se realizará en un entorno controlado y con fines educativos.

Para aplicar las distintas fases comúnmente aceptadas en el proceso de hacking, se le va a adaptar con hacking Bluetooth.

**Fase de reconocimiento**

En esta fase se realiza la búsqueda de información del objetivo que se va a atacar (dispositivo medidor de glucosa ACCU-CHEK Instant), que resulte de importancia para planificar el ataque.

ACCU-CHEK Instant es un dispositivo que sirve para monitorear los niveles de glucosa en la sangre. Este dispositivo transmite los datos a través de conexión inalámbrica Bluetooth, y para visualizar los resultados de la medición de glucosa, esta se la monitorea por medio de la aplicación móvil mySugr (iOS y Android).

El tema que nos enfocaremos es la conexión Bluetooth, debido a que hay mucha información relacionada a este tipo de vulnerabilidades.

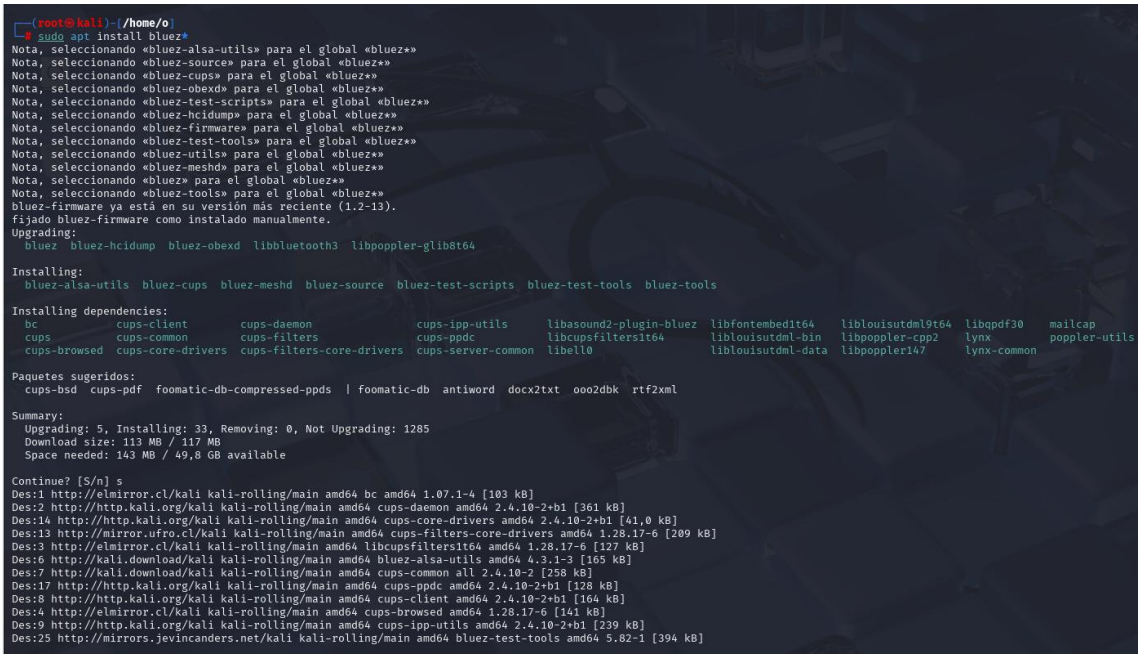
Para empezar con el laboratorio, se debe tener preparado la máquina con Kali Linux (máquina para realizar pruebas de penetración y hacking ético). La máquina Kali Linux se encuentra virtualizada en VirtualBox.

Abrimos una terminal en Kali para actualizar paquetes y herramientas antes de iniciar el reconocimiento Bluetooth. Posteriormente hay que instalar Bluetooth en Kali.

Se debe verificar si se tiene instalado BlueZ dado que es una la pila Bluetooth de Linux compatible con los dispositivos Bluetooth.

**Figura 4**

*Instalar BlueZ*

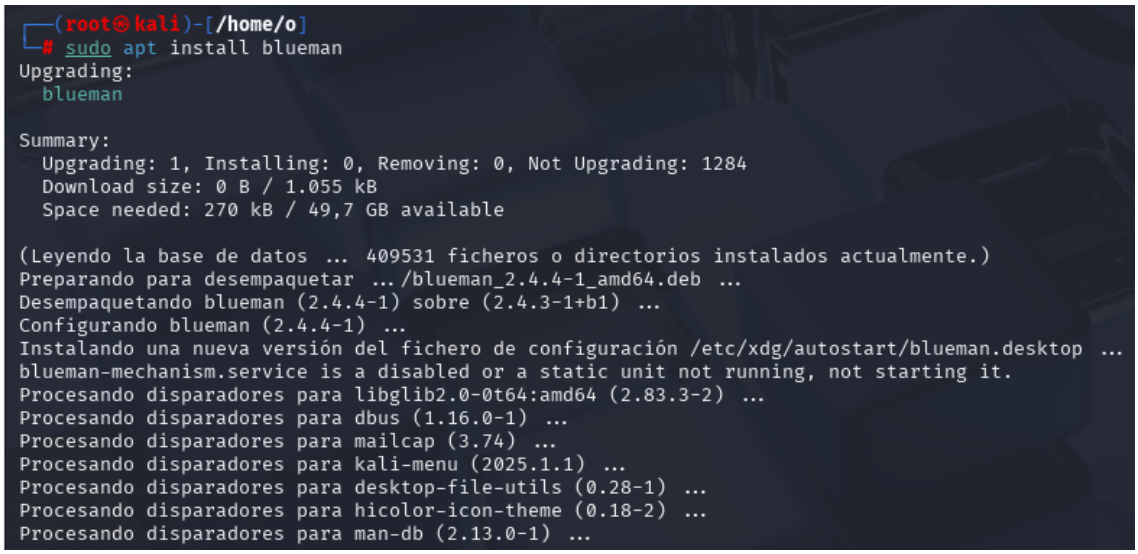



*Nota*. Instalación de BlueZ mediante comando.

Ahora instalamos Blueman, interfaz gráfica para gestionar conexiones Bluetooth.

**Figura 5**

*Instalar Blueman*

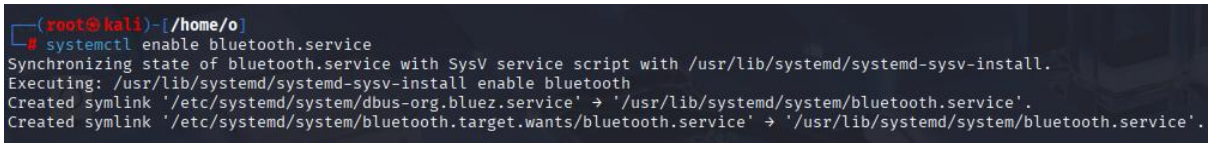



*Nota*. Instalación de Blueman mediante comando.

Habilitamos el servicio Bluetooth.

**Figura 6**

*Habilitar Bluetooth*

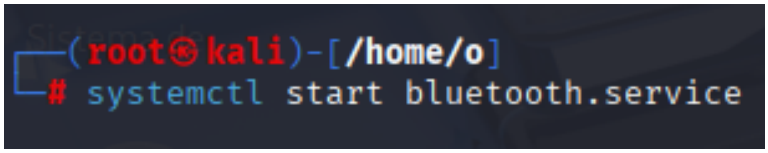



*Nota*. Habilitación del servicio Buetooth.

Ahora iniciamos el servicio Bluetooth.

**Figura 7**

*Iniciar Bluetooth*

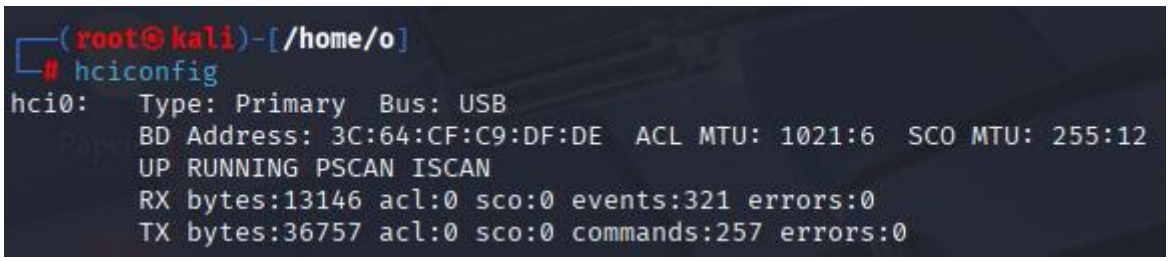



*Nota*. Tenemos nuestro servicio Bluetooth corriendo.

Una vez preparado todo para que funcione correctamente el servicio Bluetooth, utilizamos el comando “hciconfig” ya que es de utilidad para que interactúe con dispositivos Bluetooth (Tutorials Point, s.f.).

**Figura 8**

*Hciconfig*




*Nota*. Comando para interactuar con dispositivos Bluetooth.

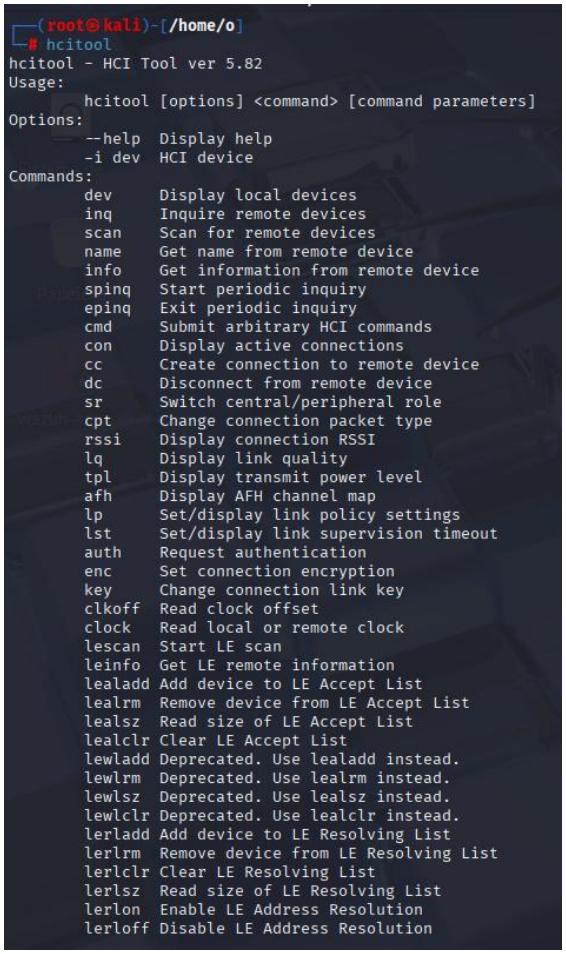
Como se puede ver, ya tenemos funcionando nuestro adaptador USB. Este comando nos muestra la interfaz y la dirección MAC del dispositivo.

Activamos el Bluetooth del móvil y del dispositivo medidor de glucosa ACCU-CHEK Instant para transferir los datos y mediante la aplicación mySugr visualizamos los resultados obtenidos.

Dentro de la utilidad “hcitool” nos encontramos con la opción que nos interesa, scan.

**Figura 9**

*Opciones hcitool*

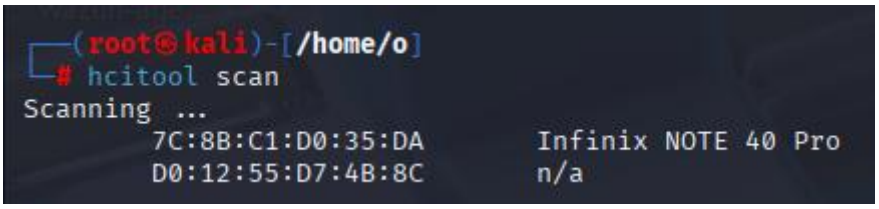


*Nota*. Opciones de comandos disponibles para interactuar con la pila de Bluetooth.

Empezamos utilizando el comando “hcitool scan”, que nos va a servir para detectar el dispositivo Bluetooth ACCU-CHEK Instant.

**Figura 10**

*Hcitool scan*



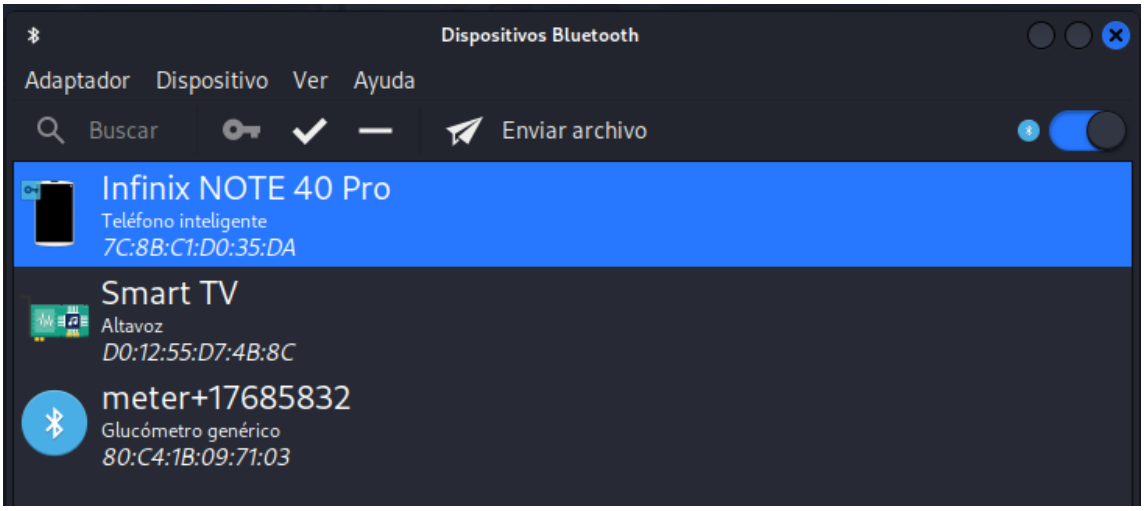

*Nota*. Dispositivos Bluetooth disponibles.

Con el comando scan, no se puedo obtener el dispositivo ACCU-CHEK Instant, sin embargo, nos arrojó información del dispositivo móvil conectado al glucómetro. Nos dio información como el nombre disponible del Bluetooth y la dirección MAC del mismo (Infinix NOTE 40 Pro).

Intentaremos de forma manual buscar el dispositivo glucómetro, en la opción en el adaptador Bluetooth.

**Figura 11**

*Buscar dispositivos Bluetooth*



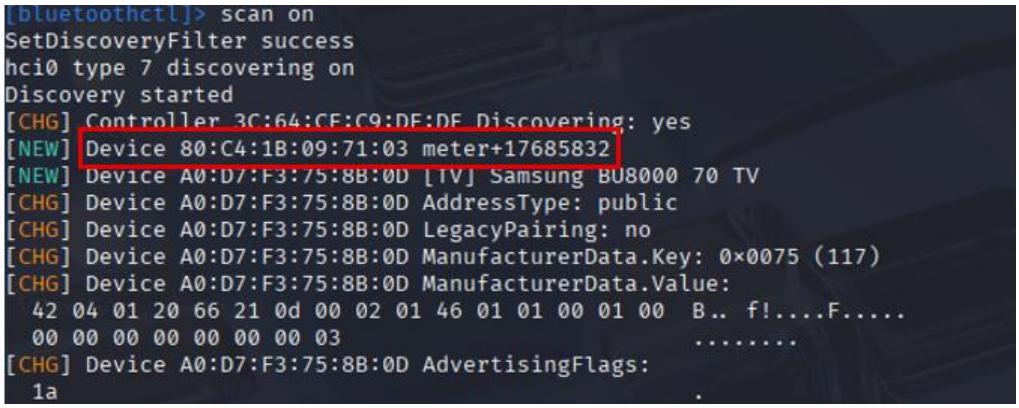

*Nota*. Dispositivos Bluetooth encontrados.

De esta manera se pudo encontrar el dispositivo glucómetro ACCU-CHEK Instant, arrojando información importante como la dirección MAC (80:C4:1B:09:71:03), de igual manera la información del dispositivo móvil sincronizado con el glucómetro.

Aplicamos otra herramienta “bluetoothctl” para ver si nos arroja más información del glucómetro.

**Figura 12**

*Herramienta bluetoothctl*




*Nota*. Dispositivo glucómetro se encuentra disponible para ser emparejado.

Tal cual que la otra utilidad entre las herramientas de Kali Linux, esta nos da información (MAC del dispositivo ACCU-CHEK Instant y el nombre disponible como se reconoce al dispositivo Bluetooth) interesante.

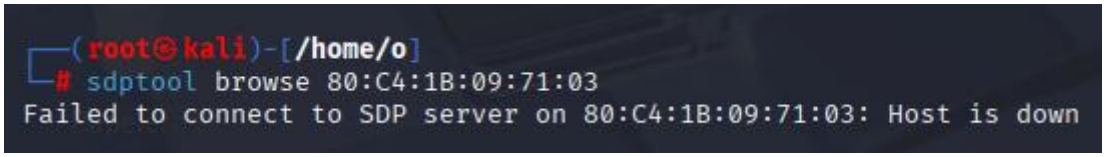
**Fase de escaneo**

En esta fase se va a tratar de obtener más información del dispositivo ACCU-CHEK Instant, información como descubrimientos de servicios que se ejecutan en el dispositivo glucómetro.

Empezamos con la herramienta “sdptool” porque esta interactúa con el servicio de descubrimiento. La herramienta nos enumeraría los servicios que se encuentran disponibles en el dispositivo Bluetooth ACCU-CHEK Instant.

**Figura 13**

*Herramienta sdptool*

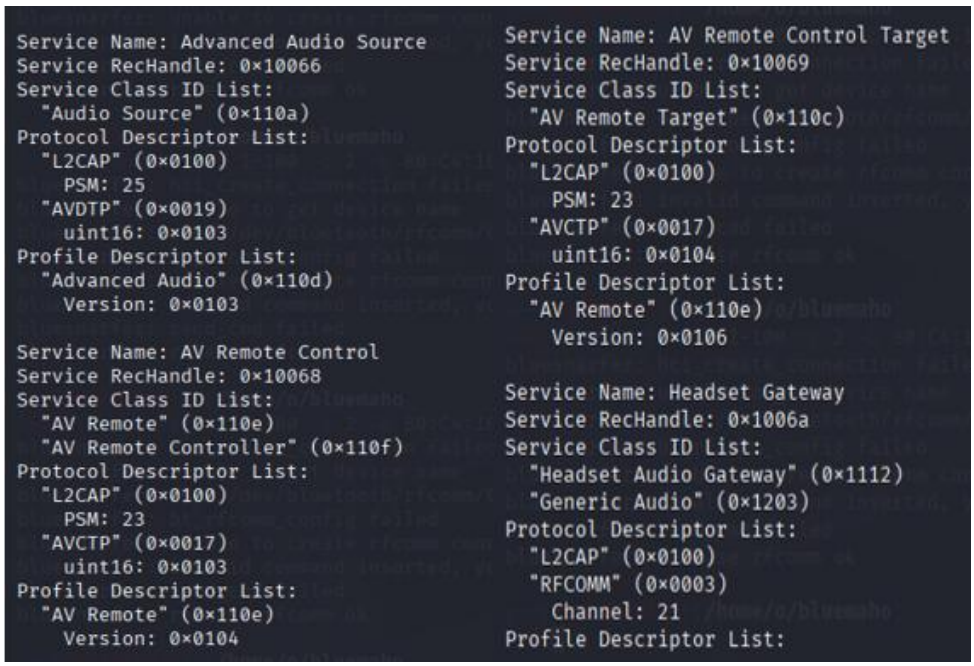



*Nota*. En busca de servicios que podría tener el glucómetro.

Posterior al escaneo, este indica que el servicio de descubrimiento de servicio público (SDP) no se encuentra o el dispositivo ACCU-CHEK Instant no ofrece este servicio. Al igual se hizo el escaneo al móvil de la víctima, y este si arrojó información de los servicios públicos.

**Figura 14**

*Sdptool aplicado al móvil*

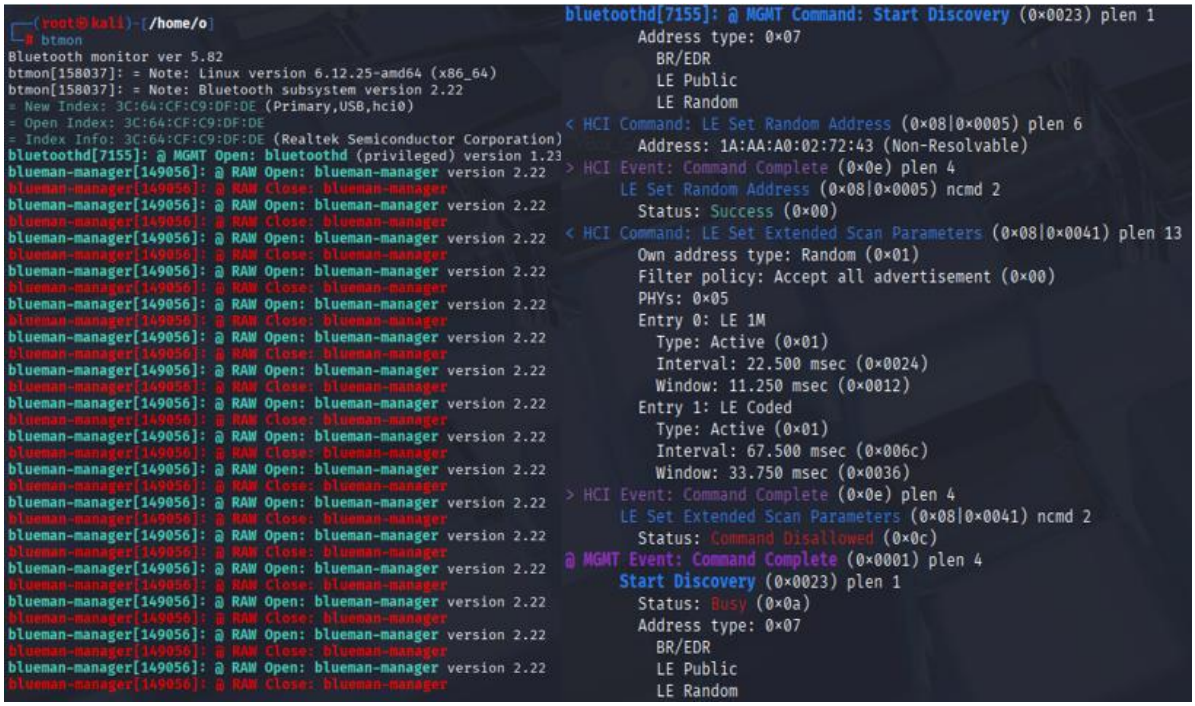



*Nota*. Servicios habilitados en el móvil.

Para analizar el tráfico Bluetooth se va a utilizar la herramienta básica “btmon”, que viene preinstalada en Kali Linux. Esta herramienta permite el monitoreo del tráfico Bluetooth.

**Figura 15**

*Herramienta btmon*



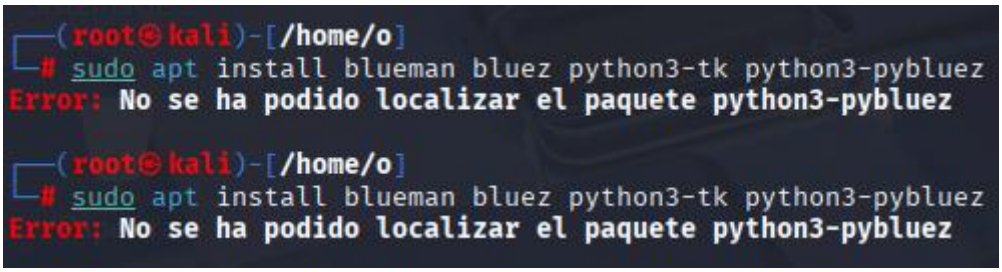

*Nota*. Con btmon analizamos el tráfico Bluetooth.

Sin embargo, btmon al ser una herramienta que es utilizada por adaptadores Bluetooth USB estándar, posee pocas limitaciones en la captura de tráfico Bluetooth, como no es el caso de un dispositivo hardware dedicado y más sofisticado para este propósito.

También se quiso utilizar la herramienta "BlueMaho" para probar la seguridad del dispositivo Bluetooth glucómetro ACCU-CHEK Instant, con el fin de que nos brindara información como registro de servicios públicos, buscar vulnerabilidades conocidas como desconocidas y sniffing básico de tráfico Bluetooth, pero no se pudo obtener dicha información. Además, hay que tener en cuenta que muchos de estos repositorios se encuentran alojados en GitHub y algunos se encuentran discontinuados y otros ya no se encuentran disponibles, como es el caso de esta herramienta BlueMaho.

**Figura 16**

*Herramienta BlueMaho*




*Nota*. Fallo en la instalación de paquete BlueMaho.

**Fase de ganar acceso**

En esta etapa nos enfocaremos en aplicar los tipos más comunes de ataques de Bluetooth, a pesar de que en la fase anterior no se pudo encontrar vulnerabilidades específicas del dispositivo glucómetro ACCU-CHEK Instant.

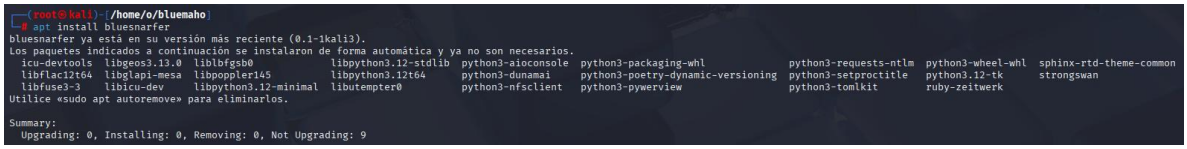
- **BlueSnarfing:** Acceso no autorizado a la información de un dispositivo Bluetooth como mensajes, datos, entre otros. El atacante necesita estar en un rango en el que se encuentre el dispositivo para explotar esta vulnerabilidad (Gupta, 2024).

  Con este ataque se pretende saltar el proceso de autenticación del dispositivo Bluetooth ACCU-CHEK Instant, para acceder a información confidencial (datos de glicemia en la sangre) del usuario.

  Hay que instalar esta herramienta que en algunos casos no viene preinstalada en Kali.

**Figura 17**

*Herramienta BlueSnarfer*

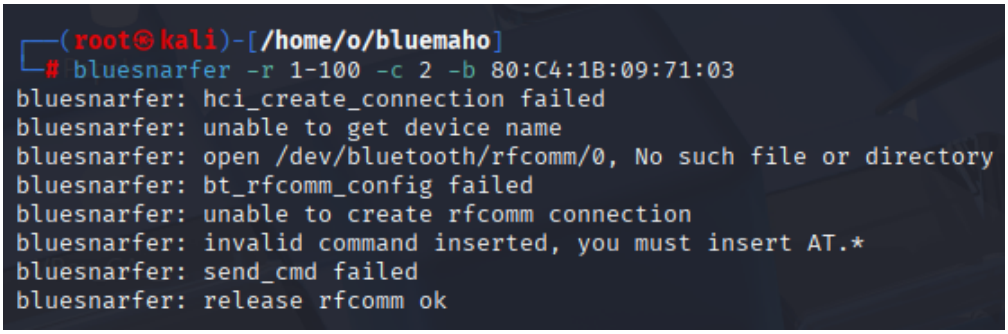



*Nota*. Instalación de herramienta BlueSnarfer.

Aplicamos una línea de comando con la herramienta BlueSnarfer seguido de la dirección MAC del dispositivo del objetivo.

**Figura 18**

*Herramienta BlueSnarfer*




*Nota*. Herramienta de acceso no autorizado al dispositivo objetivo.

Utilizando esta herramienta para obtener acceso no autorizado al dispositivo ACCU-CHEK Instant, no se puedo obtener respuesta. Esto se debe a que el adaptador Bluetooth USB que se está utilizando no posee la Interfaz del Controlador de Host (HCI), misma que sirve para la comunicación entre el host (ACCU-CHEK Instant) y el controlador Bluetooth (Adaptador USB Bluetooth 5.3).

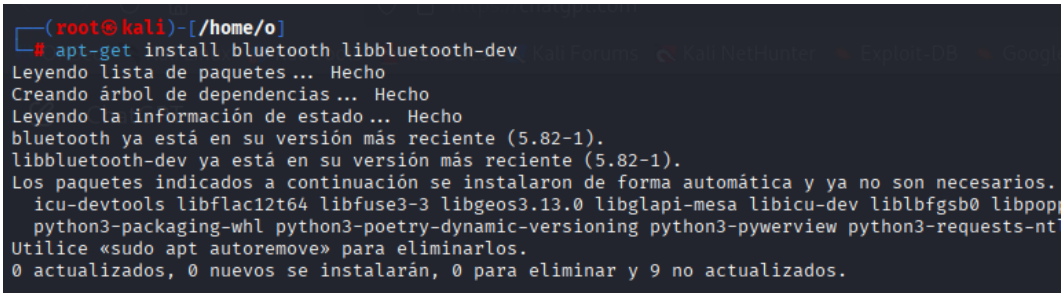
- **BlueBorne:** Este ataque es uno de los más peligrosos para dispositivos que posean vulnerabilidades. Va a permitir que el atacante tenga el control total del dispositivo, sin necesidad de que el usuario toque algún botón ni tampoco se vincule con el dispositivo del atacante (Gupta, 2024).

  Se pretende tomar el control total del dispositivo ACCU-CHEK Instant, explotando alguna vulnerabilidad del glucómetro. Una vez se tome el control del dispositivo, podremos acceder a los datos confidenciales (datos de glicemia en la sangre), y si es posible ejecutar malware.

  Vamos a tener que instalar algunas dependencias que se necesitan en nuestra maquina Kali.

**Figura 19**

*Instalación de librería*

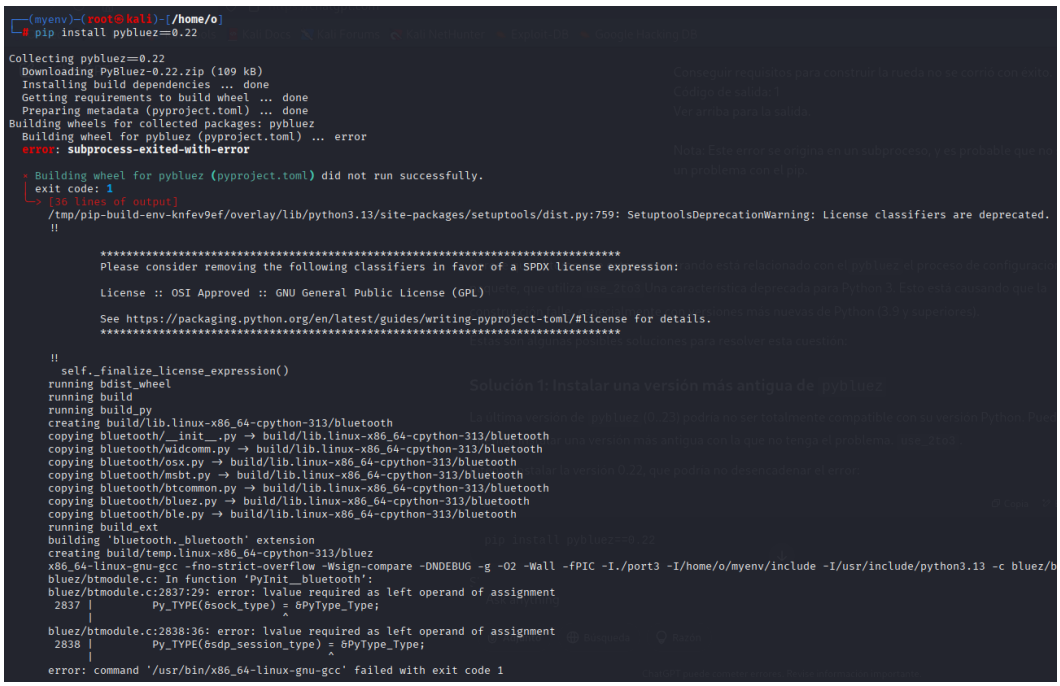



*Nota*. Librerías necesarias.

Al querer instalar las demás dependencias, ocurrió un error dado que esta herramienta se encuentra obsoleta, y si intento descargar la versión más antigua de Python para que proceda con la instalación, y persiste el problema porque ya no se encuentra habilitada esta herramienta.

**Figura 20**

*Instalación de Python versión 2*




*Nota*. Intento de instalar versión anterior de Python.

Adicional se intentó mediante la clonación del repositorio, al igual esta se encuentra no disponible.

**Figura 21**

*Clonación de repositorio BlueBorne*

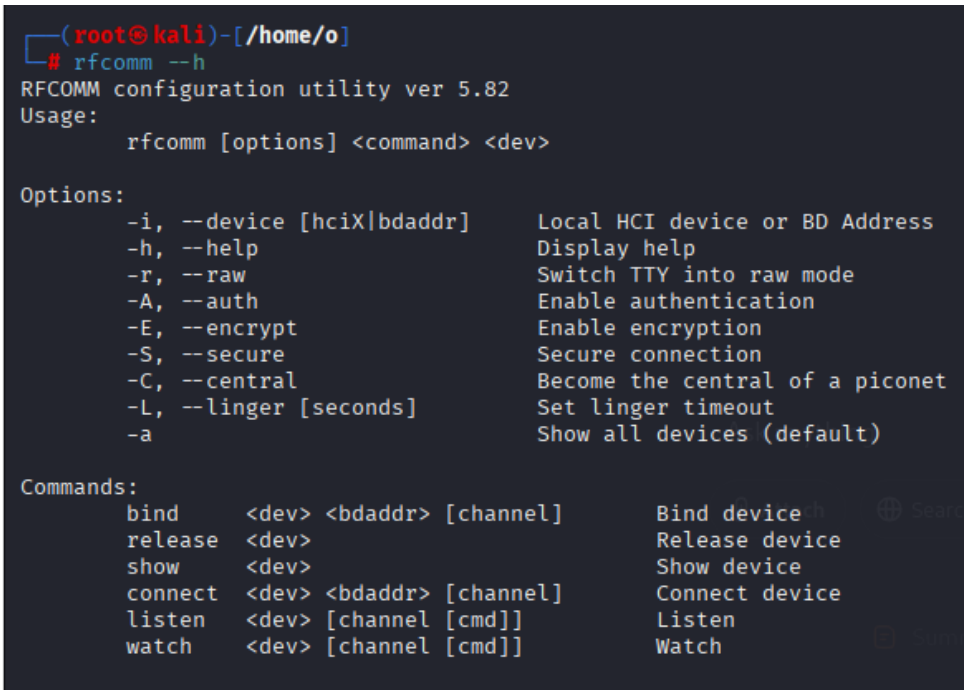

*Nota*. Repositorio BlueBorne ya no se encuentra disponible.

- **BlueBugging:** Este ataque va a permitir que el atacante (maquina Kali) pueda tomar el control remoto del dispositivo Bluetooth (ACCU-CHEK Instant) que sea vulnerable sin autorización.

  Empezamos con instalar la herramienta rfcomm en caso de que no venga preinstalada. Con esta herramienta intentaremos conectar al dispositivo glucómetro mediante un puerto serie.

**Figura 22**

*Consultar herramienta rfcomm*

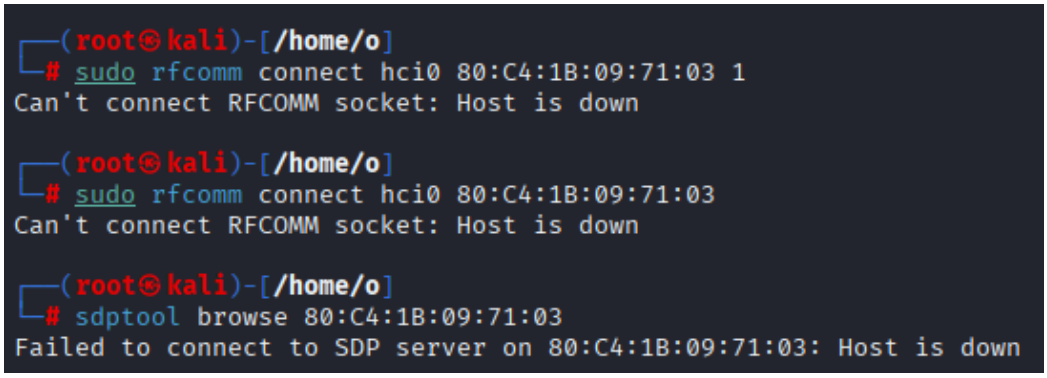



*Nota*. Consultando si la herramienta rfcomm se encuentra disponible en Kali.

Como ya conocemos la dirección MAC de nuestro objetivo, aplicamos una línea de comando para tratar de conectarse al glucómetro.

**Figura 23**

*Conectarse al dispositivo glucómetro*




*Nota*. Uso de rfcomm para conexión con el glucómetro.

Por esta vía tampoco se puedo encontrar la vulnerabilidad de poder conectarse remotamente al dispositivo y su posterior interacción. Esto se debe a que el dispositivo ACCU-CHEK Instant no funciona con la herramienta rfcomm dado que el glucómetro utiliza BLE y rfcomm no es compatible con el mismo.

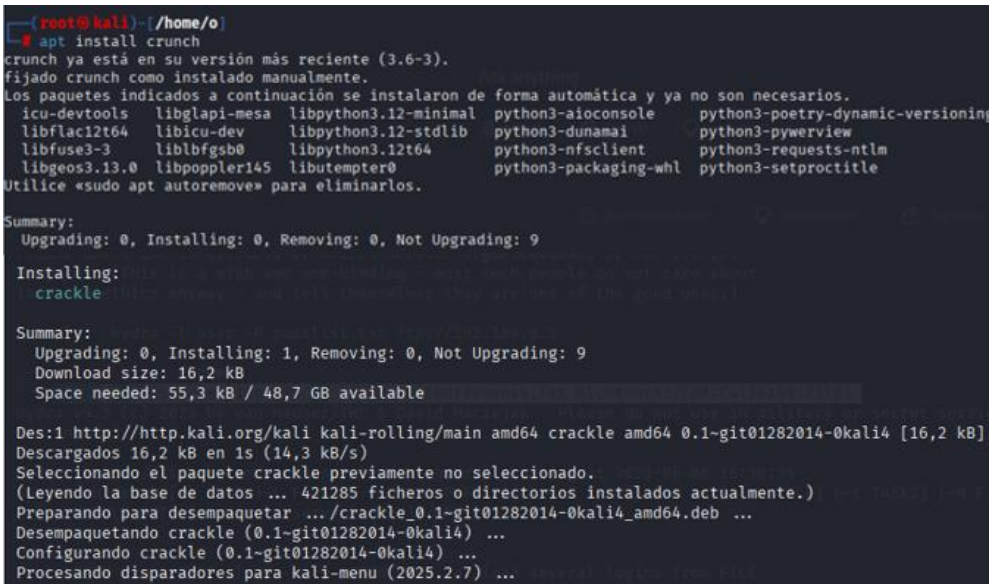
- **Ataque por fuerza bruta:** En esta parte se va a intentar obtener el PIN del dispositivo glucómetro a través de crear una lista con posibles PIN y así tener éxito para su emparejamiento (Gupta, 2024).

  Se debe comprobar si se tiene instalada la herramienta Crunch (herramienta para generar una lista de palabras).

  Al igual que la herramienta Crackle (herramienta para descifrar contraseñas) se debe verificar si viene instalada.

**Figura 24**

*Herramienta Crunch e Crackle*

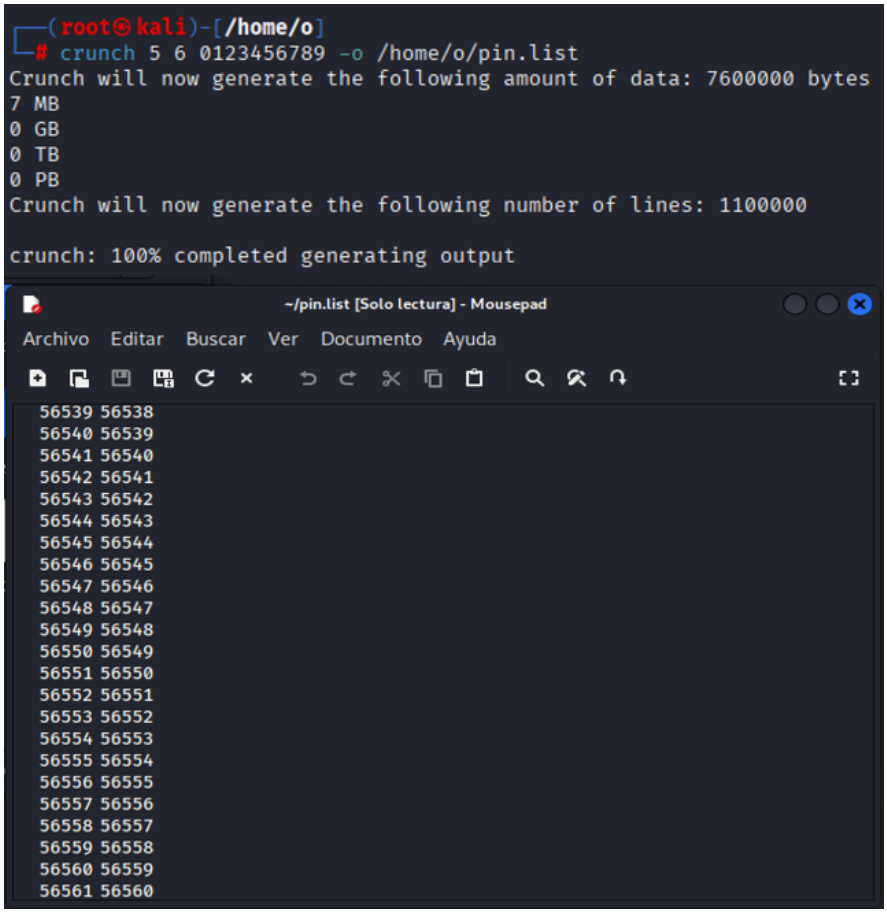



*Nota*. Herramientas ya se encuentran instalada en su última versión.

Creamos una lista de números que sirvan para pines potenciales.

**Figura 25**

*Lista de números*




*Nota*. Números potenciales para el PIN para emparejar el glucómetro.

Ahora vamos a utilizar la herramienta Crackle para forzar e intentar que adivine el PIN.

**Figura 26**

*Herramienta Crackle*


*Nota*. Crackle para atacar conexiones Bluetooth.

Nos dio error que no existen este tipo de archivo, esto se debe a que el adaptador que tenemos para realizar la auditoria no trabaja en modo monitor y no se puede capturar el tráfico Bluetooth del dispositivo glucómetro. Por ende,

la herramienta Crackle no podrá romper el cifrado de claves y poder obtener el emparejamiento con el dispositivo ACCU-CHEK Instant.

**Fase de Mantener el acceso**

Esta fase no fue posible aplicarla puesto que en la fase anterior no se encontraron vulnerabilidades del dispositivo ACCU-CHEK Instant y servicios que se podrían explotar con los recursos que se tienen para la auditoría. Por ende, tampoco entraría en juego la fase de cubrir las huellas.

### 4.1.2. Escenario 2: prueba de laboratorio practico

En este escenario se va a aplicar auditoría de seguridad para el dispositivo IoT médico medidor de glucosa, especialmente el modelo ACCU-CHEK Guide y su aplicación asociada mySugr, el objetivo principal fue identificar vulnerabilidades potenciales en la comunicación Bluetooth Low Energy (BLE) y evaluar la seguridad en el manejo de datos personales de salud dentro de la aplicación.

El laboratorio se divide en dos fases: (1) análisis del entorno Bluetooth del dispositivo físico y (2) análisis forense estático de la aplicación móvil mySugr mediante herramientas de ingeniería inversa.

**Fase 1: Análisis del entorno Bluetooth del dispositivo ACCU-CHEK Guide**

Para la fase 1 los recursos utilizados fueron los siguientes:

- Sistema operativo Kali Linux (VM sobre host macOS)
- Adaptador Bluetooth USB TP-Link UB500
- Herramientas: bluetoothctl, Wireshark
- Dispositivo ACCU-CHEK Guide
- Aplicación móvil mySugr (Android)

**Resumen de herramientas utilizadas:**

- **bluetoothctl:** interfaz interactiva para gestionar conexiones Bluetooth en sistemas Linux.
- **Wireshark:** herramienta de análisis de tráfico de red, utilizada para inspeccionar paquetes a nivel de enlace, incluyendo BLE si el hardware lo

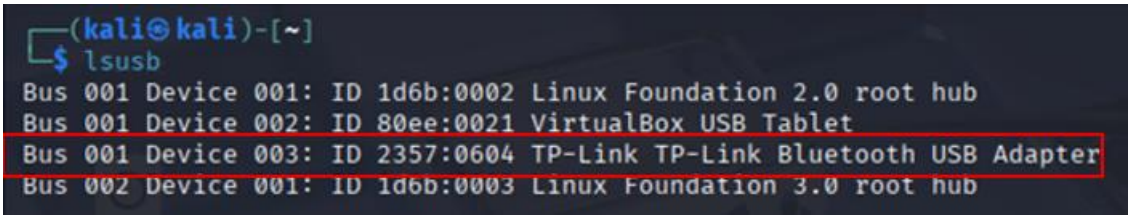
permite.

**Procedimiento y resultados**

Se realizo la detección del adaptador Bluetooth USB TP-Link UB500 mediante el comando lsusb que lista los dispositivos USB conectados al sistema.

**Figura 27**

*Comando lsusb*




*Nota*. Adaptador bluetooth reconocido en máquina virtual.

Adicionalmente validamos que el estado del bluetooth en la máquina virtual se encuentre activa.

**Figura 28**

*Estado de bluetooth en maquina virtual*

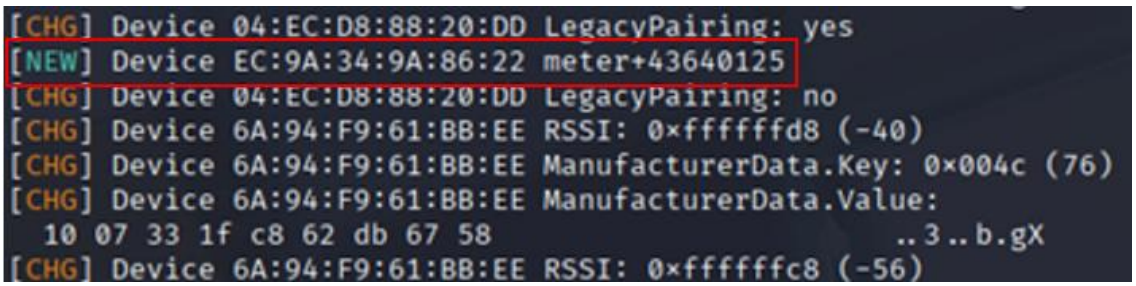

*Nota*. Estado de bluetooth en máquina virtual activa.

Se valido el estado activo del bluetooth en la máquina virtual.

Se realizó la detección del dispositivo mediante bluetoothctl, observándose su emisión BLE bajo el identificador meter+43640125.

**Figura 29**

*Escaneo bluetooth*



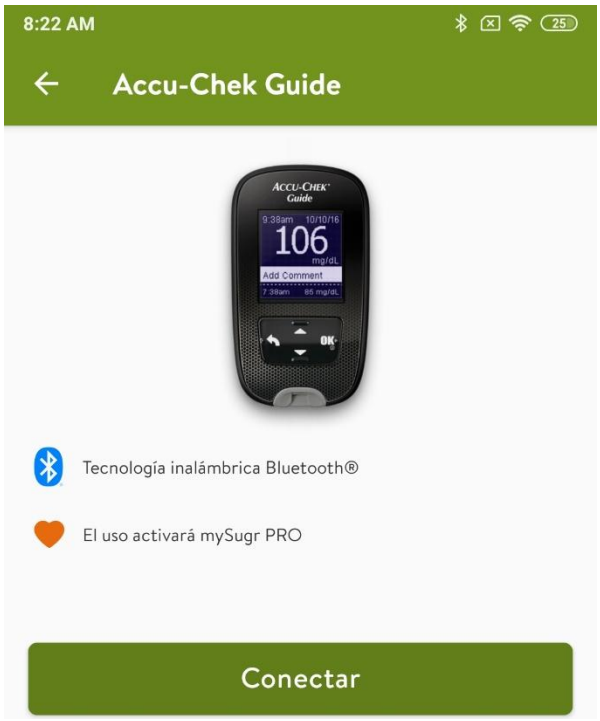

*Nota*. Escaneo de dispositivos bluetooth.

Se valido que el dispositivo si es reconocido en el escaneo mediante el adaptador bluetooth TP-Link.

Asimismo, se planeó utilizar la herramienta Wireshark para capturar el tráfico BLE entre el dispositivo ACCU-CHEK Guide y la aplicación móvil.

**Figura 30**

*Aplicación Movil mysugr*

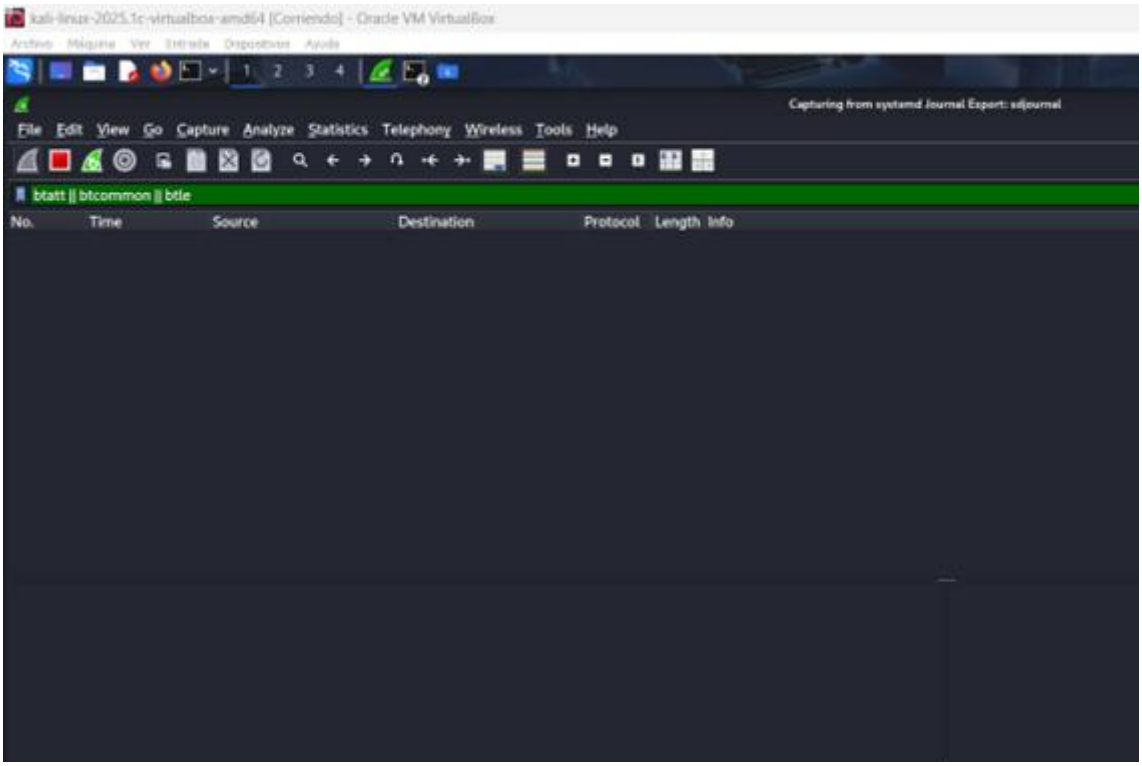



*Nota*. Aplicación Móvil para conexión bluetooth con ACCU-CHEK Guide.

El procedimiento incluía la selección de la interfaz de red Bluetooth y la observación de paquetes publicitarios o de conexión durante el emparejamiento. Sin embargo, al iniciar la captura, no se obtuvieron resultados visibles.

**Figura 31**

*Herramienta Wireshark*




*Nota*. Wireshark sin detección de paquetes esperados.

Este resultado puede atribuirse a varias causas: uso de cifrado en la conexión BLE, diseño del dispositivo para no transmitir paquetes hasta estar emparejado correctamente, o limitaciones del adaptador utilizado que impidieron el modo de captura promiscuo requerido por Wireshark para dispositivos BLE. Las transmisiones BLE modernas implementan cifrado de enlace para proteger datos médicos, y esto representa un reto adicional en contextos de auditoría sin hardware especializado.

Se concluye que, con los recursos disponibles, no fue posible interceptar el tráfico BLE del ACCU-CHEK Guide. Esto sugiere el uso de cifrado en las comunicaciones o técnicas de emparejamiento seguras como Just Works o Passkey Entry (Developers, 2021).

**Conclusión de esta fase**

A pesar de no poder capturar el tráfico BLE, se verificó la emisión del dispositivo y se ejecutaron múltiples intentos con herramientas estándar. Esto demuestra la implementación de mecanismos de seguridad en dispositivos médicos modernos, pero también limita las capacidades de auditoría sin hardware especializado.

**Fase 2: Análisis estático de la aplicación móvil mySugr**

Para la fase 2 los recursos utilizados fueron los siguientes:

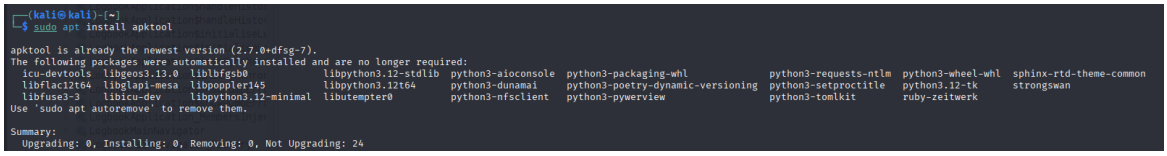
- **Archivo APK:** com.mysugr.android.companion.apk
- **Herramientas:** apktool
- Sistema operativo Kali Linux

**Resumen de herramientas utilizadas:**

- **apktool**: herramienta de línea de comandos que permite descompilar archivos APK para inspeccionar recursos y archivos de configuración.

**Figura 32**

*Herramienta apktool*



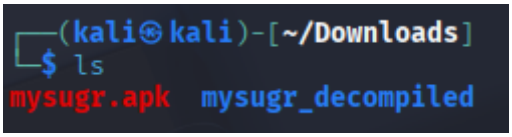

*Nota*. Instalación de apktool en máquina virtual.

**Procedimiento y resultados**

Se realizo la descompresión del archivo con la herramienta apktool de mySugr.apk que corresponde al instalador de la aplicación utilizada por el glucómetro para sincronizar sus datos de manera inalámbrica. Esto con el objetivo de validar alguna vulnerabilidad de manera de ingeniería inversa estático.

**Figura 33**

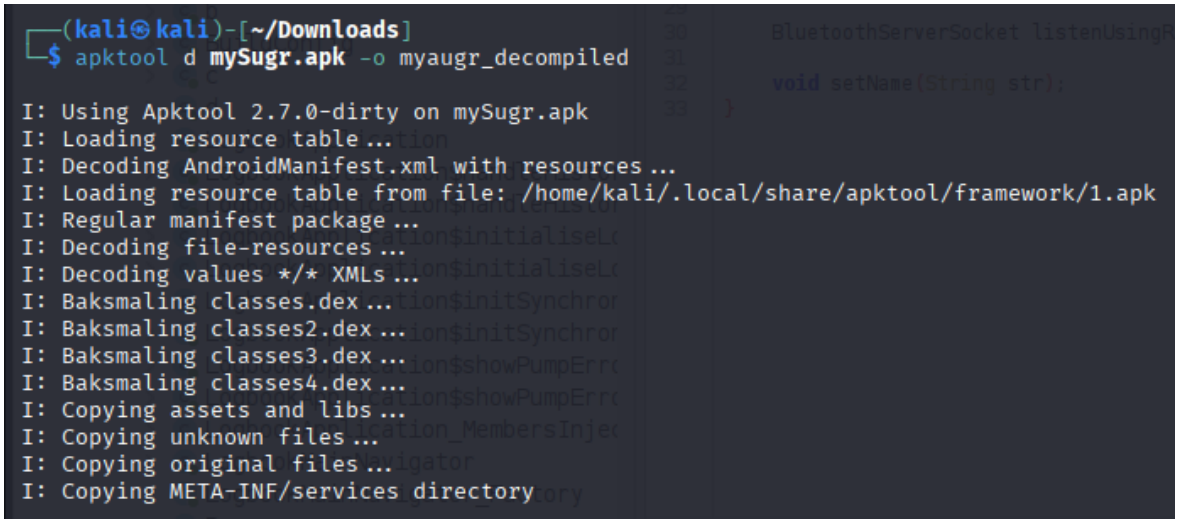
*apk descargada para analisis*




*Nota*. Apk mysugr para análisis

**Figura 34**

*Herramienta apktool para descompresion*




*Nota*. Descompresión archivo .apk para análisis.

Se obtienen los siguientes indicadores para análisis.

**Figura 35**

*Archivos obtenidos*


*Nota*. Archivos obtenidos para análisis.

**Análisis del AndroidManifest.xml**

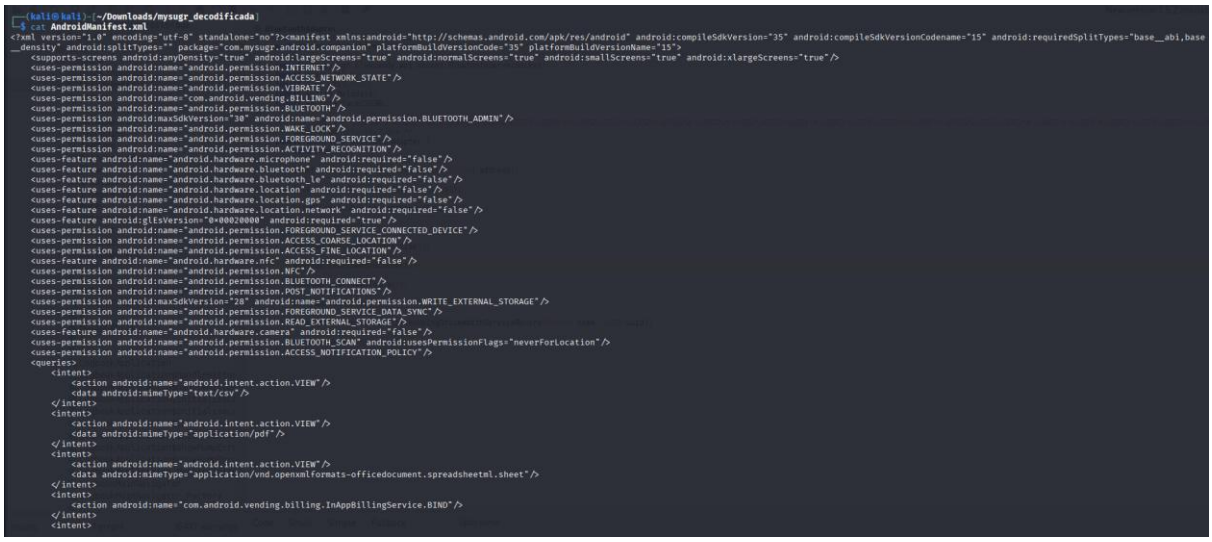
Se realizo el análisis del archivo AndroidManifest.xml.

Antes de iniciar con el análisis detallado de permisos y componentes, es importante destacar que el archivo AndroidManifest.xml es un elemento esencial en cualquier aplicación Android. Este archivo define los componentes principales (actividades, servicios, proveedores), los permisos requeridos, las configuraciones del sistema, y las intenciones que puede manejar la aplicación. En el contexto de la ciberseguridad, su revisión permite identificar posibles excesos de permisos, configuraciones de exportación de componentes que podrían ser atacables, y dependencias de servicios que revelen el uso de tecnologías específicas.

El análisis de este archivo se considera una buena práctica en evaluaciones de seguridad estática, ya que es accesible incluso sin ejecutar la aplicación y proporciona un mapa general del comportamiento esperado.

**Figura 36**

*Archivo AndroidManifest.xml*



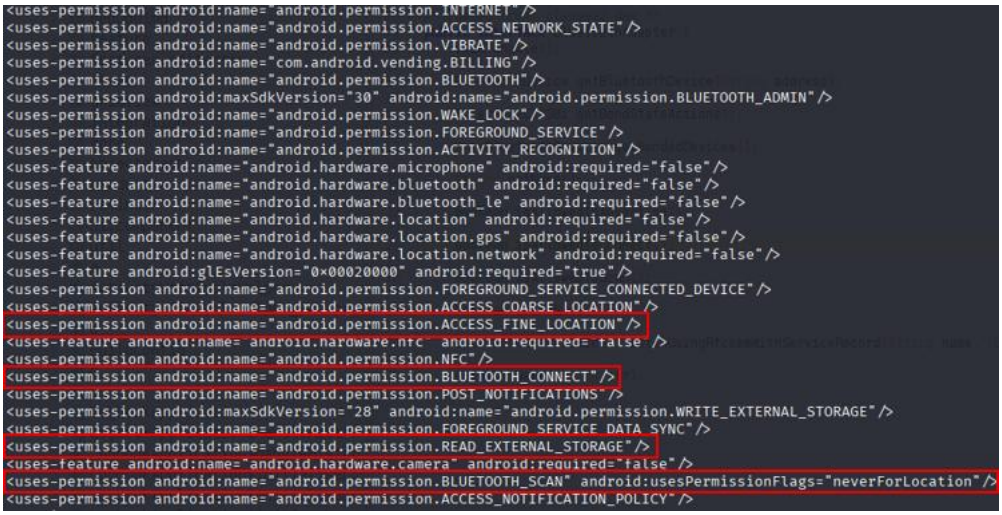

*Nota*. Análisis del archivo AndroidManifest.xml.

El archivo AndroidManifest.xml reveló una serie de permisos que implican potenciales riesgos de seguridad si no se gestionan correctamente. Entre los más relevantes están:

- **android.permission.BLUETOOTH, BLUETOOTH_CONNECT, BLUETOOTH_SCAN:** necesarios para la comunicación BLE.
- **ACCESS_FINE_LOCATION:** requisito de Android para escanear dispositivos BLE.
- **READ_EXTERNAL_STORAGE:** potencial exfiltración de datos si no está adecuadamente protegido.

**Figura 37**

*Permisos en archivo AndroidManifest.xml*



*Nota*. Permisos relevantes en AndroidManifest.xml.

La aplicación mySugr muestra buenas prácticas en la declaración de permisos y en el manejo de strings estáticos. No se encontraron evidencias de claves duras ni endpoints inseguros. Sin embargo, el uso de permisos críticos justifica una auditoría dinámica futura.

### 4.2. Análisis de Resultados

En efecto del laboratorio practico 1, como evidencia en la fase de reconocimiento se pudo obtener información importante del dispositivo (ACCU-CHEK Instant), como el nombre visible para conexión Bluetooth (meter+17685832) y la dirección MAC (80:C4:1B:09:71:03). Adicional se buscó información en motores de búsqueda (CVE Details, Exploit Database, GitHub, etc.) y no se obtuvo información ninguna. La información básica que tiene no es suficiente como para planificar el ataque al dispositivo glucómetro. En cambio, en la fase de escaneo se quiso obtener información de servicios públicos disponibles del dispositivo, y el resultado mostró que dichos servicios no se encuentran disponibles. La fase ganar acceso no se realizó con éxito dado que sin contar con vulnerabilidades encontradas del dispositivo ACCU-CHEK Instant referente a la conexión Bluetooth, de igual manera se intentó aplicar los ataques más comunes de Bluetooth (BlueSnarfing, BlueBorne, BlueBugging y Ataque por fuerza bruta) con el objetivo de poder obtener acceso al dispositivo, ya sea mediante el proceso de saltarse la autenticación, tomar el control remoto del dispositivo e intentar descifrar el PIN del glucómetro para su posterior emparejamiento. Para finalizar, se puede concluir que los recursos limitados (adaptador Bluetooth genérico) que se utilizaron para la auditoría de seguridad en dispositivo IoT médico medidor de glucosa ACCU-CHEK Instant no se encontraron vulnerabilidades algunas.

En efecto del laboratorio practico 2 con el ACCU-CHEK Guide y su aplicación complementaria mySugr arrojó resultados relevantes en ambas fases planteadas.

Durante la Fase 1, centrada en el análisis del entorno de comunicación Bluetooth del dispositivo, se logró identificar que el ACCU-CHEK Guide emite paquetes BLE de forma periódica. No obstante, a pesar de los intentos realizados con herramientas como bluetoothctl, hcitool y Wireshark, no fue posible capturar tráfico significativo entre el dispositivo y la aplicación. Este resultado fue atribuido a factores como: limitaciones del adaptador Bluetooth utilizado (sin soporte para modo promiscuo), el uso de cifrado en la comunicación BLE, y la implementación de protocolos de emparejamiento seguros por parte del fabricante. Estos obstáculos son comunes en auditorías de dispositivos médicos modernos, los cuales priorizan

la protección de datos sensibles mediante tecnologías como LE Secure Connections y Just Works. En consecuencia, aunque no se obtuvieron paquetes explícitos, el hecho de no haber podido interceptar tráfico indica un correcto blindaje de las comunicaciones.

En la Fase 2, se ejecutó un análisis estático de la aplicación mySugr, descompilando su APK con herramientas como apktool. Se evaluaron archivos clave como AndroidManifest.xml. El manifiesto reveló permisos acordes con las funcionalidades BLE y de red, como BLUETOOTH, ACCESS_FINE_LOCATION e INTERNET, sin que se detectaran configuraciones peligrosas como componentes exportados sin autorización. Asimismo, se identificaron clases asociadas a flujos de autenticación mediante OAuth 2.0, lo que indica que el acceso a datos de usuario está controlado por mecanismos robustos.

### 4.3. Medidas de mitigación

Los dispositivos IoT como el medidor de glucosa actualmente son muy utilizados para monitorear la enfermedad de diabetes y mantener así la buena salud del paciente. Estos dispositivos transmiten los datos a través de conexión inalámbrica Bluetooth para su posterior revisión de los resultados por medio de una aplicación móvil. El solo hecho de usar conexión Bluetooth sin tomar en cuenta las medidas de seguridad necesarias, presenta riesgos importantes de seguridad que deben abordarse cuidadosamente.

A pesar de que en los laboratorios prácticos de la auditoría de ciberseguridad del dispositivo medidor de glucosa no se encontraron vulnerabilidades algunas que pudiesen comprometer la integridad de este dispositivo, no estaría demás presentar recomendaciones de seguridad para mitigar vulnerabilidades conocidas en dispositivos similares que utilizan la tecnología Bluetooth.

Por tal razón, se presenta a continuación una serie de recomendaciones para mitigar vulnerabilidades y a su vez mejorar la seguridad en este tipo de dispositivos. Con estas recomendaciones se pretende aplicar buenas prácticas de seguridad tanto para el usuario como para el proveedor, con el fin de proteger la integridad del dispositivo y reforzar las buenas prácticas en el diseño e implementación de soluciones médicas conectadas.

**Mecanismos de seguridad por parte del usuario:**

- **No compartir PIN o clave:** No compartir el PIN o clave de seguridad para emparejar el dispositivo glucómetro con el teléfono móvil.

- **Cifrado de la comunicación**: habilitar el cifrado para todas las comunicaciones BLE. Se debe constatar que el cifrado se mantenga activo durante toda la sesión y evitar que el atacante pueda desactivar el cifrado.
- **Apague el Bluetooth**: desconecte el Bluetooth si no se está utilizando dado que se corre el riesgo de que el dispositivo pueda ser escaneado con hardware sofisticados y técnicas aplicadas por el atacante.
- **Actualización de aplicación**: el usuario final debe tener actualizada la aplicación asociada al dispositivo para garantizar la compatibilidad y funcionalidad.

**Mecanismos de seguridad por parte del usuario:**

- **Actualización del firmware:** el proveedor del dispositivo debe mantener actualizado el firmware.
- **Cumplimiento normativo:** al realizar el diseño del dispositivo el proveedor debe seguir normativas y estándares de seguridad.
- **Mecanismos de autenticación:** se debe implementar mecanismo de autenticación entre el dispositivo glucómetro con el teléfono móvil. A través del emparejamiento con un PIN o clave de mayor longitud y que sea de tipo alfanumérico.
- **Actualización de aplicación**: el proveedor debe mantener en revisión la aplicación para sanear parches de seguridad y que la misma no se vea comprometida para que sea vulnerable para el atacante.

# CAPITULO 5

# 5. CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

- El dispositivo medidor de glucosa ACCU-CHEK Instant tiene incorporada la seguridad mediante el emparejamiento de Bluetooth a través de un PIN numérico para su posterior conexión. Un punto extra referente a dispositivos que no usan esta capa de seguridad y pueden llegar a ser fáciles víctimas de ataques, tomando el control del dispositivo, y así poder acceder a información privada. Pero en la actualidad con tantas herramientas (hardware y software) proporciona una capa de seguridad no tan segura, al contrario de usar un PIN alfanumérico.
- La auditoría de seguridad del dispositivo se la realizó en dos escenarios distintos: el primer escenario contó con el glucómetro ACCU-CHEK Instant y el segundo escenario con el modelo ACCU-CHEK Guide. Se realizaron todas las pruebas en un entorno controlado. Se realizó el laboratorio practico con cada modelo en la máquina virtualizada Kali Linux (máquina para realizar pruebas de hacking), y no se encontraron vulnerabilidades algunas que pudieran comprometer a los dispositivos.
- Para la auditoría de seguridad de los dispositivos medidores de glucosa, se contaron con herramientas tanto hardware y software. Para hardware se utilizó un adaptador Bluetooth USB genérico ya que se necesita para la trabajar en la máquina virtual y para el caso de software se utilizaron herramientas o utilidades en Kali Linux para pruebas de auditoría Bluetooth.
- Trabajar con un adaptador Bluetooth USB genérico conlleva problemas de compatibilidad con la mayoría de las herramientas o utilidades que sea usan en Kali Linux. Con este tipo de adaptadores no se pueden realizar captura y análisis de tráfico Bluetooth, tampoco realizar ataques más sofisticados a causa de la falta de compatibilidad con herramientas de Kali Linux.

## 5.2. Recomendaciones

- Antes de realizar las pruebas controladas en los laboratorios es importante investigar sobre el uso de hardware especial para auditoría Bluetooth, al igual que las herramientas que se pueden instalar y ejecutar en Kali Linux.

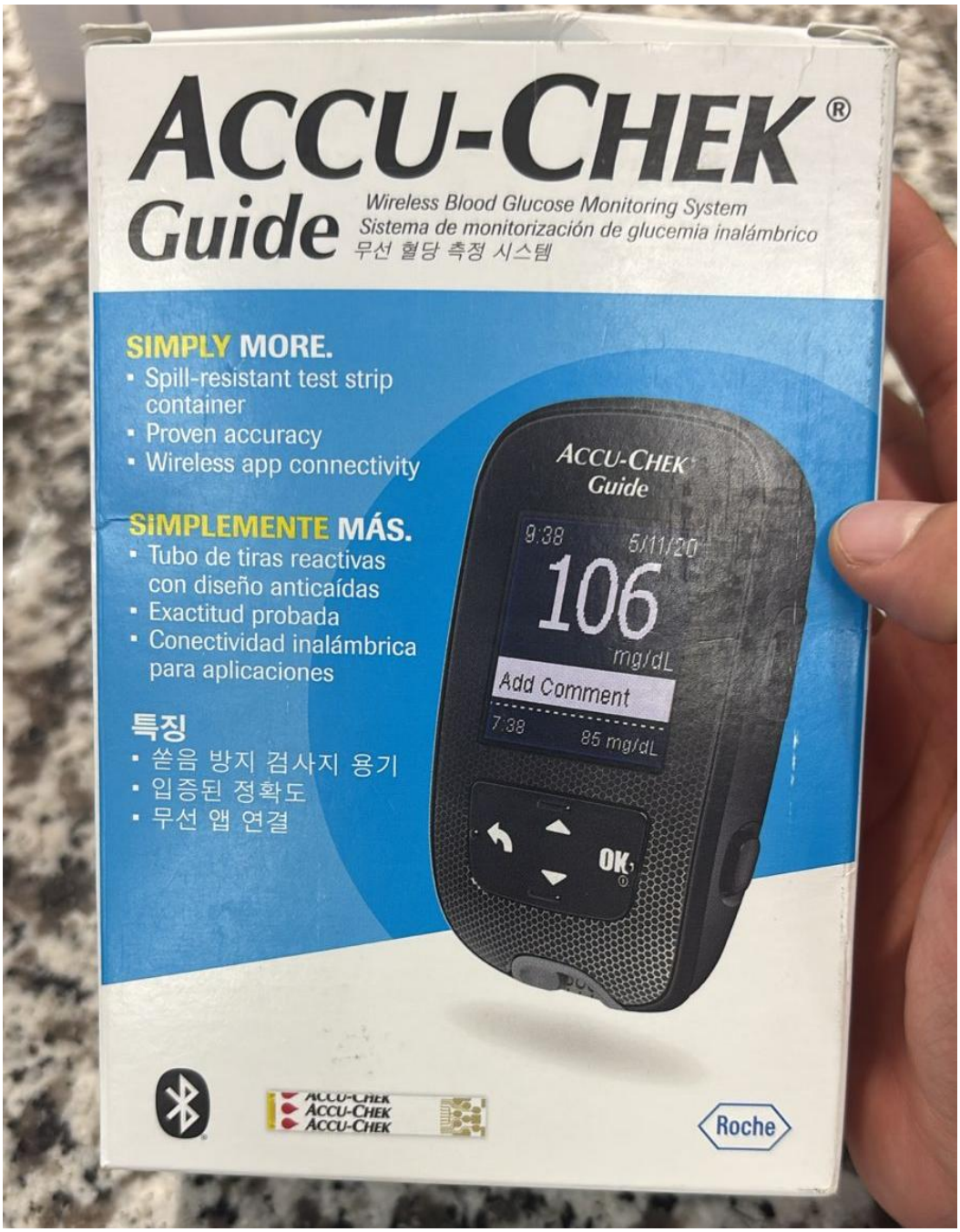
- Para tener mayor éxito en las auditorias Bluetooth se recomienda utilizar adaptadores Bluetooth USB más sofisticados, como pueden ser el adaptador Ubertooth One o el adaptador nRF52840 dongle. Con estos dispositivos se podrán realizar tareas específicas como captura de tráfico Bluetooth, detección de vulnerabilidades, recolección de datos sin necesidad de emparejamiento, entre otras.

## Apéndice A. Hardware y software utilizado en el laboratorio practico

Se adjuntan imágenes del hardware limitado que se utilizó para realizar el laboratorio practico y del software como la máquina Kali Linux.

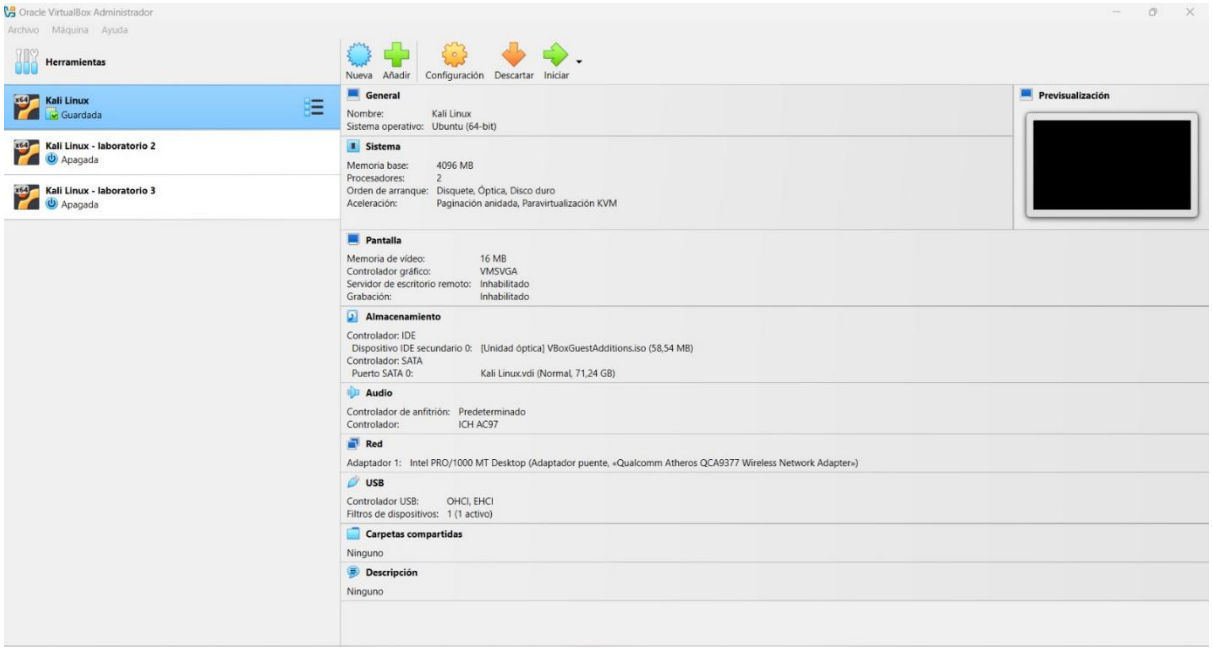
**Dispositivo IoT médico ACCU-CHEK Instant**

**Dispositivo IoT médico ACCU-CHEK Guide**

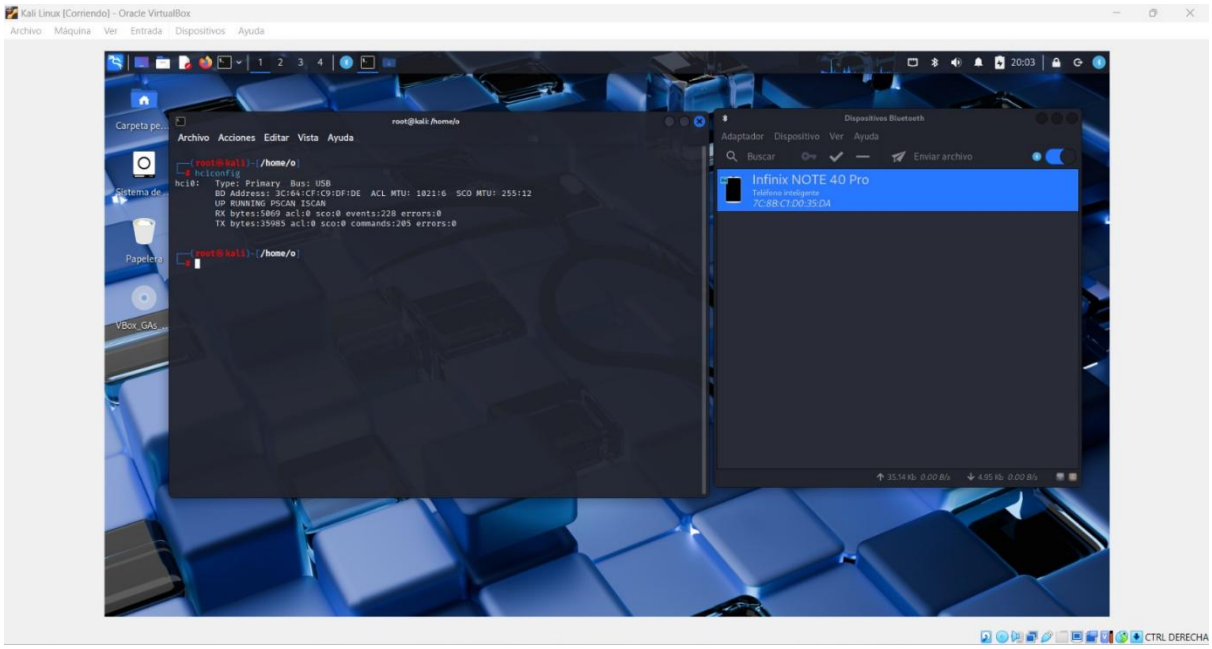


**Adaptador Bluetooth USB**

## Laptop con máquina virtual Kali Linux




## Máquina Kali Linux operativa



**Apéndice B. Laboratorio práctico 1**

En el siguiente link https://drive.google.com/file/d/1dIIXLd6hBVo-7JEIfpjG4vFp8j2_WrlU/view?usp=sharing se puede descargar el archivo donde está montada la máquina Kali Linux, que se usó para pruebas de posible identificación de vulnerabilidades en dispositivo con conexión Bluetooth.

**Apéndice C. Laboratorio práctico 2**

En el siguiente link https://drive.google.com/file/d/1_dbbdcqp-A87x7QVCjG7ZzL0bDdzgbkK/view?usp=drive_link se puede descargar el archivo donde está montada la máquina Kali Linux, que se usó para pruebas de posible identificación de vulnerabilidades en dispositivo con conexión Bluetooth.

## Bibliografía


Campo-Valera, M. (2023). El Internet de las Cosas Médicas (IoMT): Una Revolución Tecnológica aplicable a la Gestión de la Diabetes Mellitus Tipo 1. *Universidad de Malaga*, 86.

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of clinical monitoring and computing, 37*(5), 1123–1132. Obtenido de https://doi.org/10.1007/s10877-023-01013-5

Cervera García, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atención Primaria, 56*(3). Obtenido de https://doi.org/10.1016/j.aprim.2023.102854

Chatterjee, S., Rana, N., Tamilmani, K., & Sharma, D. (2019). The security of the Internet of Medical Things: A review of the literature and future research agenda. Annals of Operations Research. 283(1–2), 191–218.

Cybersecurity and Infrastructure Security Agency. (27 de febrero de 2025). *Dario Health USB-C Blood Glucose Monitoring System Starter Kit Android Application*. Obtenido de https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-058-01?utm_source=chatgpt.com

*Developers*. (2021). Obtenido de Developers: https://developer.android.com/develop/connectivity/bluetooth?hl=es-419

Dzamesi, L., & Elsayed, N. (13 de 01 de 2025). A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS. *Cornell University*, 8. Obtenido de Cornell University: https://arxiv.org/abs/2501.07703

Farahani, S. (2021). Designing and Developing Medical Devices with BLE. Newnes.

Fernández-Caramés , & Fraga-Lamas. (2018). *IEEE Access.* Obtenido de IEEE Access: https://ieeexplore.ieee.org/document/8370027

Food and Drug Administration. (2 de abril de 2022). *Medical Device Cybersecurity: What You Need to Know*. Obtenido de https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

Foudation, O. (2022). *OWASP*. Obtenido de OWASP: https://owasp.org/www-project-internet-of-things/

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (09 de Febrero de 2023). Recent Advances in the Internet of Medical Things (IoMT) Systems Security.

*Cornell University*, 13. Obtenido de Cornell University: https://arxiv.org/abs/2302.04439

Gupta, V. K. (20 de septiembre de 2024). *Learning Networks with Linux: Bluetooth Hacking [Publicación en Linkedln]*. Obtenido de Linkedln: https://www.linkedin.com/pulse/learning-networks-linux-bluetooth-hacking-vijay-gupta--vyq2c

Health Level Seven International. (2023). Obtenido de FHIR security best practices: https://hl7.org/fhir/security.html

Iberia, A. (15 de Junio de 2021). *Ambit Iberia*. Obtenido de Ambit Iberia: https://www.ambit-iberia.com/blog/internet-de-las-cosas-m%C3%A9dicas-iomt-tecnolog%C3%ADa-aplicada-a-la-salud

International Organization for Standardization. (2020). *Health software – Part 1: General requirements for product safety (ISO/IEC 82304-1:2016).* Obtenido de https://www.iso.org/standard/63116.html

Lakshminaryanan, R., & Nota, J. (2023). *Secura*. Obtenido de Secura: https://www.secura.com/blog/serious-safety-impact-found-in-bluetooth-low-energy-based-medical-devices

Lutkevich, B., & DelVecchio, A. (7 de marzo de 2023). *Internet of medical things (IoMT) or healthcare IoT*. Obtenido de TechTarget: https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things

Majumdar, S., Bastos, D., & Singhal, A. (2021). SECURITY AUDITING OF INTERNET OF THINGS DEVICES IN A SMART HOME. National Institute of Standards and Technology (NIST).

Mamani Quisbert, D. J. (2013). Fases de un Ataque Hacker. *Revista de Información, Tecnología y Sociedad*(8), 70-71. Obtenido de http://revistasbolivianas.umsa.bo/scielo.php?pid=S1997-40442013000100029&script=sci_arttext&tlng=es

Microsoft. (2023). Obtenido de Security best practices for API development. : https://learn.microsoft.com/en-us/azure/architecture/best-practices/api-security

National Institute of Standards and Technology. (2020). Obtenido de Recommendation for the transition to post-quantum cryptography (NISTIR 8309): https://doi.org/10.6028/NIST.IR.8309

Oliveira Morilla, S. (2024). *Análisis integral de seguridad en dispositivos IoT [Tesis de ingeniería, Universidat Oberta de Catalunya].* Repositorio institucional. Obtenido de http://hdl.handle.net/10609/150709

Open Web Application Security Project [OWASP]. (1 de noviembre de 2019). *OWASP Internet of Things Project*. Obtenido de https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

OWASP Foundation. (2023). Obtenido de OWASP Top 10: Web application security risks: https://owasp.org/www-project-top-ten/

Palo Alto Networks. (s.f.). *What Is Internet of Medical Things (IoMT) Security?* Recuperado el 27 de junio de 2025, de Cyberpedia: https://www.paloaltonetworks.co.uk/cyberpedia/what-is-iomt-security#iot

PDI Technologies. (s.f.). *What security threats are targeting IoMT devices (and how to prevent being hacked)*. Recuperado el 28 de junio de 2025, de https://security.pditechnologies.com/blog/what-security-threats-are-targeting-iomt-devices-and-how-to-prevent-being-hacked/

Peña Romo, J. C. (08 de 11 de 2023). *unocero*. Obtenido de unocero: https://www.unocero.com/entretenimiento/que-es-bluetooth-low-energy-ble

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R., & Cannady, S. (2019). Future developments in cyber risk assessment for the internet of things. Computers in Industry. 102, 14–22.

S2 Grupo. (26 de junio de 2024). *Ciberseguridad en el sector salud: radiografía y cómo protegerse*. Obtenido de https://s2grupo.es/ciberseguridad-en-el-sector-salud-radiografia-y-como-protegerse/

Saltzstein, W. (2020). Bluetooth Wireless Technology Cybersecurity and Diabetes Technology Devices. *Journal of diabetes science and technology, 14*(6), 1111–1115. Obtenido de https://doi.org/10.1177/1932296819864416

SANS Institute. (2019). Obtenido de Secure coding: Error handling and logging: https://www.sans.org/white-papers/secure-coding/

Shukla, A. (27 de 06 de 2024). *encstore.com*. Obtenido de encstore.com: https://www.encstore.com/blog/5834-bluetooth-low-energy-peripheral-and-central-devices-and-iot-communication

Si-Ahmed , A., Al-Garadi, M., & Boustia, N. (19 de 02 de 2022). Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things. *Cornell University*, 41. Obtenido de Cornell University: https://arxiv.org/abs/2202.09657

Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015 ). *SCIENCEDIRECT*. Obtenido de SCIENCEDIRECT: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971?via%3Dihub

*Targolic*. (2021). Obtenido de Auditoría de seguridad IoT: https://www.tarlogic.com/es/auditoria-seguridad-iot/

Technology, N. I. (2020). Obtenido de Recommendation for the transition to post-quantum cryptography (NISTIR 8309). : https://doi.org/10.6028/NIST.IR.8309

Terzidis, M., Mengidis, N., Rizos, G., Mazi, M., Milousi, K., Voulgaridis, A., & Votis, K. (2023). Challenges in Medical Device Communication: A Review of Security and Privacy Concerns in Bluetooth Low Energy (BLE). 6.

Tutorials Point. (s.f.). *Wireless Security - Bluetooth Hacking Tools*. Recuperado el 5 de junio de 2025, de https://www.tutorialspoint.com/wireless_security/wireless_security_bluetooth_hacking_tools.htm

Vaca Orellana, C., & Valle Dávila, M. (2024). Current Status and Challenges of IoT Research in the Ecuadorian Healthcare Sector: A Systematic Literature Review. *Enfoque UTE, 15*(2), 20-29. Obtenido de https://doi.org/10.29019/enfoqueute.1023

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. Neural Computing & Applications.

Zhuravel, H. (19 de diciembre de 2023). *Understanding IoMT Security: A Comprehensive Guide*. Obtenido de Binariks: https://binariks.com/blog/iomt-security-risks-best-practices/