UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

METODOLOGÍA DE AUDITORÍA DE SEGURIDAD INTRUSIVA EN REDES DE SENSORES INALÁMBRICOS WSN PARA EL ANÁLISIS DE VULNERABILIDADES.

Autor: Kevin Guillermo Oñate Pozo

Director: Msc. Fabián Geovanny Cuzme Rodríguez

Asesor: Msc. Luis Edilberto Suárez Zambrano

Ibarra – Ecuador

2023

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFIACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD:	0401679170		
APELLIDOS Y NOMBRES:	Oñate Pozo Kevin Guillermo		
DIRECCIÓN:	Ibarra, Hugo Guzmán Lara 10-24 y Manuel Zambrano		
EMAIL:	kgonatep@utn.edu.ec		
TELÉFONO FIJO:	062290661	**TELÉFONO MÓVIL**	0996385069

DATOS DE LA OBRA	
TÍTULO:	Metodología de auditoría de seguridad intrusiva en redes de sensores inalámbricos WSN para el análisis de vulnerabilidades
AUTOR (ES):	Oñate Pozo Kevin Guillermo
FECHA: DD/MM/AAAA	08/06/2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **Pregrado** ☐ **Posgrado**
TÍTULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
DIRECTOR:	Msc. Fabián Geovanny Cuzme Rodríguez

CONSTANCIAS.

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la mismo y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 08 días del mes de junio de 2023

EL AUTOR

Kevin Guillermo Oñate Pozo
CI: 0401679170

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER FABIÁN CUZME RODRÍGUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que , el presente trabajo de Titulación "METODOLOGÍA DE AUDITORÍA DE SEGUIRDAD INTRUSIVA EN REDES DE SENSORES INALÁMBRICOS WSN PARA EL ANÁLISIS DE VULNERABILIDADES" ha sido desarrollado por el señor Kevin Guillermo Oñate Pozo bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

Msc. Fabián Geovanny Cuzme Rodríguez
CI: 1311527012
DIRECTOR

DEDICATORIA

El presente trabajo de titulación es dedicado a mis padres Guillermo y Sandra por ser mi motivación día a día, por estar ahí en cada etapa de mi vida y sobre todo por ser mi inspiración y apoyo.

A mi hermana Jessi, por ser mi apoyo incondicional, por estar pendiente de mí, por sus palabras de aliento, de motivación que me impulsan cada día a crecer como persona, siendo una pieza clave en mi vida.

Kevin Oñate Pozo

AGRADECIMIENTO

Agradezco a mi familia que me han apoyado de manera incondicional en cada paso durante mi vida estudiantil, en especial a mi tía Omi por siempre brindarme sus consejos y palabras de aliento, así como también a mis primos Jhosep y Dámaris que me han acompañado en toda esta etapa.

A cada uno de mis amigos y compañeros de clase: Kevin E, Alfredo I, David A, Cristian R, Ángel R; que sin lugar a duda hicieron que mi vida universitaria fuera una aventura inolvidable y llena de grandes momentos, así como también a mis amigos de vida y aventuras: Sebastián B, Emily D, Darwin M, Dennis D, Santiago L.

A la Universidad Técnica del Norte, a la glorioso FICA y a sus maestros que lograron formarme en el ámbito profesional y personal, y en el especial a mi tutor de tesis MSc. Fabián Cuzme por su inigualable guía a lo largo del desarrollo de mi proyecto de titulación.

Kevin Oñate Pozo

Contenido

Índice de Tablas

Índice de Figuras

Resumen

El presente proyecto tiene como objetivo establecer una metodología de auditoría de seguridad para redes de sensores inalámbricos bajo el estándar IEEE 802.15.4 basada en técnicas intrusivas para la evaluación de vulnerabilidades. La metodología corresponde a un enfoque mixto, tipo descriptivo y bibliográfico. La metodología de auditoria seleccionada es Offensive Security se complementa con análisis de riesgos NIST SP 800-30 de las vulnerabilidades según los ataques y el método CVSS para comparar las técnicas. En los resultados se identificó que, en las redes de sensores inalámbricos, los nodos muestran mayor vulnerabilidad debido a que se encuentran instalados en entornos difíciles. Las principales vulnerabilidades con riesgo alto son: rastreo de redes, descifra información sensible y captura activa de tráfico. Por lo que se planificó ataques de confidencialidad, integridad y disponibilidad mediante el uso de herramientas como ZBOSS Sniffer, WireShark y Zigbee-emulador CC. Cabe mencionar que el ataque de escucha presenta mayor vulnerabilidad y con el método CVSS se determinó que la técnica intrusiva sniffing es la más adecuada para identificar vulnerabilidades. Para la validación de la metodología se realizó una prueba maestra de dirección, muestra, ajustes, conexión en red, interfaz RF e interfaz en serie, encontrando vulnerabilidades con mayor precisión. Finalmente, se elaboró medidas de seguridad.

Palabras clave: ataques, auditoria, seguridad, sensores inalámbricos, vulnerabilidad

Abstract

The objective of this project is to establish a security audit methodology for wireless sensor networks under the IEEE 802.15.4 standard based on intrusive techniques for vulnerability assessment. The methodology corresponds to a mixed descriptive and bibliographic approach. The selected audit methodology is Offensive Security and is complemented with NIST SP 800-30 risk analysis of vulnerabilities according to the attacks and CVSS method to compare the techniques. In the results it was identified that currently the wireless sensor network nodes show higher vulnerability due to the fact that they are installed in a difficult environment. The main vulnerabilities with high risk are: network tracking, decryption of sensitive information and active traffic capture. Therefore, eavesdropping, spoofing, integrity and availability attacks were planned using tools such as ZBOSS Sniffer, WireShark and Zigbee-emulator CC. It is worth mentioning that the eavesdropping attack presents greater vulnerability and with the CVSS method it was determined that the intrusive Sniffing technique is the most appropriate to identify vulnerabilities. To validate the methodology, a master test of address, sample, settings, network connection, RF interface and serial interface was performed, finding vulnerabilities with greater precision. Finally, security measures were developed.

Keywords: attacks, auditing, security, wireless sensors, vulnerability.

CAPÍTULO 1. ANTECEDENTES

1.1 Tema

Metodología de auditoría de seguridad intrusiva en redes de sensores inalámbricos WSN para el análisis de vulnerabilidades.

1.2 Planteamiento del problema

Las redes de sensores corresponden a una red de tipo compuesto en la que se interconectan nodos que permiten intercambiar datos mediante la comunicación cableada o inalámbrica. Estas comienzan a ser estudiadas a partir de la década de los 80, siendo conocidas como *Distribuited Sensor Network* (DSN) (Rueda & Talavera, 2017). En la actualidad, existe una gran variedad de aplicaciones que utilizan este tipo de redes, como las WSN (*Redes de sensores inalámbricos*), tecnología que se presenta como la más relevante, siendo un fenómeno relativamente actual. Corresponde a un tipo de arquitectura general que permite la interconexión de dispositivos tanto físicos como virtuales (Rueda J. , 2021), lo que hace posible desarrollar distintos servicios y capacidades (Freemantle, 2014), como la adquisición y procesamiento de datos, la comunicación, entre otros (Rueda & Talavera, 2017).

Como se observa, la seguridad es un aspecto crítico en las redes de sensores inalámbricos, dado que cada vez más tecnologías y ámbitos de desarrollo las utilizan. La protección de la información y del sistema en general es apremiante, sobre todo en un contexto en que se generan datos en cantidades crecientes: para 2020, las estimaciones decían que se almacenarían 35 zettabytes de información a nivel mundial, y cada persona genera en un segundo 1.7 megabytes por segundo (Petrov, 2023), los cuales se han generado en su mayoría durante la última década (Torrijos, 2021). En este escenario, la seguridad se vuelve cada día un factor crítico para un mundo interconectado.

Dado que las WSN implican una gran interconexión entre diversidad de dispositivos, la seguridad es un área crítica que debe ser constantemente

evaluada, ya que resulta un fenómeno altamente vulnerable a las amenazas de hackers (Campos, 2020). En este contexto, mantener la seguridad de las redes de sensores inalámbricos es fundamental y una tarea constante. Las pruebas de seguridad tienen como objetivo, precisamente, identificar los riesgos y vulnerabilidades a las que están expuestos los sistemas y sus datos. Así, las auditorías son la sistematización de estas pruebas para descubrir las vulnerabilidades y riesgos (Torrijos, 2021), cuestión que se evidencia como necesaria para que los proyectos académicos relacionados a WSN puedan ser validados con una metodología adecuada.

Es por esto que se plantea una metodología de auditoría de seguridad intrusiva que permita la monitorización de los datos y a su vez la ejecución de varios tipos de ataques. Dado que las distintas técnicas de auditoría que existen no se pueden aplicar directamente a cualquier dispositivo y/o software en contexto de WSN, se realizará una comparación de las distintas metodologías y modelos de identificación de vulnerabilidades existentes (como OWASP, PHVA, NUTRIA o NIST) y se seleccionará un conjunto de pruebas intrusivas adaptadas a la WSN específica a auditar mediante escenarios reales. Con esto lo que se busca es comprometer la red, para revelar vulnerabilidades que hacen que las redes de sensores inalámbricos sean susceptibles de amenazas. Una mejor comprensión de las vulnerabilidades permite mitigarlas y diseñar mecanismos de seguridad más resistentes. Así como conducir al desarrollo de aplicaciones más seguras y mejores mecanismos de detección y prevención.

1.3 Objetivos

1.3.1 Objetivo general

Establecer una metodología de auditoría de seguridad para redes de sensores inalámbricos bajo el estándar IEEE 802.15.4 basada en técnicas intrusivas para la evaluación de vulnerabilidades.

1.3.2 Objetivos específicos

- Fundamentar teóricamente las metodologías de auditoría utilizadas para valorar la seguridad en redes de sensores inalámbricos basados en el estándar IEEE 802.15.4.
- Determinar las fases de ejecución de auditoría de seguridad que se adapte al análisis de vulnerabilidades de una red de sensores inalámbrica.
- Establecer las técnicas intrusivas que permitan ser utilizadas dentro de la aplicación del proceso de auditoría de seguridad.
- Definir escenarios simulados de redes de sensores inalámbricos que permitan validar la metodología diseñada.

1.4 Alcance

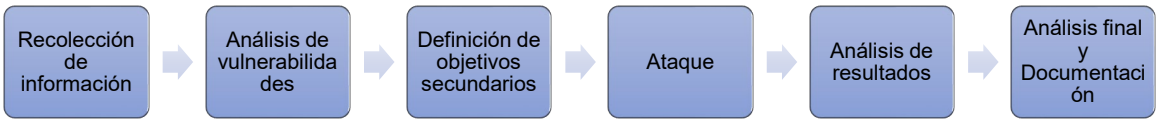
El presente trabajo busca definir una metodología de auditoría para redes de sensores inalámbricos basada en técnicas intrusivas para evaluar la seguridad. Tiene como alcance la definición y aplicación de una metodología para auditar la seguridad en WSN bajo el estándar IEEE 802.15.4, con lo que se busca identificar riesgos y vulnerabilidades.

La metodología determinada corresponderá a un análisis de los distintos modelos de vulneración y análisis de seguridad existentes más utilizados. Las pruebas intrusivas sugeridas serán comparadas y valoradas en una matriz cualitativa basada en sistema de puntuación para seleccionar las más adecuadas en base a foros de expertos.

Esta metodología debería cumplir con la mayoría de los procesos dados en la metodología “Offensive Security” la cual es líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad. Esta metodología se desarrolla en las siguientes fases (Figura 1):

Figura 1.

Proceso de la metodología Offensive Security



Nota. Adaptado de (Cuadros et al., 2022)

Se deberá probar la seguridad de las WSN simuladas tomando en cuenta los principales requisitos de seguridad para una WSN, los cuales son los siguientes (Sharma et al., 2019):

- Disponibilidad: Es esencial que los recursos estén disponibles en la red operativa para que el mensaje avance y asegurar que los nodos puedan utilizar el recurso y la red.
- Autenticación: Implica que los nodos sensores en la comunicación son genuinos y tienen acceso adecuado a la red.
- Confidencialidad: Asegura que el mensaje en la red de comunicación no pueda ser leído ni entendido por los atacantes.
- Integridad: implica que el mensaje no es alterado ni manipulado mientras se encuentre en la comunicación de la red. Simplemente inyectando paquetes adicionales, se puede cambiar el paquete completo.

Para mejorar la seguridad de la red, es importante identificar los ataques más dañinos a los que se encuentra expuesta. La naturaleza de los ataques es lo suficientemente grande como para dificultar su clasificación, sin embargo, Mohammadi en (Mohammadi & Jadidoleslamy, 2011) distinguió dos grandes categorías de ataques: pasivos y activos.

Un estudio detallado de estos ataques concluye que producen principalmente dos efectos. El primer efecto es el aumento del tráfico de la red debido a la introducción de nuevos paquetes en la red. El segundo es el efecto

contrario, la reducción del tráfico de red como respuesta a la eliminación o pérdida de paquetes de red. Un estudio más detallado de los ataques muestra que no todos los ataques pueden modelarse con estos efectos, por lo que se requiere un modelo especial adicional.

En resumen, los ataques de WSN se pueden clasificar en cuatro categorías según sus efectos en la red:

- Ataques que introducen paquetes en la red.
- Ataques que introducen ruido en la red.
- Ataques que introducen ruido y paquetes en la red.
- Ataques que modificaron el firmware de un nodo.

Para probar el funcionamiento de la metodología antes mencionada se estableció dos escenarios, el primero se enfoca en la red de sensores inalámbricos que miden la temperatura y la segunda además de medir la temperatura considera el CO2, a las cuales se aplica tres ataques (confidencialidad, integridad y disponibilidad). Las redes incluyen dos tipos diferentes de nodos: nodos sensor y coordinador (Gateway). El Gateway es responsable de coordinar la red y comunicarse con otras redes externas. El nodo sensor tiene un sensor para leer diferentes variables.

Se considera los siguientes requerimientos para cumplir con los dos escenarios:

- Determinar equipos (red de sensor inalámbrico).
- Usar herramientas como ZBOSS Sniffer, WireShark. Zigbee-emulador CC, depurador y programador USB.
- Establecer tipo de escenario, considerando un campo de aplicación para cada uno.
- Determinar ataques (confidencialidad, integridad y disponibilidad).

- ZigBee contiene suite de seguridad AESCCM* con longitud clave de 128 bits.
- Los marcos de ZigBee se cifran en la capa NWL y APL.
- Zboss debe leer tramas.
- Configurar los ataques con PAN ID.
- Considerar técnicas intrusivas para su respectiva comparativa.
- Temperatura: se mide el nivel de temperatura, es uno de los principales requisitos para estimar los efectos del ataque.
- CO2: se mide el nivel de CO2 en uno de los escenarios.
- Métrica: se establece métricas según el método comparativo determinado.

1.5 Justificación

Actualmente, las WSN tienen una gran variedad de aplicaciones, y es un ámbito de las tecnologías que crece con gran rapidez. Además de sus diversas aplicaciones, las WSN representan un cambio cualitativo en la manera en la que las personas y las organizaciones gestionan información y se comunican, con lo que ha tenido lugar el surgimiento de sistemas de tipo ciberfísicos (Martínez, 2017) (Park et al., 2012). No obstante, su aplicación a cada vez más diversos ámbitos hace que la seguridad en este tipo de redes sea un aspecto crítico. Por ejemplo, en cuanto a su aplicación en entornos de IoT (*Internet of Things*), la seguridad es de importancia fundamental, pues los usuarios de este tipo de entornos son heterogéneos, y no siempre conocen y llevan a cabo buenas prácticas de buen uso, operación y mantenimiento (Batista, 2020a).

El rastreo y el monitoreo a gran escala es una enorme ventaja de la aplicación de WSN; esto se evidencia en la gran cantidad de estudios de aplicación a nivel latinoamericano(Lopez et al., 2017) (Cedro et al., 2018), pero es un factor que hace que sean necesarios un enorme número de sensores para realizar estas aplicaciones. En este contexto, los mecanismos de seguridad tradicionales son difícilmente aplicables debido a las limitaciones que estas redes presentan: los sensores son de baja capacidad de procesamiento, pues

están diseñados para una alta durabilidad (Batista, 2020a). Además, su disposición geoespacial usual es fuente de numerosos riesgos. La seguridad en este contexto y las metodologías para evaluarla son fundamentales, puesto que son vulnerables a ataques de tipo malicioso. Los ataques *Wormhole* (en el que el atacante captura paquetes desde un nodo y hace creer a los otros nodos involucrados que es legítimo) (Ramírez Gómez et al., 2019), *Jamming* (en el que un dispositivo interfiere la señal inalámbrica mediante la creación de ruido) (Almeida et al., 2019) entre otros han sido documentados y por los que se han desarrollado estudios para diseño de contramedidas.

En Ecuador, las WSN tienen un enorme potencial de aplicación. Por ejemplo, el monitoreo de las condiciones agrícolas de producción de determinados cultivos es fundamental en un país como este, de manera que las redes de sensores ofrecen gran cantidad de aplicaciones; la agricultura de precisión, por ejemplo, es un ámbito en el que se aplican las WSN de modo que permita monitorear con precisión las condiciones en tiempo real de cultivos. Los cultivos florícolas, bananeros y azucareros tienen mayor potencial para integrar en sus procesos productivos esta tecnología, tal como Guato (Guato, 2018) lo plantea. Su uso se aboca a la identificación de aspectos como luz, humedad, temperatura, etc., a través del estándar 6IoWPAN en su mayoría, a partir de la cual se envían los datos a una web para su visualización. Otros trabajos han buscado su aplicación en el ámbito de la seguridad ciudadana (Lascano Swoboda, 2017) (Cevallos García et al., 2016) entre otros.

Dentro del contexto IoT, como se plantea en Cuzme (Cuzme Rodríguez, 2015), la seguridad es un componente fundamental, y los dispositivos son utilizados como “puntos de entrada”, de manera que es fundamental desarrollar mecanismos para investigarlos, por ejemplo, con sistemas de detección de intrusos o bien de tipo preventivo. Por lo mencionado, desarrollar auditorías constituye una necesidad impostergable para evaluar en determinado momento el estado de estos sistemas, para lo que existen múltiples herramientas.

Por esto, el presente estudio resulta relevante a nivel científico-académico, dado que busca definir una metodología de auditoría de seguridad

para proyectos IoT. Con esto será posible mejorar los proyectos implementados y otros proyectos en diseño para generar mejores mecanismos de defensa ante ataques, los que serán cada vez más crecientes. Esto permitirá gestionar adecuadamente las redes y sistemas IoT, resguardando con ello la seguridad de la información de los dispositivos, así como los servicios prestados.

Dadas las diversas aplicaciones que ya se impulsan en Ecuador, el desarrollo de una metodología adecuada para auditar la seguridad de estas redes es fundamental. La literatura actual que refiere a la seguridad en redes de sensores es amplia, no obstante, no existe una metodología unificada ni sistematizada que permita realizar una auditoría de seguridad integral para estas (Torrijos, 2021); (Tejedor Doria, 2020). Por tanto, el presente trabajo constituye un aporte al recoger las distintas metodologías y proponer una que permita realizar esta evaluación.

A nivel social, la realización de esta investigación aplicada es relevante, debido a que la seguridad de la información y de las redes es un aspecto crucial, sobre todo si se considera que esta corresponde a uno de los activos más importantes en la actualidad. En Ecuador existen normativas respecto a protección de los datos, constituyendo parte fundamental de los derechos digitales (Canales & Bordachar, 2021). Dado que todas las personas tienen derecho al resguardo de su privacidad, tal como se recoge en la Constitución (*Constitución de La República Del Ecuador 2008*, 2008) en la actualidad debido a la masificación del internet y de la gran cantidad de datos personales que se gestionan a través de las redes es fundamental diseñar mecanismos de seguridad. Con esto, se promueve el derecho a la privacidad de las personas y organizaciones.

Bajo el mismo marco de la visión país, en el Plan Toda Una Vida (2017) se hace énfasis en el aporte al desarrollo económico que tiene el trabajo sobre nuevas tecnologías e innovación. Así, se establecen como finalidades y objetivos del plan el fortalecer la innovación en el contexto de ecosistemas de emprendimientos. Esto es posible mediante el desarrollo de programas de

investigación y desarrollo que permitan fortalecer las tecnologías que tengan directa aplicación en mejoras de procesos productivos.

En definitiva, el proyecto a desarrollar constituye un aporte tanto social, tecnológico y metodológico, contribuyendo a dar facilidades de análisis que permitan tomar medidas correctivas basadas en una metodología de auditoria

CAPÍTULO 2. SUSTENTACIÓN TEÓRICA

En el segundo capítulo se presenta la sustentación teórica de la investigación, para lo cual se tomó diversas fuentes bibliográficas y consideró criterios de diversos autores sobre temas de seguridad en redes, redes de sensores inalámbricas, auditoria de seguridad, hacking ético y trabajos relacionados.

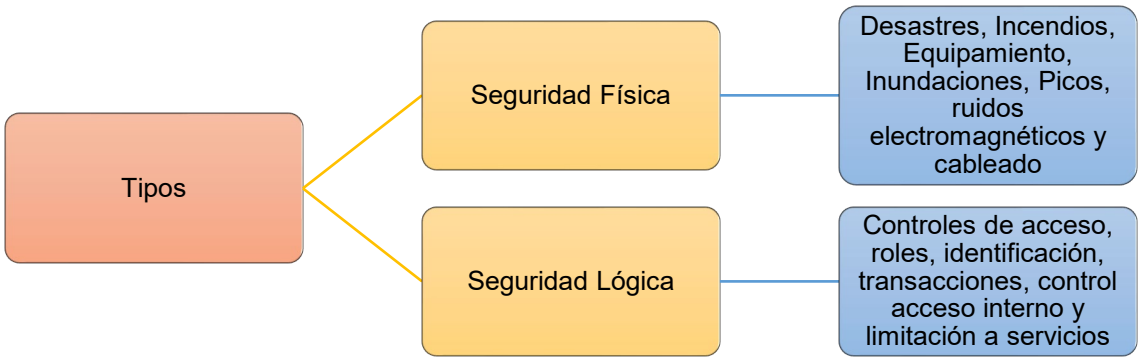
2.1 Seguridad en redes

La seguridad en redes se refiere al mecanismo de protección empleado en los recursos informáticos para hacer frente a las posibles fallas y ataques a la confidencialidad e integridad de los datos. En otras palabras, se basa en el control por parte del administrador para el acceso a los datos, asegurando la privacidad, integridad, autenticidad y disponibilidad de la información gestionada por el ordenador mediante procesos relacionados con las políticas de seguridad (Guayas, 2018).

La clasificación de seguridad se muestra en la Figura 2:

Figura 2.

Clasificación de seguridad en redes



Nota. Adaptado de (Guayas, 2018).

La seguridad física se trata de la implementación de acciones de control relacionadas con las medidas de prevención frente amenazas de los datos, es decir, se utiliza mecanismos para la protección de la información como controles

en el acceso físico, planes de contingencia, medidas preventivas, políticas, entre otros.

Respecto a la seguridad lógica se enfoca en la implementación de herramientas informáticas para la protección de los datos, por lo que se restringe el acceso a archivos, se asegura que la información sea transmitida únicamente al destinatario sin ninguna alteración, etc.

Las amenazas representan las infracciones que afectan a la integridad de los datos o posibles problemas en el acceso a los servicios. Mientras que la vulnerabilidad es una debilidad que se muestra cuando los agentes de amenaza incumplen con las políticas de seguridad. Las amenazas más comunes en la seguridad física pueden ser los desastres, incendios, equipamiento, inundaciones, picos, ruidos electromagnéticos y cableado, mientras que en la seguridad lógica son los controles de acceso, transacciones, entre otros (Trend Micro Incorporated, 2022).

2.1.1 Definiciones de seguridad

De acuerdo a Gómez (Enciclopedia de La Seguridad Informática. 2a Edición - Álvaro Gómez Vieites - Google Libros, n.d.), Romero, et al. (Romero et al., 2018), y Trend Micro Incorporated (2022), se establecen las siguientes definiciones de seguridad:

- Activos: Se refieren a los recursos que emplea el sistema de información.
- Vulnerabilidades: Representa una debilidad de un sistema de datos que pone en riesgo la seguridad de la información, ocasionando fallas.
- Amenazas: Son infracciones que dan a la integridad de la información o datos.
- Ataque: Representa una amenaza a la seguridad de los datos, es decir, tratan de obtener, cambiar, eliminar o enviar información sin autorización.

- Riesgo: Es la posibilidad de que una amenaza explote las vulnerabilidades del activo, dañando al sistema de la organización.
- Impacto: Se refiere a la estimación de la seguridad del activo previo y luego de que se presente las amenazas.
- Protocolo AAA: Hace referencia al protocolo que efectúa las funciones de autenticación, autorización y contabilización.
- Confidencialidad: Es un mecanismo que previene la divulgación de datos a otros sujetos o sistemas que no están previamente autorizados.
- Integridad: Se trata de una cualidad de los datos, es decir, mantenerse intacta y correcta sin ninguna modificación.
- Disponibilidad: Se basa en que los datos o información deben ser accesibles a quienes estén autorizados.

2.1.2 Ataques de seguridad

Para Romero, et al. (2018) un ataque es una amenaza a la seguridad de la información que implica el intento de obtener, modificar, destruir, eliminar, inyectar o divulgar información sin acceso o permiso autorizado. Esto le sucede tanto a los individuos como a las organizaciones. Hay muchos tipos diferentes de ataques, incluidos, entre otros, pasivos, activos, dirigidos, click hacking, branding hack, botnet, phishing, spam, internos y externos.

El ataque es una de las mayores amenazas de seguridad en la tecnología de la información y se presenta de muchas formas. Un ataque pasivo es un ataque que no afecta a ningún sistema, aunque se obtiene la información. Un buen ejemplo de esto son las escuchas telefónicas. Un ataque activo puede causar daños graves a los recursos de una persona u organización, ya que intenta modificar o interferir con los recursos del sistema. Un buen ejemplo de esto sería un virus u otro tipo de malware (Bustamante Sánchez, 2011).

2.1.3 Medidas de seguridad en redes

De acuerdo con Muñoz (Muñoz Campuzano, 2021) las medidas de seguridad en redes son estrategias para la prevención, detección y solución para asegurar la confidencialidad, disponibilidad e integridad de los datos. En cuanto a la prevención se debe tomar en cuenta los siguientes aspectos:

- Establecer lo que se debe proteger.
- Definir las responsabilidades de la compañía o institución.
- Determinar el proceso para la implementación de mecanismos.
- Describir el proceso para la ejecución.
- Diseñar un plan para concientizar la seguridad en los colaboradores.
- Plantear controles para administrar la manera que los colaboradores usan y acceden a los recursos (Muñoz, 2021).

En cuanto a la detección se debe emplear funciones para la supervisión y registros de las actividades del sistema. Cuando se identifica una acción maliciosa se notifica al responsable de este proceso, siendo importante la planificación a tiempo de las medidas. La solución representa la corrección que se efectúa para hacer frente a los incidentes, entre los mecanismos de seguridad puede ser paralizar los ataques, actualizar el sistema, entre otros (Muñoz, 2021; Bustamante, 2011). En la siguiente Tabla 1 se describe las medidas de seguridad:

Tabla 1.

Medidas de seguridad en redes

Medidas	Descripción
Incendios	• Evitar que los equipos están en sitios inflamables, explosivos o sustancias tóxicas. • Usar materiales incombustibles en las paredes. • Incluir piso falso resistentes al fuego. • Evitar fumar.

Equipamiento	• Revisar la temperatura que no sea superior a 18°C y límite de la humedad. • Contar con extintores.
Inundaciones	• Contar con techo impermeable y acondicionar las puertas para que contengan el agua.
Cableado	• Desviar conexión no autorizada.
Identificación y autenticación	• Contar con usuario, clave secreta (PIN, criptográfica, etc.), tarjeta magnética, huellas digitales, voz y patrón de escritura. • Realizar revisiones periódicas para verificar permisos.
Roles	• Determinar roles para el acceso a la red como programador, administrador del sistema, usuario general entre otros.
Transacciones	• Solicitar claves para efectuar transacciones.
Limitación a servicio	• Establecer parámetros de restricción cuando se incumplen las reglas.
Control acceso interno	• Contar con palabras clave, encriptación, lista de control de acceso, límites y etiquetas de seguridad.

Nota. Adaptado de (Muñoz, 2021); (Bustamante, 2011)

2.2 Redes de sensores inalámbricas

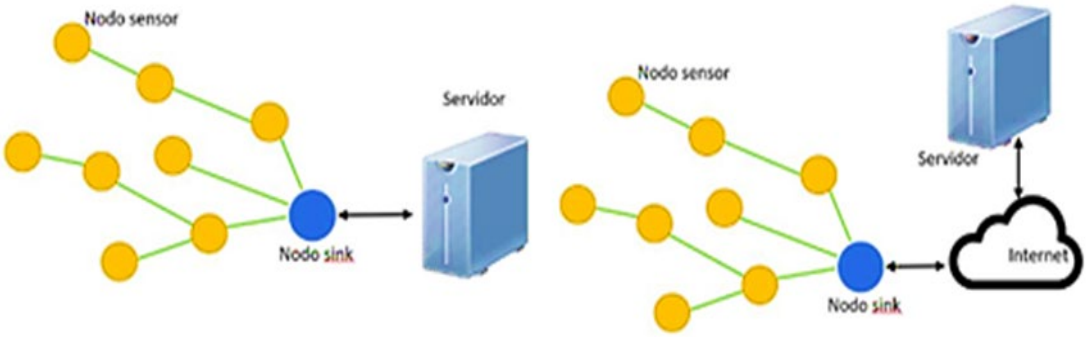
Un sensor se refiere a un transductor que ayuda a transformar un fenómeno de tipo físico en señal eléctrica, el cual depende del tipo utilizado como de resistencia eléctrica, corriente y voltaje. Las redes de sensores se tratan de dispositivos autónomos que de forma conjunta recaban información desde un ambiente específico, comunicándose de forma inalámbrica (Mendoza et al., 2020).

Una red de sensores inalámbrica o *Wireless Sensor Network* (WSN) representa a un conjunto de nodos de transmisión y conmutación de datos entre puntos específicos conectados a través de cables, medios ópticos, entre otros. Es decir, se trata de nodos que se conectan entre sí para la transmisión de señales y a la vez comparte uno o más canales para transmitir información

mediante diversas tecnologías inalámbricas, por ende, comparten recursos físicos y lógicos (Rueda & Talavera, 2017). En la siguiente Figura 3 se muestra la arquitectura de WSN:

Figura 3.

Arquitectura WSN

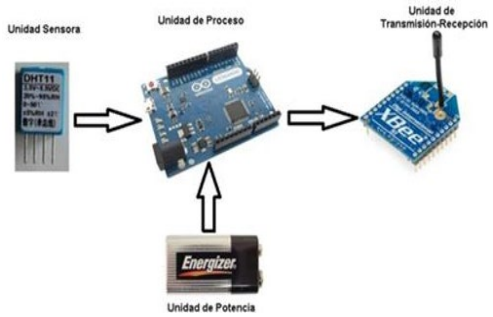


Nota. Adaptado de (Rueda & Talavera, 2017).

Una red de sensor inalámbrico está compuesta por los siguientes elementos como se muestra en la Tabla 2:

Tabla 2.

Elementos de WSN

Elementos	Características
Nodos sensores 	• Están configurados a nivel hardware y software. • Hardware: radio, sensor, procesador, fuente de energía y memoria. • Software: • Se utilizan para diferentes áreas como la medicina, industria, etc. • Obtienen información del entorno para tomar decisiones, detectar comportamiento, entre otros. • Ejemplos: mecánicos, ultrasónicos. Inductivos, capacitivos y fotoeléctricos.
Puerta de enlace	• Recepta información de los nodos para enviar a otro dispositivo.

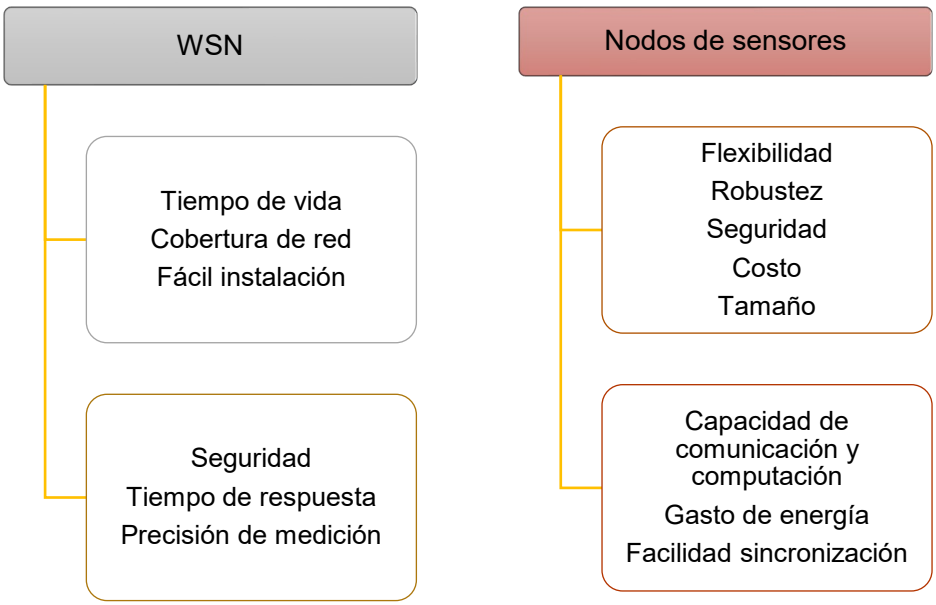
 Estación base	• La información enviada se almacena o genera alerta.
 Canal de transmisión inalámbrico	• Guarda los datos derivados de los nodos. • Puede conectarse directamente a WSN. • Cuando se ubica remotamente se conecta por ISP.
	• Transmite la información. • Se ubica en frecuencias de 433 Mhz y 2.4 Ghz.

Nota. Adaptado de (Acosta et al., 2021; Egas & Gil-Castiñeira, 2020).

Las características de una WSN y de nodos de sensores se describen a continuación en la Figura 4:

Figura 4.

Características WSN y nodos de sensores

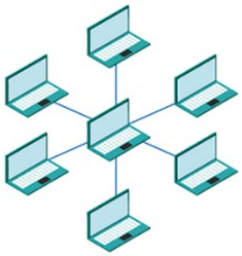
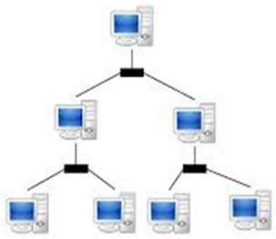
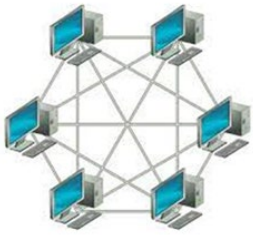


Nota. Adaptado de (Santos Benavides & Jurado Lozada, 2019).

Según Santos & Jurado (2019) existen diferentes topologías de red de sensores inalámbricos, lo cual se detalla a continuación en la Tabla 3:

Tabla 3.

Topología de WSN

Topología	Características
Estrella 	• Tiene nodo final y Gateway. • El nodo se conecta a Gateway.
Árbol 	• Posee Gateway, nodo router y nodo final. • El nodo se conecta al nodo con un alto nivel jerárquico y a Gateway. • Los datos se rutean a partir del nodo con inferior nivel jerárquico en el árbol hacia Gateway.
Malla 	• Conecta varios nodos y envía a la ruta disponible. • Se denomina ruteador.

Nota. Adaptado de (Santos Benavides & Jurado Lozada, 2019).

Por otro lado, las WSN utilizan las siguientes tecnologías y protocolos de comunicación:

- Bluetooth

Esta tecnología se trata de un sistema de red inalámbrica utilizado para conectar dispositivos fijos y móviles, por ende, no se usan cables para la

comunicación de datos, incluso se puede diseñar redes pequeñas e intercambiar información (Santos Benavides & Jurado Lozada, 2019).

La tecnología Bluetooth (IEEE 802.15.1) está formada por un transmisor pequeño de radiofrecuencia con la finalidad de conectar distintitos dispositivos electrónicos dentro de un radio de 10 metros y puede ampliarse hasta 100 metros. Está conformada por unidad de radio, control del enlace, gestión del enlace y funciones de software. En el diseño de sensores se ha utilizado esta tecnología, empleando nodos (uno maestro y siete nodos esclavos) (Santos Benavides & Jurado Lozada, 2019).

- WiFi

Se refiere a un protocolo de salto único empleada en redes para la transmisión de datos, donde, los transceptores necesitan de una mayor cantidad de energía. Este protocolo (IEEE 802.11g) debe contar con nodos que escuchen al medio debido a que recepta frame en cualquier ocasión (Santos Benavides & Jurado Lozada, 2019).

- ZigBee

Es un protocolo (IEEE 802.15.4) que cuenta con multi salto, es decir, ayuda que el mensaje puede usar diferentes saltos en las ondas radio hasta llegar al destino. Los nodos compiten para el acceso al canal, lo cual permite que exista mayor número de usuarios que accedan a este medio (Santos Benavides & Jurado Lozada, 2019).

- Enhanced Shockburst

Representa un protocolo que permite la comunicación en dos direcciones de los paquetes de datos, considerando aspectos como el almacenamiento, reconocimiento y envío automático de los paquetes. El paquete de datos contiene *preamble, address, packect* control *field, payload y cyclic redundancy check* (Santos, 2019). Además, proporciona comunicación por radio con bajo

consumo de energía, su implementación es de pequeño tamaño de código y fácil de usar, ofreciendo una gestión automatizada de las transacciones de paquetes que ayuda al enlace de datos bidireccional, admite topología estrella con receptor primario, longitud de carga útil dinámica está de 1 a 32 bytes mientras que la carga útil estática entre 1 a 252 bytes entre los dispositivos de serie nRF5 (Nordic, 2016).

- LoRaWAN

Se trata de un protocolo de red que emplea tecnología LoRa enfocada en dos redes (baja potencia y amplia); está formado por gateways y nodos. Además, utiliza una tecnología de modulación *Chirp Spread Spectrum*, tiene un alcance de 10 – 20 km, conexión punto a punto, tolera interferencia, aplicada en conexiones y redes IoT (internet de las cosas) donde se requieren sensores que no contengan corriente eléctrica (Soluciones Keller, 2021).

- XBEE

Hace referencia a pequeños radios que se comunican de manera inalámbrica, incluso cuentan con entradas y salidas (analógicas – digitales) capaces de controlar y conectar sensores. Permite el cambio de cables de comunicación serial, conexiones (punto – punto, punto – multipunto y mesh) (Ingeniería MCI Ltda, 2021).

- RFID

Se refiere a un modo de comunicación de manera inalámbrica (lector – emisor), utilizan ondas de radio, empleadas para la localización de objetos, evitando que se saquen de un sitio sin autorización. Es decir, facilita de identificación automática de un objeto (Universidad Internacional de Valencia, 2017).

2.2.1 Ataques más comunes en una WSN

Las redes de sensores inalámbricas (WSN) sufren de ataques y vulnerabilidades, entre ellos se destacan los siguientes (Tabla 4 hasta Tabla 8):

Tabla 4.

Ataques a WSN según capa física

Ataques	Características
Manipulación	• Ataque invasivo (acceso al control de nodo para extracción criptográfico e información de la memoria para modificar o eliminar). • Ataque no invasivo: control, consumo de energía de los dispositivos.

Nota. Adaptado de (Gutiérrez-Portela et al., 2021b)(Escalante Uicab, 2019) (Diaz et al., 2016)

Tabla 5.

Ataques a WSN según capa enlace

Ataques	Características
Colisión	• Los nodos se transmiten de forma simultánea en igual frecuencia.
Agotamiento	• Nodo malicioso para interrumpir la comunicación.
Interrogación	• Envío de mensajes de manera repetida para agotar los recursos del nodo.
Ataque de denegación del modo dormido	• Los nodos están despiertos por mayor tiempo y provoca alto consumo de energía.
Homing (buscador de blancos)	• Los intrusos investigan el tráfico de la red para comprender el área geográfica de los cabezales de clúster o la estación base. • Cuando los intrusos conozcan la estructura de la red, podrán determinar los nodos más críticos y luego atacar estos nodos para destruir toda la red rápidamente.

Nota. Adaptado de (Gutiérrez-Portela et al., 2021b)(Escalante Uicab, 2019) (Diaz et al., 2016)

Tabla 6.

Ataques a WSN según capa red

Ataques	Características
Ataque Blackhole	• Se descarta los mensajes de nodos hijos. • Provoca que la red sea inutilizable.
Desvío selectivo	• El atacante evita el transporte de los paquetes. • Los paquetes se dejan caer y representan como agujero negro.
Fraude de identidad	• Genera identidad artificial para acceder a la red.
Ataque Hello Flood	• El atacante envía paquetes de saludo con el fin de convencer a los nodos que es un vecino.
Ataque sinkhole	• Atrae tráfico a los nodos comprometidos.
Ataque wormhole	• Almacena el tráfico de la red para enviar a una región distinta.
Sybil Ataque	• Es un nodo malicioso que se hace pasar por diversas identidades a la red. • Afecta al almacenamiento, enrutamiento y mantenimiento (topología).
Redirección	• Se presenta por reenviar mensaje por la vía errónea. • Se envía actualizaciones de redirección falsa.
Ataque caer en el agujero	• El atacante atrae a todo el tráfico de un sitio específico a un nodo denominado compromiso. • Crean reenvió de manera selectiva • Realizan ataques de agujeros negros.
Ataque agujero negro	• Atraen y generan dropping de todo el tráfico de un sector en particular.
Fuga de información/captura de tráfico	• El atacante intenta conocer el comportamiento del tráfico, la red y los nodos.

Ataques de interferencia constante	• Interfiere en la transmisión de señal • La señal emitida por los intrusos interfiere en la señal real.
Drenaje de energía	• Inyecta informes o datos falsificados en la red o generar una gran cantidad de tráfico en la red. • Consume la energía del nodo porque los informes causarán falsas alarmas y agotarán la gran cantidad de energía en una red basada en baterías.
Mala dirección (Misdirection)	• Enruta el paquete a distintos nodos. • El nodo intruso puede desviar el paquete a diferentes nodos en lugar del nodo de destino.

Nota. Adaptado de (Gutiérrez-Portela et al., 2021b)(Escalante Uicab, 2019) (Diaz et al., 2016)

Tabla 7.

Ataques a WSN según capa transporte

Ataques	Características
Ataque por inundación	• Tiene nodo malicioso envía continuamente paquetes de datos. • Agota los recursos disponibles del nodo. • Ataques de denegación de servicio (DoS) basados en la ruta y de privación.
Ataque de desincronización	• Envío de mensaje repetidos

Nota. Adaptado de (Gutiérrez-Portela et al., 2021b)(Escalante Uicab, 2019) (Diaz et al., 2016)

Tabla 8.

Ataques a WSN según capa aplicación

Ataques	Características
Overwhelm	• Adquisición de señal errónea debido al ataque directo al sensor que se encuentra en el nodo.

Reprogramación	• Modificación no autorizada de la programación.
Protocolos de sincronización de reloj	• Cambios en dichos protocolos
De software	• Pueden presentarse infecciones por virus, gusanos, presencia de spyware, entre otros.
Applicattion	• Modifica el nodo de los sensores

Nota. Adaptado de (Escalante Uicab, 2019) (Diaz et al., 2016) (Gélvez-Rodríguez & Santos-Jaimes, 2020)

Por su parte, (Mohammadi & Jadidoleslamy, 2011) destacan que los ataques se dividen en pasivos y activos. Los ataques pasivos están relacionados con la privacidad (recopilación y robo de información mediante la interceptación de las comunicaciones de datos o la supervisión de los paquetes intercambiados dentro de una WSN). Los ataques activos realizan acciones como la inyección de datos defectuosos, suplantación de identidad, modificación de los flujos de recursos y datos, creación de agujeros en los protocolos de seguridad, destrucción de los nodos sensores, degradación del rendimiento, interrupción de la funcionalidad y sobrecarga de la red.

En cambio, (Abu Daia et al., 2018) establecen cuatro formas de ataques a la red de sensores inalámbricas, estos nuevos mecanismos reúnen en las mismas algunos de los ataques mencionados en las tablas anteriores. A continuación, se expone los cuatro tipos de ataques:

- Link-Noise Attacker: Inyecta ruido en el canal, en la que se incluyen ataques como colisión, agotamiento, interrogación, ataque de denegación del modo dormido y homing (buscador de blancos).

- Fake packet injection Attacker: Inyecta paquetes en la red, donde se incluyen el desvío selectivo, ataque Hello Flood, ataque agujero

negro, ataque de inundación, ataques de interferencia constante, drenaje de energía y mala dirección (Misdirection).

- Atacante directo: Ataque directo a un nodo como overwhelm y Applicattion.

- Link + Injector attacker: Atacante de enlace + inyector. En la que se considera Spoofed, Sybil y Looping Looping in the net Node Replication.

Los ataques más comunes en una WSN se tratan de la pérdida de equipo robado, espionaje de usuario a usuario, puntos de acceso falsos, denegación de servicio y sesiones de cuentas de secuestro (López, 2021).

2.2.2 Seguridad en redes de sensores

La seguridad en las redes de sensores es fundamental, puesto que cualquier persona podría tener acceso a la red debido a que los sensores se encuentran en distintas locaciones. Los ataques, como se indicó previamente, pueden ser varios, y es posible que se efectúen ataques múltiples de forma sincrónica. Por ello, la seguridad de la red WSN es fundamental para garantizar la integridad de la red y de la información (Valencia et al., 2019).

En este contexto, es cada vez más importante considerar la seguridad de la información como una función y un objetivo indispensable para todo sistema que trabaja transmitiéndola. Así, para considerar que un sistema es seguro a este respecto, deben presentarse los siguientes requerimientos (Oreku & Pazynyuk, 2015); (Batista, 2020a):

- Confidencialidad: es preciso que los datos que se manejen en la red, en este caso de sensores, sean tratados de modo tal que se conserve y proteja su confidencialidad. Esto implica que la información esté resguardada del acceso de terceros no autorizados.

- Integridad: el tratamiento de la información debe poder preservarla íntegramente, sin perder parte de ella o su manipulación.
- Actualización de datos: es importante que la información tratada se encuentre permanentemente actualizada y sea la información requerida por los usuarios de la red.
- Disponibilidad: la información debe estar siempre disponible para ser utilizada cuando un usuario lo requiera. Esto implica que se atiendan los mecanismos de la red permanentemente para que cumplan dicha función.
- Autogestión: los protocolos que utilice la red para autoorganizarse deben ser eficaces y eficientes, de modo que los datos sean transportados con el menor gasto de energía asociado, sobre todo en una red de sensores.
- Sincronización: en vista de la necesidad de eficiencia, es preciso que los nodos trabajen de forma coordinada y se establezcan mecanismos de ahorro de energías sincronizados para no desperdiciar recursos.
- Ubicación segura: es imprescindible en las WSN que los nodos y su ubicación se encuentre determinada de manera segura y pueda monitorearse en caso de fallos.
- Autenticación: esta refiere a que la red pueda garantizar la autenticidad de los datos, de modo que pueda identificarse cuando estos hayan sido manipulados.
- No repudio: refiere a la demostración de las identidades de envío y recibo de datos para evitar con ello el repudio o rechazo de alguna de las partes.
- Autorización: cuando se desea acceder al sistema se necesita permisos previos, es decir, se determina el tipo de recursos del sistema que los usuarios pueden acceder con los permisos respectivos.

El tipo de seguridad que se implemente en la red debe incluirse en la fase de diseño de la red, pues depende del tipo y de la finalidad de esta. Como Batista

(2020) plantea, las medidas de seguridad para redes tradicionales no suelen ser compatibles con las redes de sensores, de modo que es importante valorar en cada caso particular el diseño y las técnicas de seguridad más adecuadas.

Dado que los ataques en la red pueden tener múltiples motivaciones, es importante que se protejan todos los escenarios y componentes en que es posible intervenir la red de forma no autorizada. Así, aun cuando algunos atacantes tengan interés en la información sensible que utiliza o circula en la red, es posible que otros solo tengan intenciones de vandalismo sin obtener beneficios a cambio, pudiendo atacar cualquier aspecto del diseño (Batista, 2020b). Por ello, es relevante considerar los siguientes aspectos de las redes al momento de diseñar la seguridad:

- Limitación en recursos: como se ha revisado, las WSN deben incluir mecanismos con poco uso de recursos, además de considerar las fuentes de alimentación energéticas para esto.
- Bajo grado de confiabilidad en la comunicación: es muy común que en las WSN se pierda información, se dañe o no se procese por falta de capacidad de los nodos.
- Operación autónoma sin vigilancia: dado que, usualmente, las WSN funcionan de forma autónoma en ubicaciones geográficas determinadas, funcionan sin supervisión, haciéndolas vulnerables a los ataques directos.

En consideración de estos requerimientos de la seguridad de la información y características presentes en las WSN, existen diversos mecanismos utilizados para proteger la seguridad de la red en función de los objetivos y los tipos de red. Para Batista (2020) existen mecanismos de alto y bajo nivel, dependiendo del tipo de acción a desarrollar y de quien la ejecute en un sistema de manejo de la información.

Así, los mecanismos de alto nivel, siguiendo los planteamientos de Batista (2020) son:

- Gestión de grupos seguros: corresponde al manejo seguro de los nodos mediante su administración con protocolos adecuados. Esto permite que la comunicación entre nodos sea segura y escalable con la integración de nuevos nodos. Para asegurar que la información sea auténtica, se administran y transmiten las claves de acceso por la estación base.
- Detección de intrusos: el enfoque mencionado, además, resulta efectivo en caso de que se busque detectar la intrusión de terceros de modo descentralizado. Esto permite salvar energía a la vez que se requiere menos recursos y se genera una comunicación eficiente.
- Envío seguro: con el objetivo de reducir el tráfico de grandes cantidades de información, los datos recogidos por los nodos deben dirigirse a la estación base; esto puede llevarse a cabo en distintos puntos de la red, de modo que los nodos deben resguardarse al igual que el canal a través del cual se produzca la transmisión de los datos.

Por otra parte, los mecanismos que (Kumar et al., 2021) (AlEroud & Karabatis, 2017), y Batista (2020) señalan como de bajo nivel son los siguientes:

- Definición de claves y configuraciones confiables: la criptografía es fundamental en las redes de sensores, aunque debe tenerse en cuenta que los recursos de procesamiento son limitados.
- Autenticación y secreto: puede utilizarse criptografía de claves secretas en la capa de enlace, lo que vuelve más sencilla la implementación de seguridad; sin embargo, es posible que nodos intermedios tengan la capacidad de acceder y alterar los datos.
- Privacidad: dado que las WSN son escalables y permiten la adición de nuevos nodos constantemente, es preciso que se establezcan mecanismos de reconocimiento y legitimación de los nodos nuevos.

- Resistencia ante DoS: es posible que el funcionamiento de la red sea interrumpido por un ataque de denegación de servicio producido por señales de alta energía; por ello es preciso diseñar mecanismos que sean robustos contra este tipo de ataques.
- Seguridad del enrutamiento: los métodos de autenticación pueden fortalecer la seguridad de los protocolos de enrutamiento, dado que estos son susceptibles de ser atacados (como una introducción de enrutamiento malicioso).
- Defensa ante captura: los nodos, debido a su naturaleza, son susceptibles de ser capturados y alterados. Por ello pueden utilizarse mecanismos físicos de protección o soluciones de carácter algorítmico, como esquemas de cifrado de tipo dinámico (blockchain).

Un mecanismo comúnmente utilizado es la criptografía, ya que permite implementar diversas técnicas para cifrar y descifrar la información tratada, de modo que no puede ser obtenida por terceros que no se encuentran autorizados. Esta constituye gran parte de los mecanismos que se utilizan para proveer de seguridad a las redes WSN, siendo necesario que sea ligera; por esto, lo más utilizado es la criptografía simétrica como asimétrica (Batista, 2020).

Para sistemas en que es necesario gestionar adecuadamente los recursos por su limitación, la criptografía ligera es la más apropiada. Esta se ajusta tanto a las necesidades de software como de hardware: para software, se utiliza para valorar la optimización, la dimensión del código, y la RAM (su complejidad); mientras que para hardware se valoran el tamaño de los chips y la energía (nivel). Para desarrollar este tipo de criptografía, su algoritmo debe tener en cuenta (Tawalbeh et al., 2017).

- Seguridad contrastada con desempeño
- Seguridad contrastada con el costo
- Desempeño del algoritmo contrastado con el costo

Para el caso de la criptografía simétrica (o de clave secreta), se utiliza una clave que permite cifrar la información, la cual es utilizada por el remitente. Esta clave es conocida por el receptor, siendo la que permite, a su vez, el descifrado del mensaje. Lógicamente, existen varios mecanismos y enfoques para trabajar con este tipo de criptografía. Por ejemplo, se puede trabajar primeramente con una clave única conocida por la totalidad de los nodos; también es posible trabajar con la distribución de claves de forma centralizada, siendo el eje la estación base; o, bien, se pueden asignar claves a cada nodo previo al despliegue de la red, que puede realizarse mediante una distribución de carácter aleatorio (KPR) o no aleatorio (Batista, 2020).

En el caso de las claves públicas, el mensaje es cifrado por el remitente a través del uso de una clave pública, pero su descifrado se realiza por el destinatario con una clave privada (Valencia et al., 2019). Batista (2020) plantea que este mecanismo presenta mayor robustez y eficacia en caso de captura de nodos, siendo necesario encontrar la clave privada.

Por otra parte, para el resguardo de la confidencialidad, la integridad y los otros requerimientos de seguridad de la información en las WSN, existen distintos protocolos (de los cuales se revisaron algunos previamente) que aplicados a WSN pueden funcionar adecuadamente en términos de seguridad. Con ellos puede evitarse que terceros no autorizados o bien otros dispositivos intrusos accedan a los datos. A continuación, se describen algunos de los protocolos más relevantes para WSN en atención a su seguridad (Mbarek & Meddeb, 2016); (Batista, 2020); (Khanji et al., 2019).

- TinySec: corresponde a un protocolo que vela por la seguridad en la capa de enlace de la red, utilizando SO TinySO. Está pensado para la generación de paquetes de tamaño reducido en la red; admite el cifrado con autenticación de la identidad que cifra los datos y permite la adición de un código para la autenticación del mensaje a cada paquete (MAC). De igual manera, es compatible con métodos de solo autenticación, es decir, sin cifrado de datos;

pero, a la vez, la autenticación del paquete se lleva a cabo con MAC.

- SPINS: refiere a un protocolo que utiliza a los protocolos u TESLA y SNEP, además de un tercer protocolo para enrutar que tiene como base a los dos mencionados; u TESLA, por su parte, permite la autenticación en radiodifusión, mientras que la confidencialidad está garantizada por SNET, además de la autenticación entre dos nodos respecto de su identidad, datos actualizados y comunicación con baja sobrecarga. El algoritmo de cifrado de datos es en bloques RC5, en el cual el remitente elabora un código MAC para la difusión unidireccional de los paquetes con una clave solo conocida por ellos. Así, cada determinado intervalo de tiempo las claves de los paquetes son transmitidas hacia el receptor para autenticarlos.
- LISP: este protocolo utiliza la conmutación a partir de la utilización de nodos receptores además de servidores de claves. Como ventajas de seguridad de este protocolo, se observa que presenta una emisión adecuada de claves, puesto que no requiere del acuse de recibo. Además, utiliza bits para la comprobación que no requieren de ser añadidos al paquete de datos. Por otra parte, ya que no requiere acuse de recibo o paquetes para el control, es robusto frente a los ataques de denegación de servicios.
- Zigbee: este tiene como base el estándar IEEE 802.15.4 para la definición de protocolos de comunicación. Así, los dispositivos que utilizan Zigbee requieren pocos recursos energéticos para operar, con una duración adecuada de las baterías. Para la seguridad usa el cifrado AIG-128 fuerte; al momento de crear una clave nueva, se actualizan los datos con un contador reestablecido; por otra parte, preserva la integridad de los datos y facilita evitar la alteración de los mensajes por intrusos. Además, mediante el mecanismo de autenticación, Zigbee puede comprobar que el remitente sea legítimo, evitando el reemplazo de los dispositivos con ello. En la propia red, la autenticación se genera mediante las claves públicas, y en cada dispositivo se dispone de una clave única.

- LSec: este protocolo, en cuanto a seguridad, permite generar autenticación de la identidad y autorizaciones al tiempo que realiza intercambios de clave de carácter seguro, permite el resguardo de infracciones, preserva la privacidad de los datos y soporta el uso de codificación asimétrica y simétrica de forma simultánea.
- LISA: en términos de seguridad, LISA utiliza mecanismos de seguridad semántica, de manera que los mensajes extraídos carecen de valor para los atacantes debido al cifrado del texto; por otra parte, permite autenticar la identidad, garantizando con ello que los datos tienen un remitente legítimo; además, dispone de un mecanismo de verificación de actualización de los mensajes; y, finalmente, permite evitar la repetición mediante su protección contra ataques.
- MiniSec: este protocolo se caracteriza por presentar características de seguridad adecuadas al tiempo que consume una baja cantidad de energía para ello. Esto es posible debido a tres funciones, su cifrado de bloques que favorece la protección de la privacidad y de la autenticación, la inicialización con vector (IV) con bajo uso de bits y los saltos básicos en la operación de tipo *unicast* (con contadores sincronizados que reducen el uso de energía) y *broadcast* (con filtro de Bloom). Para el cifrado se utiliza Skipjack, mientras que OCB es utilizado para el modo de cifrado.
- LLSP: por último, cabe mencionar este protocolo que permite autenticar la identidad de igual manera con un reducido gasto de energía. Por otra parte, permite fortalecer la integridad de los datos mediante algoritmos criptográficos, lo que permite también apoyarse en seguridad semántica.

Seguridad en IEEE 802.15.4.

Respecto a la seguridad en el estándar IEEE 802.15.4, cabe mencionar que usualmente son redes que usan dispositivos de costos reducidos y una gran limitación de procesamiento, además en términos de almacenamiento y de

consumo de energía. En este sentido, su seguridad es difícil de garantizar, y es preciso realizar pruebas adecuadas para ello (Vásquez, 2021).

Los servicios que refieren a seguridad en este estándar son la confidencialidad de los datos, en que se garantiza que la información circulante no esté disponible para terceros no autorizados; la autenticidad de los datos, que se garantiza mediante la verificación de la identidad tanto de remitente como de destinatario; y, además, la protección antirepetición, evitando con ello la información duplicada. Esto se lleva a cabo en MAC una vez que se solicita por parte de las otras capas (Vásquez, 2021).

2.3 Auditoria de seguridad

La auditoría se refiere a la evaluación de forma crítica y sistemática que efectúan un conjunto de expertos, por lo cual es necesario aplicar mecanismos para una indagación exhaustiva. En este contexto, la auditoría de seguridad se enfoca en la implementación de mecanismos y técnicas para la evaluación de los aspectos relacionados con el sistema o elemento informático de una organización, esto ayuda a establecer el nivel de protección de los activos y verificar si las acciones se aplican de forma segura (Bracho, 2017a).

Aza (2019) considera que una auditoria de seguridad representa una forma de estudiar, analizar y gestionar los recursos o sistemas informáticos, el cual se efectúa por profesionales (auditores) con la finalidad de conocer y corregir las vulnerabilidades que pueden presentarse, para ello se enfocan en revisar de forma exhaustiva los sitios de trabajo, redes y servidores.

Por lo tanto, al aplicar la auditoria de seguridad se puede identificar la situación de los activos de la compañía respecto al tipo de control, protección y medidas implementadas, hallando las vulnerabilidades y la presentación de un informe sobre las falencias y recomendaciones para mejorar la seguridad. En otras palabras, permite mejorar la eficacia del sistema informático a través de la identificación de los problemas de seguridad y posteriormente establecer planes correctivos. La importancia radica en que la auditoría permite inspeccionar los

posibles riesgos para dar una solución concreta. Las características de una auditoría se seguridad se describen a continuación:

- Debe ser independiente para lograr objetividad en las evaluaciones.
- Debe aplicarse de forma planificada para obtener un análisis exhaustivo.
- Se debe analizar la situación actual de los recursos para brindar soluciones adecuadas.

Para Baca (Baca, 2016) una auditoría de seguridad consta de las siguientes etapas que son las más comunes:

Tabla 9.

Etapas comunes de auditoría de seguridad

Etapas	Características
Planeación	• Obtener información de la empresa. • Identificar la existencia de políticas de seguridad. • Identificar la topología de la red, firewall, etc. • Revisar que los equipos de la red estén funcionando.
Realización	• Solicitar la participación de los colaboradores. • Aplicar instrumentos de investigación (encuestas, entrevistas, entre otros). • Evaluar las conexiones inalámbricas, red de datos, entre otros con la finalidad de identificar vulnerabilidades.
Análisis de datos recabados y condiciones observadas	• Analizar información recopilada en la etapa anterior. • Utilizar herramientas gráficas para comparar los resultados con los estándares. • Sustentar el análisis.

Elaboración informe escrito y emisión de opinión	• Se presenta un resumen de la auditoría aplicada. • Se detalla las vulnerabilidades encontradas. • Se emite sugerencias para mejorar la situación actual de la seguridad.

Nota. Adaptado de (Baca, 2016)

Por su parte, Bracho (2017) destaca que existen cuatro tipos se auditoría de seguridad, lo cual se describe de la siguiente manera:

Tabla 10.

Tipos de auditoría de seguridad

Tipos	Características
Seguridad interna	• Se analiza; riesgos, impacto y vulnerabilidades dentro de la compañía. • Se evalúa la seguridad de la red local.
Seguridad perimetral y de DMZ	• La auditoría se efectúa desde el Internet. • Evalúa el nivel de protección de la red o servidores la empresa. • Se aplican ataques contra la red con previa autorización de la compañía. • Permite identificar si la red es vulnerable respecto al ataque planificado.
Forense	• Se aplicado cuando ya existe un ataque a la red. • Se valora los daños ocasionados por el ataque. • Se selecciona únicamente a la máquina o elementos de la red atacada para una valoración detallada.
Test de intrusión	• Se accede a los sistemas para verificar el nivel de resistencia de la red a una intrusión. • Se aplica una base de datos de las vulnerabilidades con el fin de la automatización del análisis. • Complementa a la seguridad perimetral.
Aplicaciones	• Representa una evaluación externa de la web.

	• Enfocado a evaluar las aplicaciones de la compañía. • Se aplican diferentes pruebas como: inyección SQL, escalamiento de directorios, desborde de búfer, entre otros.

Nota. Adaptado de (Bracho, 2017)

2.3.1 Modelos de auditorías de seguridad en redes de sensores

Dada la heterogeneidad de las WSN, las pruebas y revisiones de seguridad dependen bastante del tipo particular de entorno, topología, etc. que se esté utilizando. No obstante, Tejedor (2020) plantea que las auditorías en entornos con WSN se basan en los mismos factores que las auditorías de sistemas tradicionales. En este sentido, es importante definir claramente el eje de la auditoría (hardware, software, conexión, etc.), los objetivos, el alcance y el procedimiento (Tejedor, 2020).

Además, cabe mencionar que existen distintos estándares que han diseñado procesos de auditoría generales para sistemas que gestionan información. Entre estos se encuentran los estándares ISO, ISACA, CISA, CISM, entre otros. De esta manera, estos estándares generales permiten identificar a los activos informáticos de que disponen las organizaciones para protegerlos y preservarlos (Pomachagua, 2021).

Algunas de las principales metodologías existentes para el desarrollo en general de auditorías informáticas son las siguientes:

- OSSTM: método de evaluación propuesto por el *Institute For Security And Open Methodologies* (ISECOM), la cual se basa en el estudio de seis ámbitos en particular: seguridad de información, de procesos, de tecnología de internet, de comunicaciones, inalámbrica y física(Allaica & Guevara, 2020). Esta cuenta con cuatro fases: inducción, en la que se recolecta toda la información disponible sobre la organización y la que sea pertinente en función del objetivo de la auditoría; la fase de interacción,

en la que se determinan las pruebas en particular a aplicar una vez que se ha definido el alcance de la auditoría; la investigación, en donde se llevan a cabo actividades sobre análisis de activos; y, por último, la fase de intervención, la que consiste en la valoración de la efectividad del control de los mecanismos de seguridad y se establecen conclusiones a partir de la información obtenida (Gordón & Pacheco, 2018).

- OWASP: centrada en las aplicaciones web, OWASP (Open Web Application Security Project) busca el resguardo de la integridad de las aplicaciones web a partir de la identificación de los riesgos que se presentan sistemáticamente en este tipo de tecnología (Muñoz & Mayorga, 2017).

- Offensive Security: metodología que busca identificar vulnerabilidades de seguridad a través de auditorías de seguridad que presentan los siguientes pasos: recolección de información, análisis de las vulnerabilidades, definición de los objetivos secundarios, ataques y análisis de resultados (León Gudiño, 2017).

- ISSAF: refiere a una metodología de carácter estructurado para el análisis de la seguridad en sistemas informáticos. Desarrollada por OISSG (Open Information System Security Group), tiene un amplio alcance, y permite el análisis de infraestructura de red, S.O., aplicaciones y gestores de bases de datos (Fuertes, 2014). No tiene actualizaciones recientes.

Como metodologías de análisis de riesgos en sistemas informáticos de organizaciones. (Tejena-Macías, 2018) detalla:

- OCTAVE: *Operationally Critical Threats Assets and Vulnerability Evaluation* (OCTAVE) corresponde a una metodología que permite analizar los riesgos de seguridad que se presentan a nivel de información en las empresas, además de la proposición de planes para mitigarlos. Con base en los principios de la seguridad en la información, esta metodología equilibra los aspectos operativos, mecanismos de seguridad y las

tecnologías. Hasta la fecha tiene tres versiones dependiendo del enfoque organizacional y el tamaño de la entidad a auditar.

- MEHARI: esta metodología (*Method for Harmonized Analysis of Risk*) ofrece una serie de instrumentos para analizar riesgos y vulnerabilidades (ya sean cualitativos o cuantitativos), diseñada igualmente para el estudio organizacional de la gestión y seguridad en la información.

- CRAMM: desarrollado por Central and Telecommunications Agency (CTTA), CRAMM es una iniciativa del gobierno británico para el análisis en riesgos de ataques a los que están expuestas las organizaciones. Así, a partir de los principios de la seguridad informática, CRAMM analiza riesgos y vulnerabilidades de forma mixta (cualitativos y cuantitativos), mediante el uso de una matriz de cruce entre los activos y los riesgos en ámbitos de integridad, disponibilidad y confidencialidad.

- EBIOS: la metodología EBIOS (Expresión de las Necesidades e Identificación de los Objetos de Seguridad) nació para fortalecer la gestión de riesgos informáticos en organizaciones compatible con ISO. Enfatiza el conocimiento sobre los activos más importantes de la organización y en la identificación de las vulnerabilidades a las que se encuentra más expuesta.

- NIST SP 800-30: elaborado por NIST (Instituto Nacional de Estándares y Tecnología), este estándar tiene por objetivo evaluar los riesgos que presentan los sistemas informáticos, para lo que provee nociones para gestionar los riesgos y herramientas para su evaluación, control y mitigación. Se compone de nueve fases, que van dese la caracterización del sistema hasta la generación de un informe con los detalles de los resultados obtenidos y las propuestas de mejora.

- MAGERIT: esta metodología permite analizar los riesgos del sistema de información y establecer recomendaciones de acciones adecuadas con el fin de controlar, disminuir y prevenir riesgos. Las fases inician con la

identificación de activos, caracterización – valoración de amenazas, valoración de salvaguardias, estimación y gestión del riesgo (Alvarado-Zabala et al., 2018).

- 27005 ISO: es una norma que determina recomendaciones para la gestión del riesgo de la seguridad informática. Inicia desde la identificación del contexto de la organización, analizar riesgos de los activos, valoración y gestión de riesgos (Sisteseg Consulting Services, 2018).

2.3.2 Herramientas y técnicas de auditorías en seguridad en redes

Las herramientas y técnicas de auditorías en seguridad en redes se describen de la siguiente manera:

Tabla 11.

Herramientas y técnicas de auditorías en seguridad

Descripción	Características
Técnicas	
Enumeración en redes	• Identifica las redes IP de la compañía. • Se puede utilizar Whois o servicio DNS para conocer la IP. • Permite el rastreo masivo de la red.
Barrido de puertos	• Permite conocer la red TCP y UDP. • Se puede emplear la herramienta Nmap.
Fingerprinting	• Técnica para conocer las aplicaciones y sistema operativo usada por en los servidores. • Se puede emplear la herramienta Nmap y Wireshark.
Rastreo de redes	• Se recaba información de la enumeración de redes. • Permite analizar las vulnerabilidades. • Se puede emplear Nmap. • Las técnicas utilizadas pueden ser: barrido IP, TCP y UDP, identificar aplicaciones y sistema operativo.

Test de penetración	• Evalúa la efectividad de los protocolos de seguridad. • Cuando hay vulnerabilidades aplica la técnica de explotación. • Utiliza la técnica de fuzzing para detección de vulnerabilidades no conocidas. • Se clasifica en caja negra (emulsión de ataque), blanca (acceso total de la información) y gris (mezcla caja blanca – negra).
Análisis de vulnerabilidades	• Técnica aplicada para detección de vulnerabilidades del sistema para su corrección. • Se puede emplear herramientas como Nessus.
Herramientas	
Nmap	• Realiza auditoría en la red. • Escanea la red de forma pasiva o activa. • Ayuda a identificar los dispositivos conectados a la red. • Permite la extracción de información de los dispositivos.
Tcpdump	• Captura el tráfico de la red de forma pasiva. • Presenta solo información relevante.
Airodump-ng	• Permite la filtración de los datos capturados. • Presenta las características relevantes de las redes inalámbricas.
Wireshark	• Captura el tráfico en tiempo real en una interfaz de la red. • Solo permite la visualización de paquete de datos.
Nessus	• Facilita el escaneo de vulnerabilidades. • Permite la reparación de las vulnerabilidades, parches, configuraciones, malware, defectos del software, entre otros.

Nota. Adaptado de (Bracho, 2017); (Otero Dans, 2021)

2.4 Trabajos relacionados

El estudio documental de (Gutiérrez-Portela et al., 2021a) aporta una síntesis importante de cómo se ha venido trabajando e investigando en materia de seguridad en WSN. Como se obtiene en los resultados, los principios de seguridad más extendidos son los planteados por la norma ISO / IEC 27001: 2013, sobre seguridad de la información, los que identifican a la preservación de la confidencialidad, la integridad, la disponibilidad y la autenticidad como relevantes. Los principales ataques identificados en la literatura son los *flood attack*, ataques al tráfico en la información e interceptación, interferencia, desvíos selectivos, *phishing*, *routing*. La criptografía se presenta como la tendencia en gestión de la seguridad en WSN.

El trabajo de Mejía (Mejía, 2019) buscó identificar e implementar mecanismos de seguridad en un sistema en particular basado en WSN en función de las vulnerabilidades identificadas. Para esto, realizó un análisis documental que permitió identificar como vulnerabilidades intrínsecas de WSN como ataques de acceso, a la privacidad, a la integridad, denegación de servicios, entre otros. Se utilizó el software Nessus para identificar vulnerabilidades, entre las que contaron: fallo de parche de actualización de Ubuntu 18.04 Lts, Apache 2.4x (fallas de escritura en funciones, omisiones, defectos en manipulación de datos, fallas de lectura, entre otras), vulnerabilidad en el certificado del servidor (X.509), posibilidad de acceso al servidor sin identificación, entre otras.

En el contexto de la aplicación de WSN al IoT, el trabajo de Carrizo y Vargas (Carrizo-Díaz & Vargas-Lombardo, 2017) realiza una valoración de la seguridad en el estándar ZigBee. La red analizada es de topología de malla, construida con base en estándares de seguridad de norma IEEE 802.15.4, la cual presenta tres mecanismos fundamentales para la seguridad: control de acceso, es decir, autenticación; cifrado con criptografía (clave simétrica AES); e integridad. Las principales vulnerabilidades a que está expuesta esta WSN en particular son en capa física: clonación de etiquetas, espionaje, spoofing; en la capa de control se encuentran accesos sin autorización, ataques DDOS; en la

capa de red se identificaron ataques de privación de hibernación en nodos, introducción de código malicioso, ataque de escuchas ilegales con hombre en medio (interceptación); en capa de aplicación se encontró inyección del código malicioso, denegación de servicios, *phishing*, y *sniffing*.

Respecto a las valoraciones de seguridad, auditorías de seguridad y pruebas de penetración en redes, Tejedor (2020) realizó un estudio en el cual se enfocó en la tecnología Bluetooth, dada su relevancia en ecosistemas IoT. Así, para evaluar la seguridad realizó una auditoría de seguridad mediante *pentest* de un *smartlock*, en particular a la tecnología BLE utilizada, la cual se desarrolló en un laboratorio particular y con el uso de un smartphone con S.O. Android. Además de vulnerar la seguridad del dispositivo, una de las conclusiones relevantes obtenidas es que el alcance de la auditoría fue insuficiente, dada la cantidad de factores emergentes que requerían ser analizados para garantizar la seguridad del dispositivo.

Por su parte, Arias et al. (Arias Martínez et al., 2021) analizaron la seguridad en el contexto de redes de sensores de telemetría en internet de las cosas. El foco estuvo puesto en el análisis de hardware, software y otros componentes de la nube de gestión de IoT a nivel privado. Con ello se buscó determinar una arquitectura robusta y segura ante ataques de penetración, denegación de servicios y robo de información, efectuando un análisis por capas; el producto resultante es una red de sensores en IoT que con pocos recursos dispone de elevados grados de seguridad.

En base a lo expuesto, se evidencia que las investigaciones se enfocan a la implementación de seguridad, valoración de seguridad, auditorias, especialmente relacionadas con investigación documental y en menor proporción análisis de seguridad. Por lo tanto, con la presente investigación se aplica un análisis técnico mediante pruebas en escenarios reales para identificar vulnerabilidades en la red WSN.

CAPÍTULO 3. DISEÑO Y APLICACIÓN DE LA METODOLOGÍA

En el tercer capítulo se presenta el diseño de la metodología, por lo que se determina el enfoque, tipo de investigación y el mecanismo de desarrollo a través de Offensive Security para realizar la auditoría de seguridad a redes de sensores inalámbricas, así como la metodología de análisis de riesgos NIST SP 800-30. Posteriormente, se describe las primeras fases de la metodología Offensive Security, complementando la evaluación de riesgos según cada ataque.

3.1 Enfoque

En la presente investigación se considera un enfoque cuantitativo, pues, permite recolectar información de la cantidad de vulnerabilidades identificadas en una red de sensores inalámbrica. Entre las vulnerabilidades que se aplicaron a los sensores se relacionan con los ataques más comunes que se detallan en el capítulo IV. De igual modo, se aplica el enfoque cualitativo debido a que se analiza las técnicas intrusivas y la vulnerabilidad encontrada obtenidos de las pruebas basadas en dos escenarios reales (medir temperatura y medir temperatura + CO2).

3.2 Tipos de investigación

Para el desarrollo del proyecto se toma en cuenta el tipo de investigación descriptivo y bibliográfico – documental. En la investigación descriptiva se detalla las vulnerabilidades de la red de sensores inalámbrica, esto luego de aplicar los escenarios reales.

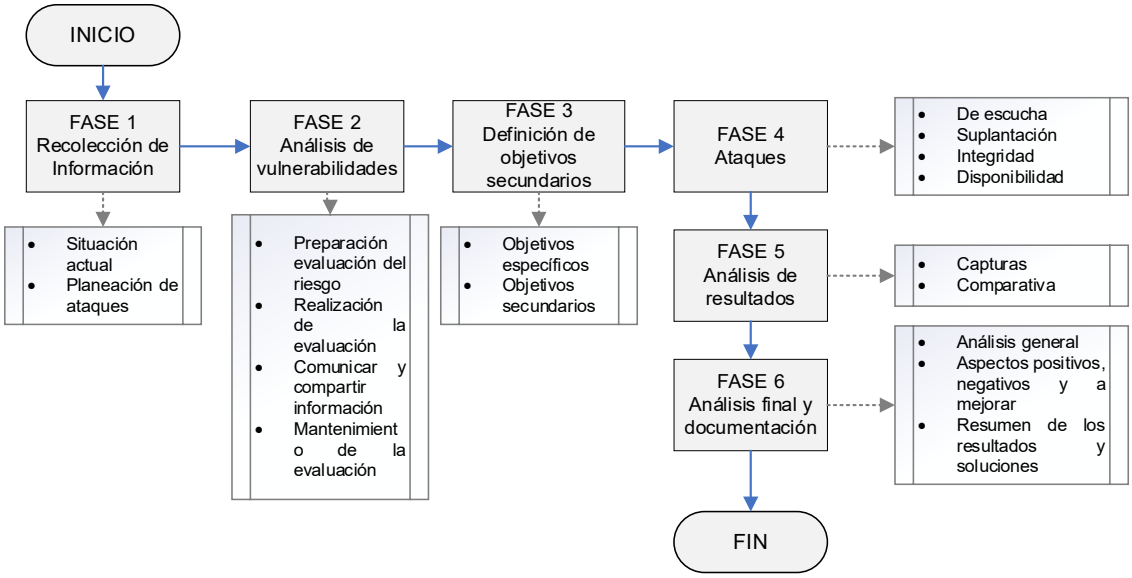
Por otra parte, con la investigación bibliográfica – documental se recopila información de fuentes secundarias como libros, revistas, artículos científicos, guías respecto a la seguridad en redes, redes de sensores inalámbricas, auditoría de seguridad; lo cual ayuda a sustentar teóricamente el proyecto.

3.3 Metodología de desarrollo

En cuanto a la metodología de desarrollo se toma como base “Offensive Security” que se muestran sus fases en la Figura 5 para realizar la auditoría de seguridad a redes de sensores inalámbricas. A continuación, se detallan las etapas de la metodología:

Figura 5.

Diagrama de la metodología de auditoría



Nota. El diagrama muestra las fases de la metodología de auditoría

- **Recolección de información:**

En la primera etapa se evalúa la situación actual respecto a la seguridad de la red de sensores inalámbricas, lo que ayuda en la planeación de ataques. Por lo que se utiliza la herramienta WireShark y ZBOSS Sniffer para obtener información.

- **Análisis de vulnerabilidades:**

Previo el desarrollo se utilizó la metodología de análisis de riesgos NIST SP 800-30, es así que se preparó, realizó, compartió y efectúa mantenimiento de la evaluación a cada ataque planificado.

A continuación, se presenta las matrices para análisis de riesgo y su respectiva interpretación:

Tabla 12.

Matriz nivel de riesgo

Probabilidad de amenaza	**Impacto**		
	Bajo (10)	**Medio (50)**	**Alto (100)**
Alta (1,0)	Bajo 10*1,0=10	Medio 50*1,0=50	Alto 100*1,0=100
Media (0,5)	Bajo 10*0,5=5	Medio 50*0,5=25	Alto 100*0,5=50
Baja (0,1)	Bajo 10*0,1=1	Bajo 50*0,1=5	Bajo 100*0,1=10

Nota. Tomado de la Guía NIST SP 800-30 (NIST, 2002)

Tabla 13.

Descripción nivel de probabilidad

Nivel	**Descripción**
Alto	Está altamente motivada, donde los controles que previenen muestran la vulnerabilidad no eficiente.
Medio	Está motivada, donde los controles previenen que se presente una vulnerabilidad.
Bajo	No tiene motivación y se evita la presencia de vulnerabilidad.

Nota. Tomado de la Guía NIST SP 800-30 (NIST, 2002)

Tabla 14.

Descripción magnitud de impacto

Nivel	**Descripción**
Alto	1. Pérdidas costosas de los recursos. 2. Daño significativo 3. Pérdidas extremadamente significativas.
Medio	1. Pérdidas costosas de los recursos. 2. Daño significativo 3. Lesiones o afectación en ocasiones.

Bajo	1. Pérdidas de algunos de los recursos. 2. Afecta intereses.

Nota. Tomado de la Guía NIST SP 800-30 (NIST, 2002)

Tabla 15.

Descripción riesgos y acciones

Nivel	Descripción
Alto	Plantear medidas correctivas lo más pronto o a corto plazo.
Medio	Plantear medidas correctivas en período razonable.
Bajo	Se decide si se aplican medidas o el riesgo es razonable.

Nota. Tomado de la Guía NIST SP 800-30 (NIST, 2002)

Cabe mencionar que para el desarrollo se utiliza la herramienta Zigbee-emulador CC, depurador, programador USB. Por lo tanto, se combina la ejecución del código de software en una plataforma virtual de la arquitectura de hardware.

Por ende, con el simulador se evaluará el comportamiento de la red bajo diferentes condiciones, detectando los ataques más dañinos y los nodos o configuraciones más vulnerables. El proceso incluye los siguientes pasos:

- Identificar los nodos (coordinador y sensor).
- Determinar parámetros orientados al rendimiento (temperatura y CO2).
- Enlazar en un ordenador.
- Generar un ejecutable instrumentado.
- Realizar diferentes tipos de ataques para evaluar el comportamiento y las prestaciones de los nodos de la WSN.
- Obtener los resultados del análisis y comparativa de las pruebas intrusivas.

Los datos obtenidos pueden ser utilizados para evaluar los efectos de los ataques en los nodos de la red. Con la información recopilada se puede hallar las vulnerabilidades existentes en la red de sensores inalámbricas, empleando ZBOSS Sniffer y WireShark con la finalidad de realizar pruebas y encontrar

vulnerabilidades. Respecto al escaneo de nodos, hallar la información crítica y el escaneo. Posteriormente, se detalla todas las vulnerabilidades y la seguridad con el propósito de identificar los principales problemas de seguridad.

- **Definición de objetivos secundarios:**

Para evitar barreras que impiden cumplir el objetivo general de manera adecuada se establece medidas para superar los obstáculos, es así que los objetivos secundarios están relacionados con la red de sensor inalámbrica, lo cual ayuda a obtener éxito al momento de ejecutar un ataque.

- **Ataques:**

En la cuarta fase se planifica el desarrollo para realizar ataques. Por lo que se inicia con la explotación de la vulnerabilidad de la red de sensor inalámbrico, utilizando ZBOSS Sniffer y WireShark.

- **Análisis de resultados:**

En esta fase se presenta los resultados de los ataques efectuados (capturas de pantalla) y se aplica el método CVSS (*Common Vulnerability Score System*) para comparar las técnicas o pruebas intrusivas. Este modelo representa un mecanismo para establecer puntuación a las características de los elementos (CVSS, 2023a).

Tabla 16.

Escala de calificación CVSS

Calificación	Escala
0	Nulo
1 – 3,9	Bajo
4 – 6,9	Medio
7 – 8,9	Alto
9 - 10	Muy Alto

Nota. Tomado de (CVSS, 2023)

- **Análisis final y documentación:**

En la última fase se presenta el informe final de la auditoría de seguridad, donde se detalla las vulnerabilidades y ataques identificados, así como la respectiva solución a las mismas.

3.4 Análisis preliminar

En este apartado se comienza a aplicar las primeras fases de la metodología de desarrollo como la recolección de información, análisis de vulnerabilidades y definición de objetivos secundarios.

3.4.1 Introducción

La red de sensores inalámbricos tiene diferentes aplicaciones como la automatización industrial, video vigilancia, monitorear el tráfico, hogares inteligentes, entre otros. Por lo que es importante que los sensores deben contar con un mecanismo o identificar posibles ataques que afectan a la funcionalidad y seguridad. Al identificar los ataques se podrá emplear mecanismos que impidan o limiten el acceso a la información confidencial, evitando que sea obtenida por terceros.

En este sentido, previo a la primera fase se debe planificar la forma de aplicar la metodología o su respectiva actividad. Además, de tomar en cuenta los siguientes aspectos:

- Adquisición e instalación de equipos: Se considera las especificaciones técnicas de los sensores previo a la compra o la instalación. Tomando en cuenta las necesidades de los usuarios o clientes.
- Protección de sensores: Se debe realizar análisis de la seguridad para identificar los posibles ataques y establecer mecanismos de protección.
- Mantenimiento de sensores: Es importante establecer un plan de mantenimiento preventivo y correctivos.

- Control de acceso de los sensores: Se revisa periódicamente que los sensores funcionen adecuadamente.
- Reubicación de sensores: Si después de realizar el mantenimiento, el equipo no funciona se debe cambiar el equipo.
- Control de acceso de la red: Se debe verificar el funcionamiento correcto del acceso.
- Acceso a la red: Se controla el acceso a los servidores de la red.

Por otro lado, se presenta la planificación para el desarrollo de la auditoría de seguridad, donde las horas de esfuerzo representan la cantidad de tiempo diaria que el desarrollador debe cumplir con cada una de las actividades planificadas. El esfuerzo se obtiene de la multiplicación de la duración en días por horas esfuerzo. El tiempo total para el desarrollo del proyecto es de 106 días con esfuerzo de 679 horas.

Tabla 17.

Planificación

	AUDITORÍA DE SEGURIDAD					
	Metodología de auditoría de seguridad intrusiva en redes de sensores inalámbricos WSN para el análisis de vulnerabilidades.					
N	**Actividades**	**Duración**	**Fecha**		**Horas esfuerzo**	**Esfuerzo**
		(días)	**Inicio**	**Fin**		
A	**Introducción**	**2**	**26/10/2022**	**26/10/2022**		**8**
A.1	Descripción general	1	26/10/2022	26/10/2022	4	4
A.2	Diseño de plan de desarrollo	1	27/10/2022	27/10/2022	4	4
B	**Recolección de información**	**8**	**28/10/2022**	**4/11/2022**		**32**
B.1	Análisis de situación actual de seguridad en sensores	4	28/10/2022	31/10/2022	4	16
B.2	Determinación de herramientas	1	1/11/2022	1/11/2022	4	4
B.3	Diseño de planificación de ataques	3	2/11/2022	4/11/2022	4	12
C	**Análisis de vulnerabilidad**	**30**	**5/11/2022**	**4/12/2022**		**210**
C.1	Determinación de herramientas	2	5/11/2022	6/11/2022	4	8
C.2	Utilizar herramientas (evaluación)	18	7/11/2022	24/11/2022	9	162
C.3	Identificar vulnerabilidades	10	25/11/2022	4/12/2022	4	40
D	**Definición de objetivos secundarios**	**6**	**5/12/2022**	**10/12/2022**		**24**
D.1	Revisión de objetivos específicos	3	5/12/2022	7/12/2022	4	12
D.2	Revisión de objetivos secundarios	3	8/12/2022	10/12/2022	4	12
E	**Ataques**	**35**	**11/12/2022**	**14/1/2023**		**290**

E.1	Planifica ataques	5	11/12/2022	15/12/2022	4	20
E.2	Realiza ataques	15	16/12/2022	30/12/2022	9	135
E.3	Explotación de la vulnerabilidad	15	31/12/2022	14/1/2023	9	135
F	**Análisis de resultados**	**19**	**15/1/2023**	**2/2/2023**		**76**
F.1	Presentación de hallazgos	5	15/1/2023	19/1/2023	4	20
F.2	Determinación de método comparativo	4	20/1/2023	23/1/2023	4	16
F.3	Determinación de métricas	3	24/1/2023	26/1/2023	4	12
F.4	Comparación de pruebas intrusivas	5	27/1/2023	31/1/2023	4	20
F.5	Selección de la mejor alternativa	2	1/2/2023	2/2/2023	4	8
G	**Análisis final y documentación**	**6**	**3/2/2023**	**8/2/2023**		**39**
G.1	Presenta evidencias	3	3/2/2023	6/2/2023	4	12
G.2	Presentación documentación (aspectos positivos, negativos, a mejorar y medidas o soluciones)	3	7/2/2023	8/2/2023	9	27
	Total (días)	**106**	**Total (esfuerzo)**			**679**

Nota. La tabla presenta la planificación

3.4.2 Fase 1: Recolección de información

En esta fase se analiza la situación actual de los sensores inalámbricos respecto a la vulnerabilidad. Además, se presenta el flujo del proceso del nodo coordinador, sensor y topología. Posteriormente, se realizó la planeación de ataques de confidencialidad, integridad y disponibilidad, por lo que se planteó dos escenarios reales con la finalidad de identificar vulnerabilidades para establecer medidas preventivas, lo cual ayuda a que los sensores inalámbricos sean seguros y evitar ataques o tener mecanismos de protección. A continuación, se detalla dos tipos de escenarios:

- **Escenario 1:** Red de sensores inalámbricos que miden la temperatura.

En este sentido, el proceso del escenario comienza con la configuración de la red y puertos, verifica datos, se obtiene datos y se muestra el nivel de temperatura, considerando para ello, los tres tipos de ataques. Para este procedimiento, se tomó en cuenta que la red de sensor inalámbrico se enfoca en el campo de la agricultura moderna, pues, según MeteoSur SRL (MeteoSur, 2020) es uno de los principales usos para monitorear mediante tecnología con precisión, el clima, temperatura, humedad del suelo, entre otros; esto ayuda a

los cultivos de calidad debido a que con los datos recopilados de la red de sensores se tiene la posibilidad de mitigar los riesgos (falta de agua, hongos, exceso de calor, etc.) mediante toma de decisiones oportunas y la rentabilidad de los mismos.

- **Escenario 2:** Red de sensores que mide temperatura y CO2.

Para el segundo escenario se aplica similar proceso que el primero, pero se añade la medición del CO2. Por lo tanto, se consideró como campo de aplicación en transporte automotriz debido a que ayuda a monitorear el nivel del aire, es decir, la contaminación (CO2) y la temperatura o calor en las ciudades, la cual es empleada por el departamento o unidad de transporte o entidades responsables del cuidado del entorno con la finalidad de establecer acciones concretas para mitigar los problemas. Incluso en el sector automotriz se aplica para medir las emisiones de CO2 derivadas del motor de combustión interna y establecer mecanismos que ayuden disminuir el nivel de contaminación en el interior de la cabina de auto (Mordor Intelligence, 2023).

3.4.2.1 Situación actual

Para el análisis de la red de sensores inalámbricos se consideró la información recopilada respecto a los ataques de seguridad a los que están expuestos, estos se detallan en la sustentación teórica. Además, según (Gutiérrez-Portela et al., 2021a) los nodos de los sensores muestran mayor vulnerabilidad debido a que se encuentran instalados en un entorno difícil, tienen energía y memoria limitada, así como el bajo nivel de procesamiento y transmisión de medios de difusión. De tal modo que, para identificar las amenazas se debe aplicar un mecanismo oportuno con la finalidad de establecer soluciones de seguridad y privacidad. Otro de los aspectos que generan vulnerabilidad en la red de sensores se relacionan con la ubicación geográfica, limitación de recursos computacionales y el medio de transmisión. Por lo tanto, la red de sensores inalámbricas puede sufrir principalmente los siguientes ataques:

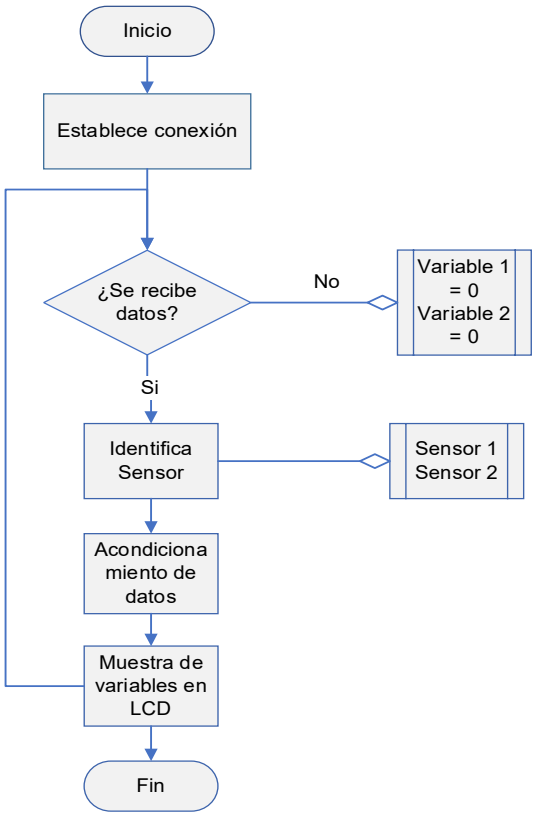
- Capa física: manipulación.
- Capa de enlace: Colisión, agotamiento, interrogación, denegación del modo dormido y Homing.
- Capa de red: Ataque Blackhole, desvío selectivo, fraude de identidad, Hello Flood, sinkhole, wormhole, Sybil, redirección, caer en el agujero, fuga de información/captura de tráfico, interferencia constante, drenaje de energía y mala dirección.
- Capa transporte: inundación y desincronización.
- Capa de aplicación: Overwhelm, reprogramación, protocolos de sincronización de reloj, software y applicattion.
- Otros: Link-Noise Attacker, Fake packet injection Attacker, atacante directo y Link + Injector attacker, pérdida de equipo robado, espionaje de usuario a usuario, puntos de acceso falsos, denegación de servicio y sesiones de cuentas de secuestro.

Cabe mencionar que se pueden presentar riesgos como datos no cifrados, falta de protección de firewall y conexiones de dispositivos que no se encuentran autorizados de la puerta de enlace. Por lo tanto, la perspectiva sobre los mecanismos de seguridad de las WSN se convierte en un tema de interés, pues, aunque existen contramedidas contra ataques se requiere el desarrollo de nuevos mecanismos de seguridad para proteger las WSN y protocolos de enrutamiento que aseguren la comunicación entre los nodos.

Por otra parte, en la actualidad se identifican avances en la disponibilidad de la red de sensores inalámbricos mediante el desarrollo de IDS y autenticación. Respecto a la privacidad se está usando cifrado de extremo a extremo, pues, se emplean clave simétrica y minería de datos, este último permite identificar si se tiene privacidad adecuada. A continuación, se identifica el flujo de funcionamiento del nodo coordinador (Figura 6) y sensores (Figura 7):

Figura 6.

Diagrama de flujo funcionamiento nodo coordinador

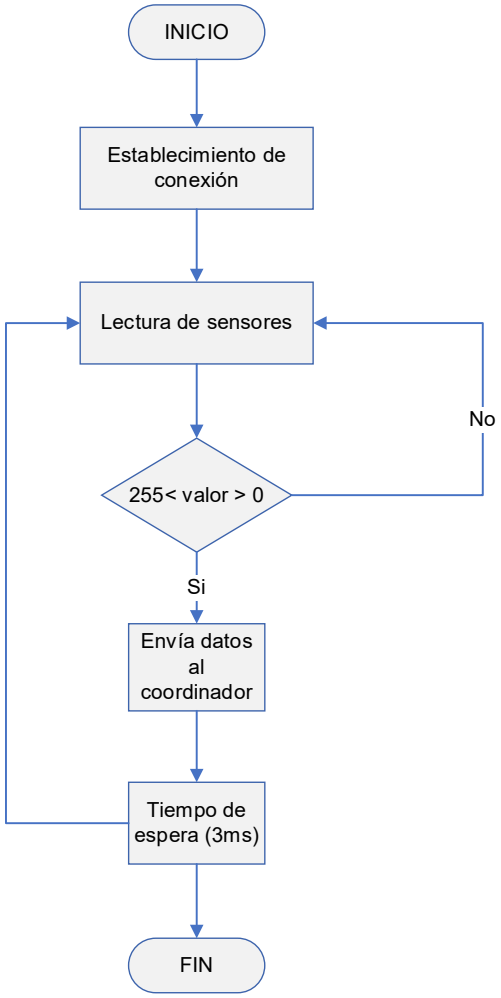


Nota. Se presenta el diagrama de la funcionalidad del nodo coordinador.

Por ende, se inicia con la configuración de la red de sensores inalámbricos y los puertos. Luego se verifica si recibe los datos. Una vez determinado que se recepta los datos proceso a identificar el sensor (1 y 2) y por último presenta la temperatura de los mismos.

Figura 7.

Diagrama de flujo funcionamiento nodos sensores

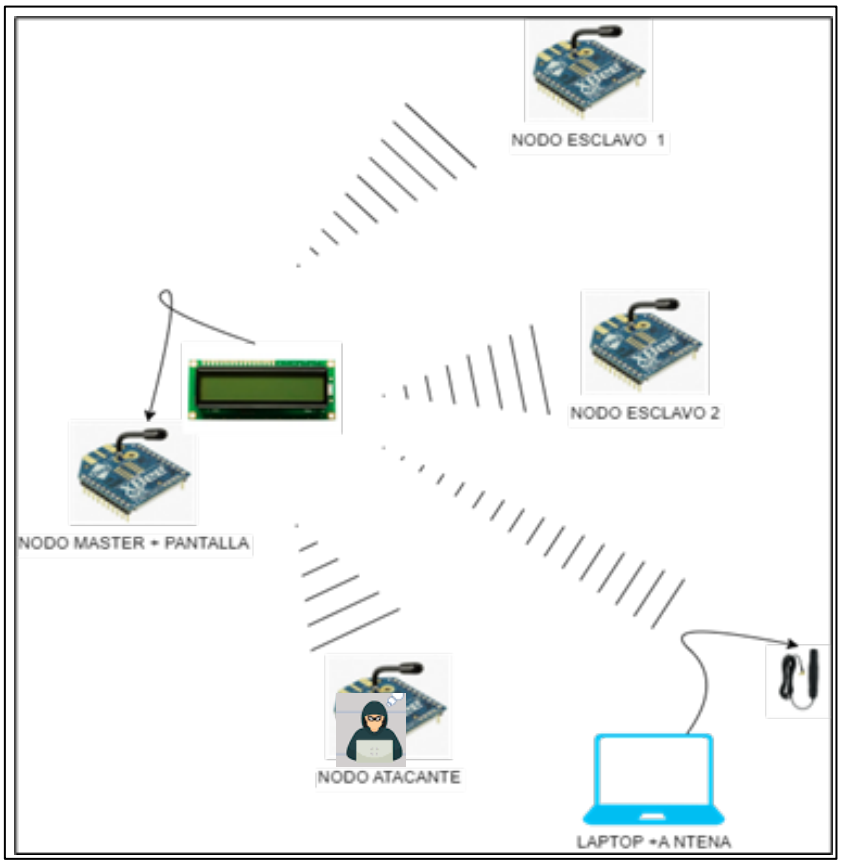


Nota. Se presenta el diagrama de la funcionalidad de los nodos sensores.

El funcionamiento del nodo sensor comienza con la activación, en la que se realiza el vínculo a la red. Luego se efectúa la lectura de información de los nodos sensores. Cuando culmina la lectura, procede a la transmisión de los datos y se tiene el nodo esclavo 1, 2 y el atacante, este se conecta a la laptop para capturar las tramas. Cuando no culmina el proceso vuelve a leer la información en la pantalla caso contrario finaliza el período. A continuación, se presenta los elementos del sistema:

Figura 8.

Topología de elementos del sistema de nodos sensores



Nota. Se presenta el diagrama de la funcionalidad del nodo.

El sistema está compuesto por:

- Un nodo máster que tiene conectado una pantalla que muestra la información de los nodos esclavos.
- Dos nodos esclavos con sensores de temperatura que envían información al nodo máster.
- Una laptop que tiene conectada una antena, en la cual se realiza la captura de las tramas que envían los nodos esclavos
- Un nodo atacante que realiza los ataques de confidencialidad, integridad y disponibilidad.

3.4.2.2 Planeación de ataques

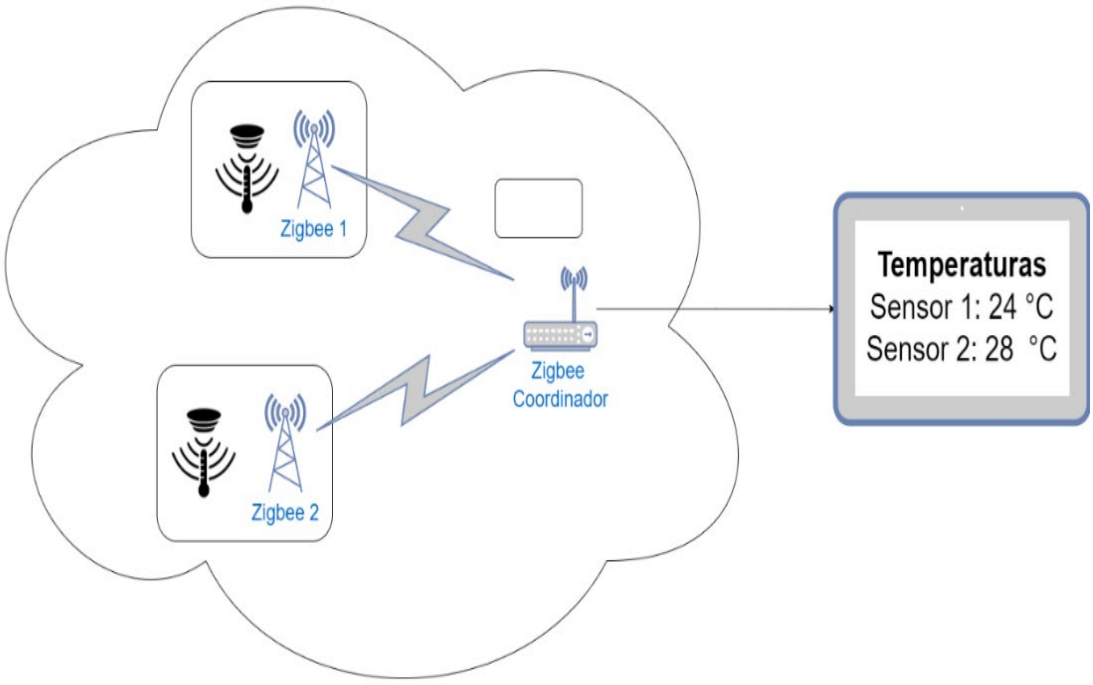
Para la planificación de ataques se consideró la guía para la gestión de pruebas según el estándar PCI SSC, por lo que se debe definir los alcances, selección del evaluador y coordinación (GlobalSec, 2021).

Alcance.

Se realiza la descripción de las actividades para el desarrollo de los ataques a la red de sensores inalámbricos. En la Figura 9 se aprecia la topología tanto de la red de sensores sin ataque:

Figura 9.

Topología de WSN sin ataque

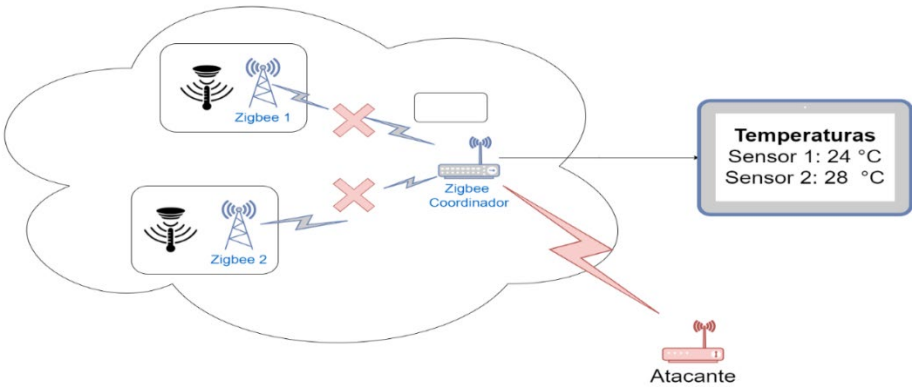


Nota. La figura muestra la topología de la red de sensores sin ataque.

Mientras que en la 11 y Figura 11 se muestra la topología y diagrama de flujo del ataque a la red de sensores inalámbricos:

Figura 10.

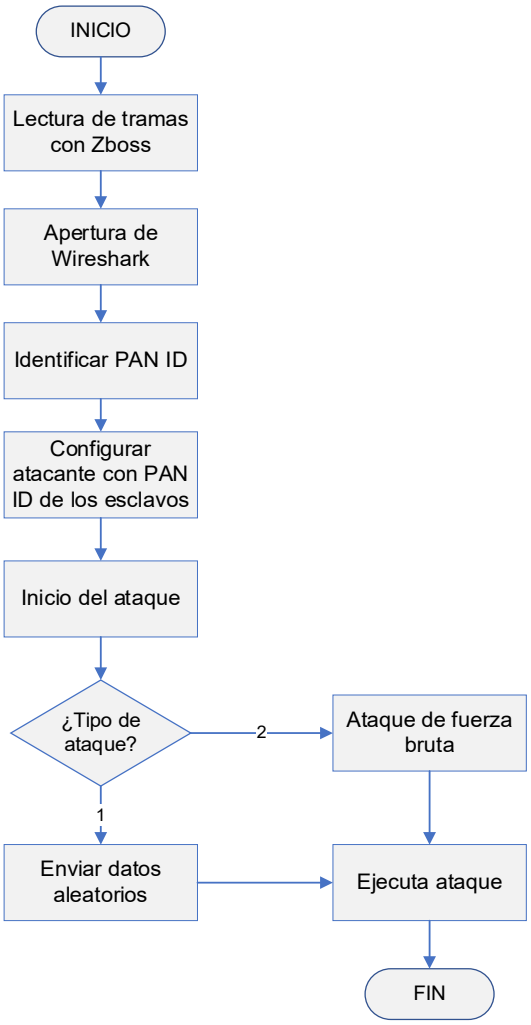
Topología ataque



Nota. Se presenta la topología de la planificación de ataque.

Figura 11.

Diagrama de flujo del proceso de ataque



Nota. Se presenta el diagrama de flujo del atacante.

Este proceso inicia con la lectura de tramas mediante el uso de la herramienta Zboss. Luego se apertura o emplea el programa Wireshark para la lectura de los paquetes capturados. Cuando se haya identificado la dirección del nodo coordinador PAN ID se procede a ejecutar el ataque. La cual depende del tipo de ataque, en el primero se envía datos aleatorios y el segundo se aplica el ataque de fuerza bruta.

Selección del evaluador.

En este caso, el responsable es el estudiante con el apoyo de un especialista en *penetration tester*, pues, se tiene el conocimiento y experiencia.

Coordinación.

Se establece como herramienta ZBOSS Sniffer, WireShark y Zigbee-emulador CC, depurador, programador USB. Los cuales se describen a continuación:

- **ZBOSS Sniffer**

Esta herramienta representa un rastreador de los paquetes Zigbee multiplataforma de código abierto, incluso cuenta con interfaz de uso sencillo y se adapta para funcionar con la herramienta de análisis de protocolos Wireshark. Además, admite el modo multicanal, lo que significa que puede usar con varios dispositivos y obtener paquetes de varios canales en una ventana de Wireshark.

Al ser una herramienta de código abierto incluye un archivo de binarios para Windows x64 (XP/Vista/7/10) y un paquete *deb* para Ubuntu Linux (12.04+). Está completamente probado y listo para usarse de inmediato. Cada archivo contiene la aplicación ZBOSS Sniffer GUI e imágenes hexadecimales de sniffer para la programación del hardware.

- **Zigbee-emulador CC, depurador, programador USB**

Es un hardware que permite recibir y decodificar señales dentro de la frecuencia del protocolo Zigbee.

Figura 12.

Emulador CC-Debugger, programador USB

Nota. Adaptado de (BdSpeedytech, 2016)

- **WireShark**

Es un software que permite la lectura de paquetes capturados en una red.

Figura 13.

Wireshark

Nota. Adaptado de (Wireshark, 2023)

Estas herramientas se emplean para realizar los ataques a la red de sensores. Los tipos de ataques a realizar en la red de sensores son los siguientes:

- Ataques de confidencialidad.
- Ataque de integridad.
- Ataque de disponibilidad.

Por otra parte, se establecen las reglas para la implementación de los ataques a la red de sensores:

- Establecer escenarios únicamente reales.
- Seleccionar las herramientas para realizar el ataque e identificar vulnerabilidades.
- Debe enfocarse en el control de los ataques.
- Seleccionar una red de sensor para los ataques.
- Sondear los puertos.

Tabla 18.

Planificación de ataques

Actividades	Tiempos (días)	Recursos	Responsables
Determinar las herramientas y equipos necesarios.	2	Económicos Tecnológicos Humanos	Kevin Oñate
Identificar tipo de ataques	2		
Determinar tipo de ataques	2		
Aplicar ataques según tipo	20		
Obtener resultados	3		
Identificar vulnerabilidades	2		
Analizar el nivel de seguridad en la red de sensores	2		
Presentar informe final de los ataques	2		

Nota. La tabla presenta la planificación de ataques a la red de sensores

3.4.3 Fase 2: Análisis de vulnerabilidades

Para el análisis de las vulnerabilidades se considera la metodología de análisis de riesgos NIST SP 800-30, este inicia desde la preparación para

evaluación de riesgos, realización de la evaluación, comunicación y mantenimiento.

3.4.3.1 Preparación para evaluación de riesgos

El propósito es identificar el nivel de riesgos que se presentan en cada ataque planificado. El alcance de la evaluación es aplicar la metodología para identificar los riesgos en los ataques en la red de sensor inalámbrica. La valoración del riesgo se define la matriz de riesgo, probabilidad, magnitud del impacto, escala de riesgos y acciones necesarias. Se utiliza los ataques definidos para los sensores inalámbricos.

3.4.3.2 Realización de la evaluación de riesgo

A continuación, se detalla el resultado de la evaluación de riesgos según cada ataque efectuado a la red de sensor inalámbrico:

Tabla 19.

Matriz fuente de amenaza

Activo	Ataque	Vulnerabilidad	Fuente de amenaza
Red de sensores inalámbricos	Confidencialidad	Rastreo de redes	Hacking
		Descifra información sensible	Hacking
		Captura activa de tráfico	Hacking
		Captura de paquetes	Hacking
		Lectura de datos	Hacking
	Integridad	Envío de datos manipulados	Alteración de datos
		Modificación aleatoria de datos mostrados	Alteración de datos
	Disponibilidad	Denegación del servicio	Hacking

Nota. La tabla presenta las fuentes de amenaza según cada ataque

Tabla 20.

Matriz nivel de evaluación de riesgo

Activo	Ataque	Vulnerabilidad	Probabilidad de amenaza	Impacto	Valoración de Riesgo
Red de sensores inalámbricos	Confidencialidad	Rastreo de redes	1,0	100	100
		Descifra información sensible	1,0	100	100
		Captura activa de tráfico	1,0	100	100
		Captura de paquetes	0,5	100	50
		Lectura de datos	0,5	50	25
		Envío de datos manipulados	0,5	100	50
	Integridad	Modificación aleatoria de datos mostrados	0,1	50	5
	Disponibilidad	Denegación del servicio	1,0	50	50

Nota. La tabla presenta la evaluación del riesgo adaptada de (NIST SP 800-30, 2002)

3.4.3.3 Comunicar y compartir información de evaluación de riesgos

Según la evaluación realizada se identifica que las amenazas identificadas en los sensores inalámbricos se relacionan con el hacking y alteración de datos. Las vulnerabilidades se basan rastreo de redes, descifrar información sensible, lectura de datos, entre otros. En cuanto a la evaluación de riesgos se observa que en el ataque de confidencialidad tiene un alto nivel probabilidad de amenaza, impacto y valoración, representando el 38% del total de las vulnerabilidades identificadas.

Aunque se aprecia que la mayoría presenta un rango moderado. En la captura de paquetes se presentan información de las distintas tramas, lo mismo ocurre en rastreo de redes. En el acceso sin autorización a la red de sensores se pueden modificar información, pues, suplantan la identidad con el fin de obtener los datos y utilizar a su convenio, lo cual afecta en la funcionalidad de la red.

3.4.3.4 Mantenimiento de la evaluación del riesgo

Una vez identificada las vulnerabilidades, se establece mantenimiento a través del control adecuado, por lo que se toma en cuenta el estándar ISO/IEC 27002 (2022). Es decir, a las medidas que se determinen se establecen controles con la finalidad de verificar el cumplimiento de las mismas.

Para ello se considera los controles físicos (sensores inalámbricos), propiedad de seguridad de información (confiabilidad, integridad, etc.), personas (personal) y tecnología (red). Los controles se describen a continuación:

Tabla 21.

Matriz control del riesgo

Tipo de control	Información	Seguridad	Capacidad operacional	Dominio de seguridad	Frecuencia
Preventivo	Físicos, seguridad de información, personal y tecnología	Revisión de la información y planificar medidas de protección Mantenimiento cuando se presenta el problema para su protección Mantenimiento de recursos (información)	Gestión de identidad Gestión de acceso	Reglamento y políticas	Trimestral Semestral Anual
Detectivo					
Correctivo					

Nota. La tabla presenta el mantenimiento a través de controles.

3.4.4 Fase 3: Definición de objetivos secundarios

En la tercera fase se define los objetivos específicos del proyecto y los secundarios enfocados a la identificación de vulnerabilidades según la metodología.

Objetivos específicos

- Determinar la herramienta adecuada para el desarrollo del ataque.
- Establecer a la persona responsable del proceso de implementación del ataque.
- Planificar actividades para la gestión de desarrollo de ataques.

3.4.4.1 Objetivos secundarios

Los objetivos secundarios para identificar las vulnerabilidades en la red de sensores se detallan a continuación:

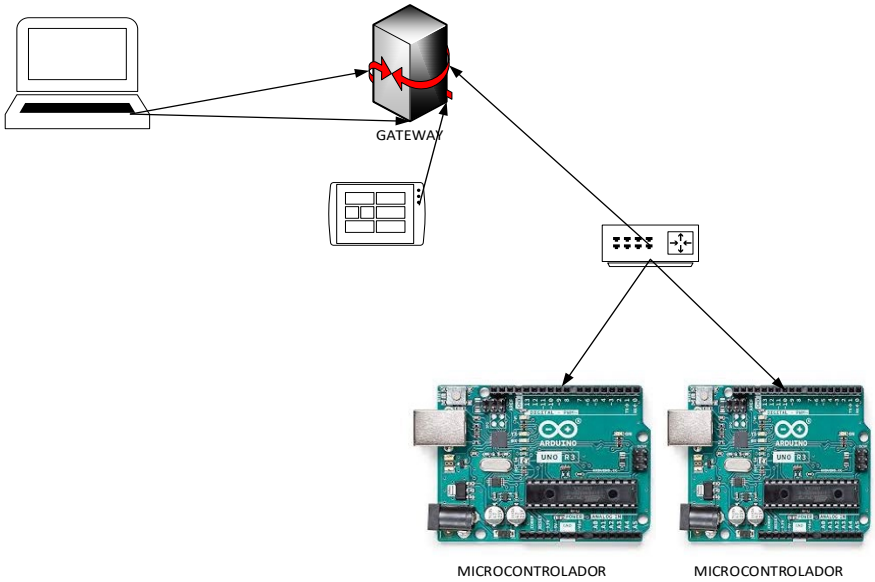
- Aplicar los ataques establecidos en la planificación.
- Realizar comparativa para escoger la técnica intrusiva adecuada para identificar vulnerabilidades según ataques planificados, considerando la metodología OWASP.
- Elaborar el informe final de las vulnerabilidades encontradas y ataques con sus respectivas soluciones.

3.5 Fase 4: Ataques

En primera instancia se diseña la red con sus respectivos nodos, representando en una arquitectura de hardware y un software embebido similares. La cual se aprecia en la Figura 14, donde se tiene el despliegue de la red inalámbrica con diferentes nodos. Al momento que los nodos terminan su operación, pasan a un modo de reposo para reducir el consumo de energía y aumentar la duración de la batería. Todos los nodos simulados integran un microcontrolador, una memoria y un transceptor. Los nodos (Gateway y sensor) se ejecutan y la frecuencia de adquisición de datos es cada 30 segundos.

Figura 14.

Arquitectura modelo de red

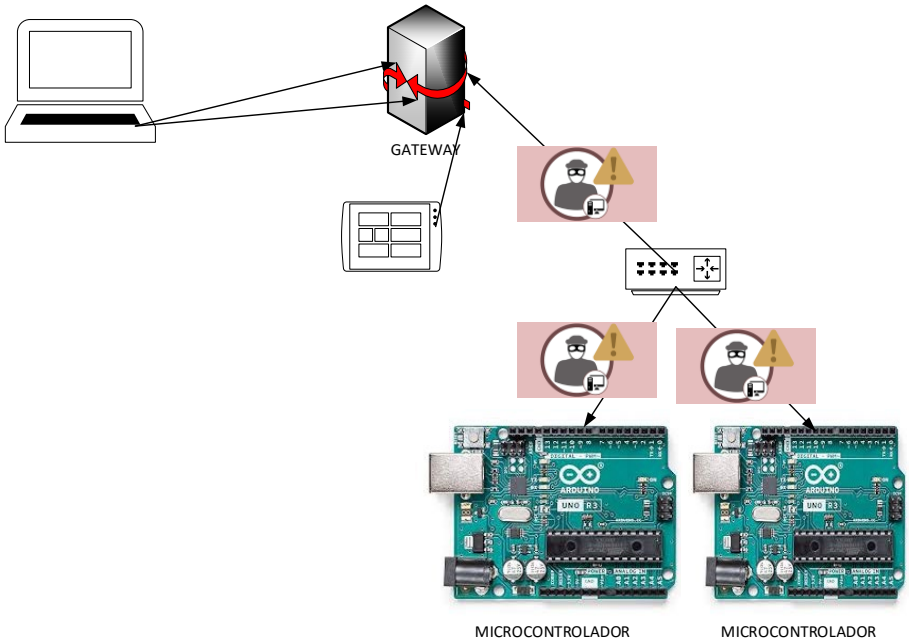


Nota. Esta figura es la arquitectura de la red con sus nodos.

De igual modo, se presenta la topología de la red de sensores inalámbricos atacada, esto se muestra en la Figura 15.

Figura 15.

Topología de red para evaluación



Nota. Esta figura es la topología de red.

Los nodos presentan una arquitectura diferente, donde se inyectan los ataques y los componentes están interconectados por un sistema de bus. La aplicación o sistema diseñado en conjunto con firmware solicita información a los dispositivos cada tres segundos. Estos se coordinan, una vez recibida la petición proceden a leer los sensores, cifrar, enviar información y reposan por tres segundos.

A continuación, se describe el proceso utilizado para diseñar firmware:

- Inyectar o insertar ataques en el simulador para identificar vulnerabilidades.
- El análisis de los ataques identifica el más peligroso.
- Para detectar el ataque, se puede definir una tasa máxima de paquetes recibidos.
- Si el ataque introduce una tasa superior, se detectará y se ejecutará la contramedida.
- Una vez detectado el ataque se puede aplicar una contramedida.

Por lo tanto, una vez identificada las vulnerabilidades presentadas en la red de sensor inalámbrica se procede a la explotación, es así que se efectuó pruebas según las vulnerabilidades. Cabe mencionar que para los ataques se estableció la técnica intrusiva de inyección y en ambos escenarios se aplicó los tres ataques planificados (confidencialidad, integridad y disponibilidad).

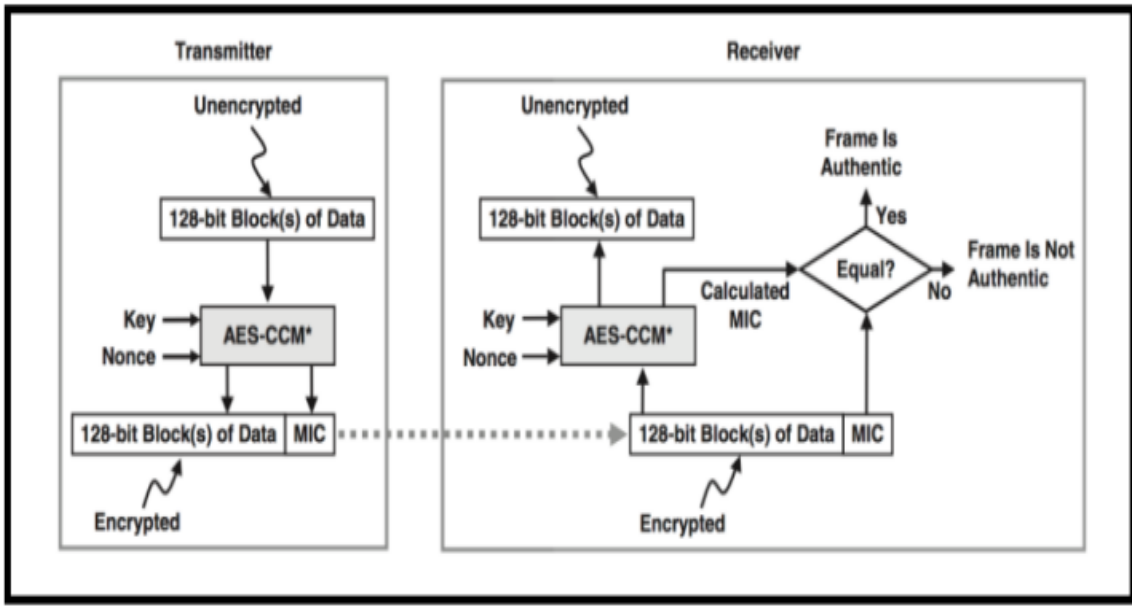
3.5.1 Ataque de confidencialidad

ZigBee logra la confidencialidad, la autenticación y la integridad de los datos a través de la suite de seguridad AESCCM*, que utiliza longitudes de clave de 128 bits. En una red ZigBee, los marcos se cifran opcionalmente en las capas NWK y APL. Los dispositivos ZigBee usan claves simétricas para cifrar tramas a través de pasos de seguridad usando AES-CCM* en las capas NWK y APS. El dispositivo en el extremo receptor aplica AES-CCM y la clave simétrica compartida de 128 bits para descifrar y autenticar las tramas (Yang, 2009).

La Figura 16 muestra el funcionamiento de AES-CCM para proporcionar confidencialidad y autenticación de datos:

Figura 16.

Funcionamiento AES-CCM

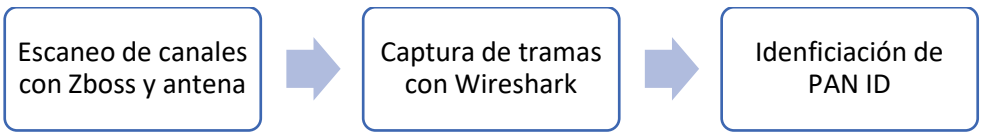


Nota. Esta figura representa el funcionamiento de AESCCM.

El ataque de confidencialidad consiste en robar información personal, desde la identificación del individuo hasta la obtención de los datos más específicos, para lograr este ataque, la antena colocada en la laptop permitió a través de Zboss capturar las tramas en un formato pcap y después a través de Wireshark identificar el PANID de los nodos 1 y 2. En la siguiente
Figura **17** se presenta la secuencia para el ataque:

Figura 17.

Diagrama de secuencia para ataque de confidencialidad



Nota. Esta figura representa el proceso de ataque.

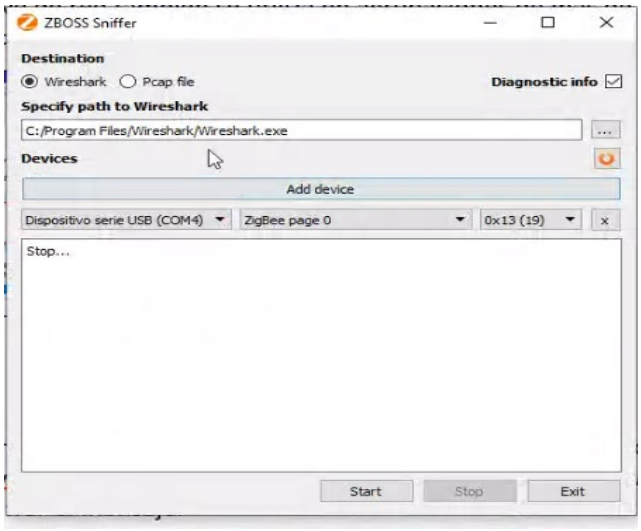
En otras palabras, la secuencia de ataque de confidencialidad inició con el escaneo de los canales de la capa de la red, para lo cual se utilizó la

herramienta Zboss, este se conecta a la antena y se obtiene los canales. Una vez identificado los canales, se aplicó la herramienta Wireshark para capturar las tramas; por lo que en la computadora se ingresó a la aplicación Wireshark, donde se visualiza las redes existentes e interfaces y se identifica la red que se encuentra en uso. En la red identificada se presiona doble click para capturas el tráfico que están entrando y saliendo. Por último, efectúa la identificación de PAN ID de la red, lo cual sirve para realizar los demás ataques.

Los siguientes experimentos son ataques de confidencialidad (rastreo de redes) contra redes ZigBee 3.0. Estos ataques implican la captura activa de tráfico en la red de la víctima, canal operativo y usando las claves simétricas comprometidas para descifrar redes sensibles información (Figura 18).

Figura 18.

Ataque de confidencialidad

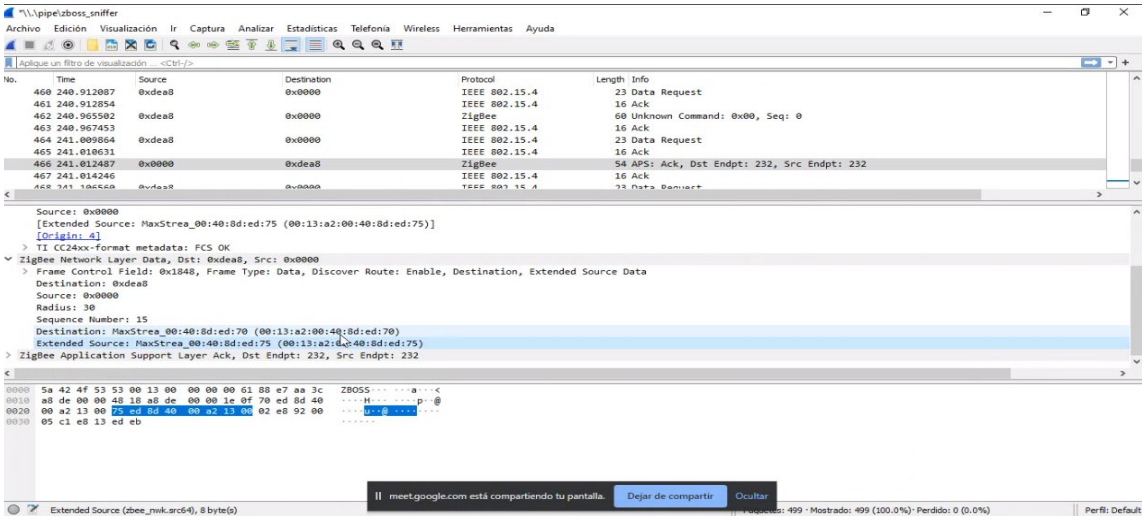


Nota. Esta figura representa el ataque de escucha en la red de sensores inalámbricos.

En la imagen se muestra la interfaz de ZBOSS, donde, se selecciona el puerto serial al que se conecte la antena y decodificador zigbee, así como el canal que se quiere escuchar. Se realiza varias pruebas hasta identificar el canal de comunicación de la red inalámbrica. Una vez identificada el canal se procede a capturar los paquetes. Se utiliza la herramienta Wireshark para una mejor visualización de las tramas capturadas.

Figura 19.

Captura de paquetes (tramas)



Nota. Esta figura representa el ataque de escucha en la red de sensores inalámbricos.

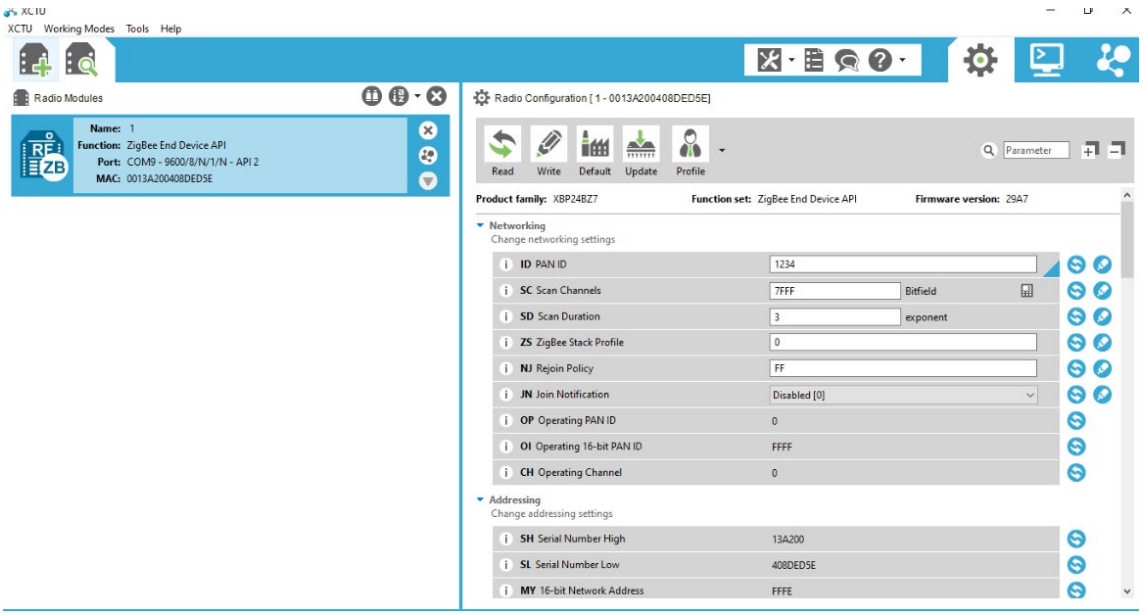
Se puede observar las tramas de coordinador como de clientes (Figura 19). Se analiza las tramas para la extracción de información. Si la configuración de la red Zigbee no se encuentra protegida por cifrado se puede observar directamente los datos de las distintas tramas. Se identifica la dirección del coordinador, los datos enviados, el PAN ID y datos que sirven para realizar otros ataques. Cabe señalar que, PAN ID es un identificador de una red de área personal, donde cada red es definido por PAN único y sirve para establecer comunicación entre los nodos, es así que, un valor es seleccionado aleatoriamente por el coordinador al momento que comienza el funcionamiento. Por lo tanto, un nodo no tiene la capacidad de enviar o receptar datos mientras no se vincule a una PAN (Intriago Velásquez & Cevallos Ulloa, 2015).

3.5.2 Ataque de integridad

Con los datos capturados anteriormente mediante configuración de módulos Zigbee se puede copiar la configuración de un esclavo para realizar envíos de datos manipulados a la red.

Figura 20.

Ataque de integridad

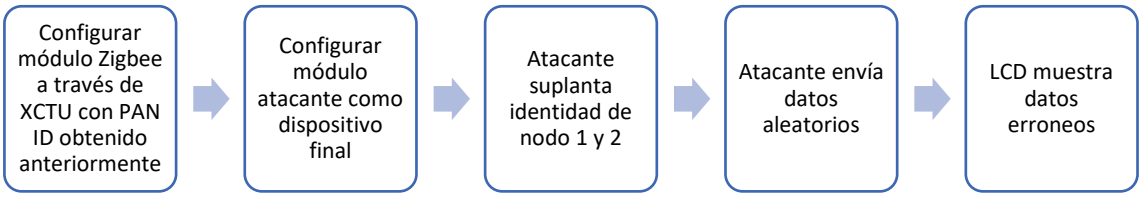


Nota. Esta figura representa el ataque de suplantación de identidad.

A través del programa XCTU se realiza la configuración del esclavo atacante enviando sus propios datos a la red. ZigBee proporciona integridad de mensajes para evitar que un atacante modifique un paquete en tránsito. Este paso se logra a través del MIC o Message Authentication Code. El MIC o código de autenticación de mensajes es incrustado en un marco antes de enviarlo para garantizar la integridad del encabezado MAC y la carga útil datos (Farahani, 2008). En el presente trabajo de titulación se realizó un ataque de integridad en el cual se modificó de manera intencional los datos, sin autorización. Se creó un nodo atacante el cual sustrajo el PAN ID de los nodos de la red y de esta manera enviar datos aleatorios al nodo máster. En la siguiente Figura 21 se presenta la secuencia para el ataque:

Figura 21.

Diagrama de secuencia para ataque de integridad

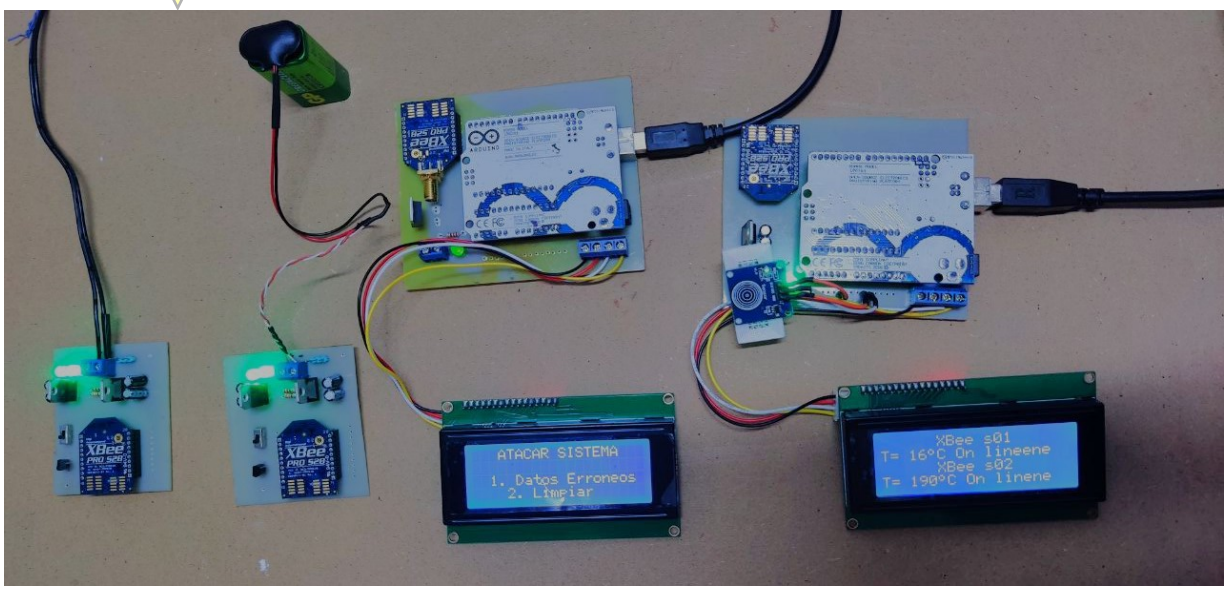


Nota. Esta figura representa el proceso de ataque.

Para el ataque de integridad se inicia con la configuración del módulo Zigbee, utilizando el programa XCTU para la configuración de los módulos que se muestra en la interfaz gráfica, es decir, se configuró el módulo atacante como un dispositivo final. Posteriormente, el atacante realiza la suplantación de identidad para el nodo 1 y 2, donde el atacante efectúa la modificación y envío aleatorio de los datos mostrados, considerando PAN ID obtenidos en el primer ataque (confidencialidad). Posteriormente, se lee el puerto digital y recibe datos aleatorios del Arduino atacante, enviando los datos a la red como nodo 1 y 2 aleatoriamente. En la pantalla LCD del nodo coordinador muestran información errónea, es decir, las temperaturas generadas aleatoriamente en lugar de los sensores pertenecientes a la red (Figura 22).

Figura 22.

Ataque de integridad



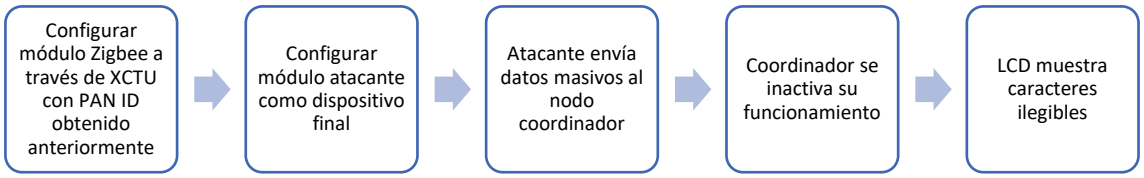
Nota. Esta figura representa el ataque de integridad.

3.5.3 Ataque de disponibilidad

ZigBee se implementa con un mecanismo de seguridad de agilidad de frecuencia que está diseñado para proteger la disponibilidad de la red en caso de un problema de interferencia, un ataque de interferencia o ataques específicos de denegación de servicio (DoS). Este proceso permite que la red ZigBee migre a un nuevo canal de frecuencia para abordar estos problemas (Sajjad & Yousaf, 2014). Como parte de la funcionalidad central del coordinador para establecer una red, realiza un escaneo de proximidad para detectar redes y dispositivos ZigBee existentes en su vecindad y para determinar su canal de frecuencia. El coordinador continúa dinámicamente este proceso después de que se haya establecido la red al monitorear constantemente las señales que podrían indicar una amenaza para la disponibilidad de la red. En el presente trabajo de titulación después del ataque de confidencialidad se procedió a enviar datos masivos al nodo máster y de esta manera se inactiva su funcionamiento y la pantalla muestra caracteres ilegibles. En la siguiente Figura 23 se presenta la secuencia para el ataque:

Figura 23.

Diagrama de secuencia para ataque de disponibilidad



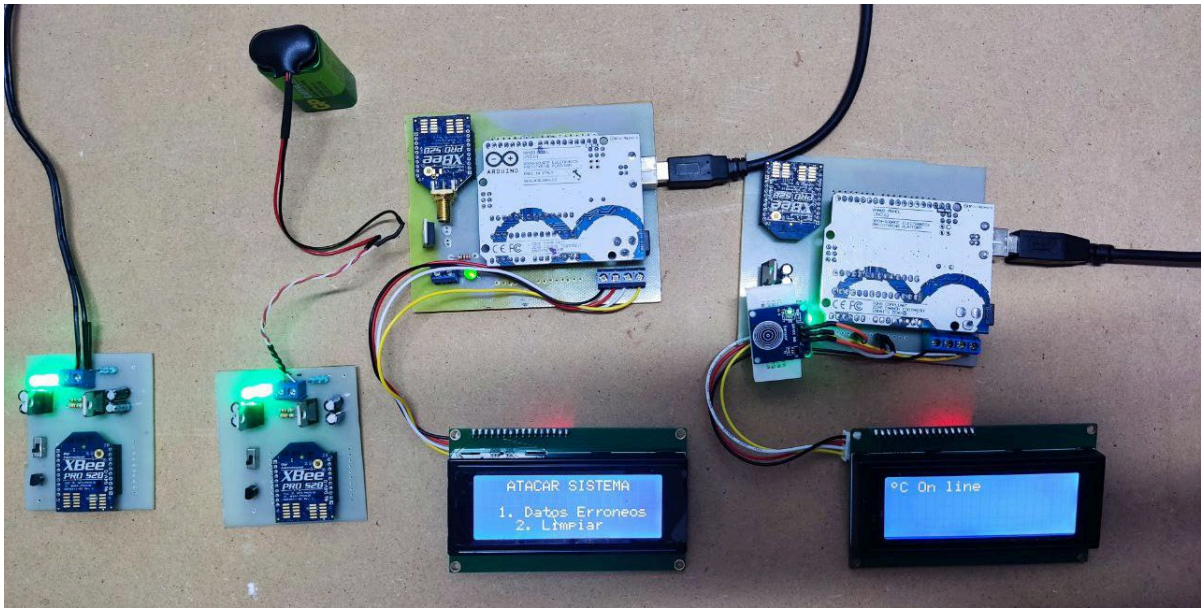
Nota. Esta figura representa el proceso de ataque.

Para el ataque de disponibilidad se basó en la técnica de denegación de servicio (DoS). De igual modo, se configuró el módulo Zigbee (atacante) como dispositivo final mediante el uso de la herramienta XCTU. Después, el atacante envía datos masivos al nodo coordinador de la red, en la cual se utiliza los datos de PAN ID obtenidos en el primer ataque. Luego el nodo coordinador se vuelve inactivo y no funciona, pues, se lee el puerto digital y recibe datos aleatorios del Arduino atacante, enviando los datos a la red como nodo 1 y 2 aleatoriamente.

Por último, en la pantalla LCD del nodo coordinador muestran caracteres ilegibles, es decir, se envía códigos generados con caracteres especiales que no muestra una pantalla LCD (Figura 24).

Figura 24.

Ataque de disponibilidad



Nota. Esta figura representa el ataque de disponibilidad.

CAPÍTULO 4. RESULTADOS Y PRUEBAS DE LA METODOLOGÍA

En el cuarto capítulo se continua con la aplicación de las demás fases de la metodología a través de Offensive Security para realizar la auditoría de seguridad a redes de sensores inalámbricas. Además, se complementa con la metodología OWSAP con la finalidad de realizar la comparativa de las pruebas o técnicas.

4.1 Fase 5: Análisis de resultados

En la quinta fase se presenta el análisis de los resultados, donde se muestra los hallazgos de las vulnerabilidades encontradas en cada escenario, determina el método comparativo, métrica, entre otros.

4.1.1 Presentación de hallazgos

A continuación, se presentan las vulnerabilidades encontradas en cada escenario:

Tabla 22.

Presentación de hallazgos (vulnerabilidad)

Escenario	Hallazgo
Escenario 1: Red de sensores inalámbricos que miden la temperatura.	• Lectura de datos de la temperatura • Envío de datos manipulados, es decir, presenta información errónea del nivel de temperatura, esto afecta a la calidad de los cultivos, pues, no se realiza el riego adecuado. • Denegación del servicio, pues, no se aprecia ninguna información de la temperatura. • Captura de tráfico, pues, no se puede identificar el pico de carga de la temperatura en intervalos regulares. • Captura de paquetes inusual en la red.

Escenario 2: Red de sensores que mide temperatura y CO2.	• Rastreo de redes • Descifra información sensible del nivel de temperatura y CO2 que únicamente deben conocer las entidades responsables. • Captura activa de tráfico • Captura de paquetes • Lectura de datos sin autorización del nivel de temperatura en el tráfico y CO2 en la combustión interna. • Envío de datos manipulados sobre el nivel de CO2. • Modificación aleatoria de datos mostrados del nivel de temperatura. • Denegación del servicio, es así que no se puede obtener información del nivel de temperatura ni CO2.

Nota. La tabla presenta la comparativa de las vulnerabilidades identificadas en cada escenario.

En la Tabla 22 se identifica que, se mostró mayor cantidad de vulnerabilidades en la red de sensores inalámbricos del escenario 2. Por lo tanto, al utilizar las herramientas tecnológicas permitió conocer la presencia de más de tres vulnerabilidades que a diferencia del primer escenario, es así que se podrá aplicar mecanismos de protección contra las mismas.

Posteriormente, se realizó ataques de confidencialidad, integridad y disponibilidad para cada escenario, especialmente en el nodo esclavo 1 – 2 y maestro, donde se utilizó PAN ID, configuración tanto el nodo como la red de sensor (dispositivo). En el primer escenario se identificó las temperaturas aleatorias por manipulación de los datos, denegación del servicio, captura de tráfico y paquetes. Para el segundo escenario se aplicó los mismos ataques, en la que se conoció vulnerabilidades como el rastreo de redes, descifra información sensible del nivel de temperatura y CO2, captura activa de tráfico – datos, lectura de datos sin autorización, envío de datos manipulados, modificación aleatoria de datos y DoS.

4.1.2 Determinación de método comparativo

El método de cálculo CVSS (*Common Vulnerability Score System*) corresponde a un cálculo cuantitativo que permite transformar fórmulas sencillas en un índice de gravedad para cada vulnerabilidad identificada; así, a través de la observación de métricas estándares es posible realizar de forma objetiva una evaluación comparativa de las vulnerabilidades (Gencer & Başçiftçi, 2021).

Se utilizó el método comparativo de CVSS (*Common Vulnerability Score System*) que facilitó la contrastación de las pruebas intrusivas. Por lo tanto, se permitió captar las características principales y estimar puntuaciones para las métricas seleccionadas. Al final se califica la métrica por cada prueba intrusiva y se selecciona la que tiene mayor puntuación según escala (Ver Tabla 16).

4.1.3 Determinación de la métrica

Bajo el método CVSS se tiene el siguiente grupo de métricas utilizadas para comparar las pruebas intrusivas (Celis & Arévalo, 2018):

1. **Métrica Base:** Se trata de características que se encuentran de forma específica y en el entorno del usuario, es decir, constantes.

Explotabilidad: Se refiere a la facilidad y los mecanismos técnicos para la explotación.

- Vector de Acceso a red de sensores
- Complejidad de Acceso a red de sensores
- Autenticación

Impacto: Se trata de una consecuencia directa de un dispositivo sufre un impacto.

- Confidencialidad
- Integridad
- Disponibilidad

- Impacto en Reconocimiento de Puertos

2. **Métricas Temporales:** Representa las características de la vulnerabilidad que se modifican en el transcurso del tiempo.
   - Explotabilidad
   - Confiabilidad
   - Fiabilidad del Informe de vulnerabilidad y facilidad de solución

4.1.4 Comparación de pruebas intrusivas

A continuación, se describe los pro y contras de las pruebas intrusivas:

Tabla 23.

Comparativa de pruebas intrusivas

Pruebas	Ventajas	Desventajas
Sniffing	• Posibilidad de controlar el tráfico. • No necesita de conocimientos sofisticados para aplicarse. • Permite la verificación del comportamiento del usuario. • Ayuda en la verificación de falencias y las fortalezas de los equipos analizados. • Posibilidad de efectuar cambios en la seguridad. • Captura contraseñas y nombres de usuario. • Permite la identificación de los servicios más utilizados • Se aprecia el uso inadecuado del recurso.	• Requieren conocimiento previo.
Suplantación de identidad (Phishing)	• No necesita de conocimientos sofisticados para aplicarse. • Permite identificar los mensajes, correos no deseados o información confidencial. • Ayuda a identificar • Se puede filtrar de mensajes seguros.	• No se encuentran vulnerabilidades técnicas.
Modificación de datos	• Menor costo en la implementación de la prueba. • Presenta información sencilla y práctica de las vulnerabilidades. • Posibilidad de identificar información cambiada y establecer medidas	• Se puede crear cuellos de botella. •

Denegación de servicio (DoS)	• Técnica sencilla de aplicar. • Permite verificar la capacidad del tráfico de datos. • Ayuda a identificar la alteración de los paquetes. • Posibilidad de enviar códigos generados con caracteres especiales.	• Necesita conocimientos previos.

Nota. La tabla presenta la comparativa de las pruebas intrusivas

4.1.5 Análisis de seguridad de trabajos existentes

En la siguiente tabla se muestra la comparativa de tipos de seguridad y vulnerabilidad de tesis o trabajos relacionados con redes de sensores inalámbricos realizados por parte de la Academia UTN:

Tabla 24.

Análisis de seguridad de trabajos existentes

Trabajos	Tipo de seguridad	Vulnerabilidades
Diseño de un radio enlace inalámbrico de alta disponibilidad para el transporte de información recolectada a través de una WSN (red de sensores inalámbricos) de un sistema de alerta temprana de incendios forestales (Pule Méndez, 2017).	Protección de datos Encriptación Control de tráfico	Captura activa de tráfico
Diseño de una red de sensores inalámbricos LPWAN para el monitoreo de cultivos y materia orgánica en la granja experimental La Pradera de la Universidad Técnica del Norte (Domínguez, 2020).	Claves de seguridad del nodo Protección de datos Contraseña	Manipulación de sensores Modificación aleatoria de datos
Sistema de monitoreo de monóxido de carbono mediante una red de sensores inalámbricos y una	Claves, contraseñas para el transporte,	Descifra información sensible

plataforma como servicio en la nube para una residencia (Carrión & Maya, 2016).	protección del marco y la gestión de WSN.	
Red WSN para el control y monitoreo de un sistema de riego por goteo de una plantación de fresas en la granja experimental Yuyucocha – UTN (Burbano García, 2014).	Protección de datos	Manipulación de sensores Denegación del servicio
IPV6 en una red WSN para el monitoreo remoto de cultivos en la Granja La Pradera de la Universidad Técnica del Norte (Tambaco Suarez, 2015).	Encriptación Autenticación usuario	Modificación en los datos receptados por los nodos sensores.
Diseño e implementación de una red de sensores inalámbricos definidos por software para el monitoreo de un sistema hidropónico NFT (Bautista & Maya, 2022).	Autenticación Cifrado de paquete de datos	Captura de tráfico de datos
Red de sensores inalámbricos bajo protocolo lora y gestión de procesos para la analítica de datos mediante meta sistema operativo para monitoreo ambiental en invernaderos (Gordillo, 2021).	Autenticación de nodos Autenticación de usuario	Redundancia de datos Acceso no autorizado a datos Lectura de datos
Diseño de una red inalámbrica para una WSN de un sistema de alerta temprana de incendios para el bosque protector Guayabillas. (Enríquez Burgos, 2018)	Autenticación de usuario	Modificación de datos Manipulación de los nodos

Nota. La tabla presenta la comparativa de trabajos de redes de sensores inalámbricos.

Como se observa en la Tabla 24 las vulnerabilidades que se observan en los trabajos recientemente implementados con redes de sensores son numerosas, y algunas revisten una importante vulnerabilidad en seguridad. Desde la manipulación de los sensores hasta la modificación y lectura de datos, estos sistemas requieren de un mecanismo de auditoría que permita estandarizar procesos de evaluación que sean efectivos para la prevención.

4.1.6 Comparativa

Por otro lado, se realizó la comparativa de los mecanismos empleados para realizar los ataques en la red de sensor inalámbrica. Para lo cual se consideró cuatro técnicas intrusivas, por lo que se adaptó las métricas base del modelo o metodología CVSS. Al final se selecciona la técnica que tiene mayor puntuación. Los resultados se detallan a continuación:

Tabla 25.

Comparativa

Parámetro	P	Suplantación de identidad		DoS		Sniffing		Modificación de datos	
		C	T	C	T	C	T	C	T
Vector de Acceso a red de sensores	0,10	4	0,40	6,9	0,69	10	1,00	6	0,60
Complejidad de Acceso a red de sensores	0,10	6,9	0,69	7	0,7	9	0,90	3,9	0,39
Autenticación	0,09	3,9	0,35	4	0,36	8,9	0,80	6	0,54
Confidencialidad	0,09	6	0,54	4	0,36	10	0,90	6	0,54
Integridad	0,09	10	0,90	6,9	0,621	7	0,63	10	0,90
Disponibilidad	0,09	6,9	0,62	10	0,9	9	0,81	6	0,54
Explotabilidad	0,09	7	0,63	8,9	0,801	10	0,90	7	0,63
Confiabilidad	0,09	3,9	0,35	3,9	0,351	7	0,63	6	0,54
Impacto en Reconocimiento de Puertos	0,10	6	0,60	6	0,6	8	0,80	6	0,60
Facilidad de Solución	0,08	6	0,48	6	0,48	7	0,56	7	0,56

Fiabilidad del Informe de Vulnerabilidad	0,08	6	0,48	9	0,72	9	0,72	9	0,72
Total	1,00		**6,04**		**6,58**		**8,65**		**6,56**

Nota. La tabla presenta la comparativa de los mecanismos aplicados.

La tabla anterior muestra los resultados, donde se identifica que en la red de sensores la mayor puntuación la técnica Sniffing, pues, obtuvo una puntuación de 8,65, incluyendo DoS con 6,58 puntos. Por ende, se determina que son las más adecuadas porque permiten identificar de las vulnerabilidades que más se presentan en la red de sensores.

4.2 Fase 6: Análisis final y documentación

En la última fase, se presenta el análisis final y documentación, detallando las evidencias y diseño de auditoría del proyecto.

4.2.1 Presentación de evidencias

En la siguiente tabla se presenta el resumen de las evidencias del proyecto desarrollado:

Tabla 26.

Resumen evidencias

Escenario	Ataque	Técnica de ataque	Herramientas utilizadas	Vulnerabilidad
Red de sensores inalámbricos que miden la temperatura.	Confidencialidad Integridad Disponibilidad	• Sniffing • Suplantación y modificación de datos • DoS	• ZBOSS Sniffer • Software WireShark • Software XCTU • Antena Zigbee	• Lectura de datos • Envío de datos manipulados • Denegación del servicio • Captura activa de tráfico • Captura de paquetes
Red de sensores que mide temperatura y CO2.	Confidencialidad Integridad Disponibilidad	• Sniffing • Suplantación y modificación de datos • DoS	• ZBOSS Sniffer • Software WireShark • Software XCTU • Antena Zigbee	• Rastreo de redes • Descifra información sensible • Captura activa de tráfico • Captura de paquetes • Lectura de datos sin autorización • Envío de datos manipulados • Modificación aleatoria de datos

	• Denegación del servicio, no se puede obtener datos del nivel de temperatura ni CO2.

Nota. La tabla presenta el resumen de las evidencias

4.2.2 Informe de auditoría

En el informe de auditoría consta de datos generales, metodología, hallazgos y recomendaciones.

En el Anexo 3 se indica los datos que deben estar presentes en el título de la auditoría.

4.2.2.1 Datos generales

- Objetivo de la auditoría

Identificar las vulnerabilidades en la seguridad de redes de sensores inalámbricos mediante técnicas intrusivas.

- Alcance de la auditoría

El alcance es realizar una auditoría sobre la red de sensores inalámbricos, considerando las vulnerabilidades e implementación de ataques, así como la comparativa de las técnicas intrusivas; donde se consideró los siguientes aspectos:

- Datos / Software: Aplicación metodología de auditoría, identificación de vulnerabilidades, sensores inalámbricos, herramienta ZBOSS Sniffer, WireShark y Zigbee-emulador CC, depurador y programador USB.
- Ataques: confidencialidad, integridad y disponibilidad.
- Técnicas intrusivas: Suplantación de identidad, DoS, Sniffing y modificación de datos.

4.2.2.2 Metodología

En la metodología se considera el método, aspectos evaluados, proceso y manejo. Se elaboró a este respecto una guía de usuario para aplicar este

método de auditoría, la que consta en el anexo 2, además de un formato de informe de auditoría, que consta en el anexo 3.

- Método

Se utilizó el método basado en la visualización del panorama y verificación de los documentos. En el primer caso, se revisó el funcionamiento de los equipos como la red de sensores inalámbricos, ZBOSS Sniffer, WireShark y Zigbee-emulador CC, depurador, programador USB y WireShark. Esto con la finalidad de aplicar los tres ataques en los dos escenarios. Mientras que en la verificación de los documentos se tomó en cuenta las fuentes secundarias (libros, revistas, entre otros) para la identificación de la situación de la seguridad en la red de sensores inalámbricos. Las técnicas utilizadas fueron la observación y la digitalización de imágenes de los resultados obtenidos.

- Aspectos evaluados

El cuanto a los aspectos evaluados se consideró la identificación de las vulnerabilidades, evaluación del riesgo según NIST SP 800-30, implementación de ataques (confidencialidad, integridad y disponibilidad) en dos escenarios. Además, de la comparativa de las pruebas intrusivas según las métricas del método CVSS (*Common Vulnerability Score System*).

- Proceso

El proceso para el desarrollo inició desde la recolección de la información, análisis de vulnerabilidades, objetivos, implementación de ataques, análisis de resultados y presentación del informe de auditoría. En este último aspecto, se presentó los datos generales, metodología, hallazgos y recomendaciones.

- Manejo

Respecto al manejo se establece los mecanismos o recomendaciones para mitigar o hacer frente los posibles ataques y vulnerabilidades que se presentan en la red de sensores inalámbricos.

4.2.2.3 Hallazgos

El principal problema encontrado en la red de sensor inalámbrica está relacionado con la facilidad de acceso a los datos para hacer uso indebido, es así que se aprecia una red sensible de la información, pues, se tiene cifrado inadecuado.

Es así que, el primer ataque de confidencialidad muestra mayor vulnerabilidad, incluso no se puede detectar si el sistema está siendo atacado, pues, es un ataque sigiloso. Además, sin realizar ese ataque no se puede obtener el PAN ID, datos que sirven para realizar otros ataques, es decir no sería posible efectuarlos. Por lo tanto, en la implementación de ataques se identificó que el acceso a la red de sensores puede ser fácil si no se cuenta con soluciones o mecanismos. Es así que es necesario que se aplique medidas para evitar o hacer frente a los ataques que sufren la red de sensores inalámbricas.

En los hallazgos obtenidos de los ataques implementados en la red de sensores se clasifican en aspectos positivos y negativos, tal como se detalla de la siguiente manera:

Tabla 27.

Aspectos positivos y negativos

Aspectos	Descripción
Negativos	• Fallas en la seguridad debido a que se hay facilidad de rastreo, descifrado y captura de datos. • El ataque escucha es sigilo y muchas veces no se detecta a tiempo. • Limitaciones en el cifrado de la red.
Positivos	• Estabilidad en la red debido a que no se presentó mucha variabilidad en la conexión.

Nota. La tabla presenta las ventajas y desventajas de los resultados obtenidos

Una vez identificada las vulnerabilidades y los ataques a los que están expuestos la red de sensores inalámbricos se sugiere revisar el cableado y acceso inalámbricos de la red, aplicando mecanismos de autenticación que únicamente el usuario pueda acceder. En caso de utilizar la red de sensores inalámbricos en alguna organización se debería determinar políticas de seguridad.

4.2.2.4 Recomendaciones

Una vez identificada las vulnerabilidades y ejecutado los ataques planificados se presenta recomendaciones para establecer medidas o soluciones a las mismas, estos se consideran el criterio de diferentes autores para la sustentación técnica. Para la implementación de las medidas dependen del nivel de riesgo de las vulnerabilidades por cada ataque.

Tabla 28.

Resultados de ataques identificados y medidas

Vulnerabilidades	Ataques	Medidas
Rastreo de redes Descifra información sensible Captura activa de tráfico Captura de paquetes Lectura de datos	Ataques de confidencialidad	Aplicar claves de cifrado con los nodos vecinos. Aplicar protocolo SCADD para detección y defensa, realizar cifrado de la red. Monitorizar cambios en el cubrimiento de la red. Protocolo de inferencia del cubrimiento básico. Cifrar datos esenciales.
Envío de datos manipulados		Utilizar protocolo enrutamiento y autenticación. Contar con autenticación de paquetes entrantes.

		Utilizar estándares.
		Realizar monitoreo constante de la red.
		Utilizar programas sniffers.
		Aplicar segmentación.
		Realizar control de acceso físico.
	Ataque de integridad	Utilizar tecnologías de seguridad.
		Respaldo frecuente de los datos.
		Autenticación segura.
		Adoptar el estándar 802.1x, TKIP (Protocolo de integridad de clave temporal).
Modificación aleatoria de datos mostrados		Uso sistema de detección y prevención de intrusión.
		Mantener software actualizado.
		Gestionar usuarios y cuentas privilegiadas.
		Analizar contenido de paquete de la red para detección de protocolos de la capa aplicación.
	Ataque de disponibilidad	Aplicar plan de recuperación (copia de seguridad periódica).
Denegación del servicio		Interceptar tráfico entrante.
		Supervisar las conexiones de red recién creadas enviadas o recibidas por hosts que no son de confianza.

Nota. Elaboración propia con base en resultados y normas (MITRE Corporation, 2022), (NIST, 2002), (OWASP Fundation, 2017)

Como se observa, las medidas planteadas se encuentran en línea con las vulnerabilidades identificadas; además, están basadas en los lineamientos que indican las normas MITRE, NIST y OWASP.

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se realizó la fundamentación teórica de las metodologías de auditorías, en la cual se consideró el IEEE 802.15.4. Entre estas se encuentran OSSTM, OWSAP, Offensive Security y ISSAF, para el estudio se tomó en cuenta la metodología Offensive Security. Además de complementó con la información de la seguridad, redes de sensores inalámbricas y herramientas de auditoría.
- Las fases de la ejecución de auditoría de seguridad inician con la recolección de la información, análisis de vulnerabilidades, definición de objetivos secundarios, ataques, análisis de resultados y final (resultados finales). Para el análisis de la vulnerabilidad se aplicó una metodología para análisis de riesgos NIST SP 800-30 de los cuatro ataques establecidos.
- Se utilizaron las pruebas intrusivas sniffing, phishing, DoS y modificación de datos y los resultados fueron comparados mediante el método CVSS, el cual las compara con base en diversos criterios. Se obtuvo que la prueba de sniffing tuvo un mejor desempeño respecto de las otras técnicas utilizadas, pues presentó un mejor puntaje global, con mejores resultados en vector de acceso a la red de sensores, complejidad de acceso a la red, autenticación, confidencialidad, disponibilidad, explotabilidad, confiabilidad e impacto en reconocimiento de puertos. Las pruebas restantes tuvieron similares resultados entre ellas, siendo la de mejor desempeño DoS después de sniffing.
- En la definición de los escenarios planteados se utilizaron las herramientas Wireshark, Zboss Sniffer y Zigbee para identificar las vulnerabilidades de la red, entre las que constan el rastreo de redes, el descifrado de información sensible, captura activa de tráficos, captura de paquetes, etcétera. El primer ataque de confidencialidad realizado evidenció una mayor vulnerabilidad debido a que no fue detectado, y sin él no sería posible obtener el PAN ID. A partir de las vulnerabilidades

detectadas se establecieron medidas correctivas y soluciones para mitigar las vulnerabilidades correspondientes a cada ataque realizado.

- La metodología propuesta de auditoría de seguridad para redes de sensores inalámbricas se compone de seis fases secuenciales que tienen por objetivo estandarizar los procedimientos para la detección de las vulnerabilidades en las redes. Esta metodología propuesta contiene diversos métodos y técnicas sugeridos, pero puede ser adaptada a otras herramientas o, bien, puede ser utilizada para diversos tipos de ataques en función de los objetivos y el alcance que se tengan.

5.2 Recomendaciones

- Se sugiere complementar la fundamentación teórica con aspectos relacionados con hacking ético debido a que se sustenta y valida la planificación de ataques, considerando el estándar IEEE 802.15.4.
- Se recomienda emplear todas las fases de la metodología seleccionada con la finalidad de identificar las vulnerabilidades de manera oportuna, lo que permitirá establecer medidas de seguridad, considerando los métodos o mecanismos que complementa a Offensive Security como CVSS y NIST SP 800-30.
- La metodología de auditoría propuesta puede ser adaptada para distintos escenarios y para distintos tipos de ataque a realizar. Por ello, se recomienda estudiar la metodología propuesta y utilizar las herramientas en ella sugeridas para detectar vulnerabilidades en redes de sensores de diversos tipos. Además, se sugiere testear las redes con varios tipos de ataques.
- Tomar en cuenta las técnicas empleadas para el análisis a futuro con el propósito de identificar las vulnerabilidades en la red de sensores, es decir, se puede ampliar con nuevos ataques y complementar con otras técnicas.
- Utilizar las herramientas de WireShark y ZBOSS Sniffer para futuros análisis para la red, así como el programa XCTU, es decir, de manera continua, esto permite contar con una evaluación más precisa de las vulnerabilidades. Además, es importante tomar en cuenta las medidas de

seguridad establecidas según las vulnerabilidades identificadas y tipos de ataques.

- Para futuras investigaciones, se sugiere modificar los escenarios aquí establecidos de modo de obtener distintas perspectivas desde donde mejorar la seguridad de las redes de sensores inalámbricos. Es pertinente, por tanto, implementar esta auditoría en futuros trabajos que propongan modelos de redes de sensores inalámbricas, testeando y mejorando con ello la seguridad que estas prestan.
- Se sugiere investigar sobre otros métodos y herramientas disponibles para la realización de ataques tanto intrusivos como no intrusivos, de manera de aumentar el número de herramientas disponibles para llevar a cabo la auditoría.

Bibliografía

25+ Impressive Big Data Statistics for 2023. (2023). Petrov, C. https://techjury.net/blog/big-data-statistics/#gref

Abu Daia, A. S., Ramadan, R. A., & Fayek, M. B. (2018). Sensor networks attacks classifications and mitigation. *Annals of Emerging Technologies in Computing*, *2*(4), 28–43. https://doi.org/10.33166/AETIC.2018.04.003

Acosta, C. E., Gil-Castiñeira, F., & Costa-Montenegro, E. (2021). Red inalámbrica de sensores con topología lineal sin capa de red. *Revista de Investigación En Tecnologías de La Información*, *9*(17 (Especial)), 56–65. https://doi.org/10.36825/RITI.09.17.006

AlEroud, A., & Karabatis, G. (2017). Using contextual information to identify cyber-attacks. *Studies in Computational Intelligence*, *691*, 1–16. https://doi.org/10.1007/978-3-319-44257-0_1

Allaica, J., & Guevara, D. (2020). *Auditoría de la seguridad informática siguiendo la metodología Open Source Security Testing Methodology Manual para la empresa Megaprofer S.A.* [Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial.]. https://repositorio.uta.edu.ec/jspui/handle/123456789/31313

Almeida, F., Bontempo, M. M., Santos, J. R. dos, & Alberti, A. M. (2019). Uma Proposta de Contramedida ao Ataque Jamming em Redes IEEE 802.15.4 utilizando Rádio Cognitivo. *Anais Do Workshop de Segurança Cibernética Em Dispositivos Conectados (WSCDC)*, 12–22. https://doi.org/10.5753/WSCDC.2019.7702

Alvarado-Zabala, J., Pacheco-Guzmán, J., & Martillo-Alchundia, I. (2018). El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT. *Contribuciones a Las Ciencias Sociales*, *noviembre*.

Arias Martínez, E., Caparrós, J., Directora, R., & Pous, H. R. (2021). *Securización de un entorno de telemetría IoT*. https://openaccess.uoc.edu/handle/10609/127129

Aza, A. (2019). *Auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, basada en la Norma ISO/IEC 27001 y la metodología OSSTMMV3*. http://repositorio.utn.edu.ec/handle/123456789/9028

Baca, G. (2016). *Introducción a la seguridad informática - Gabriel Baca Urbina - Google Libros*. Grupo Editorial Patria. https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=false

Batista, K. (2020a). *Diseño e implementación de un modelo individual para la simulación de la propagación de malware en redes de sensores inalámbricas*. https://gredos.usal.es/handle/10366/145241

Batista, K. (2020b). *Diseño e implementación de un modelo individual para la simulación de la propagación de malware en redes de sensores inalámbricas*. https://gredos.usal.es/handle/10366/145241

Bautista, J., & Maya, E. (2022). *Diseño e implementación de una red de sensores inalámbricos definidos por software para el monitoreo de un sistema hidropónico NFT*. http://repositorio.utn.edu.ec/handle/123456789/12195

BdSpeedytech. (2016). *CC Debugger ZIGBEE Bluetooth Emulator*. https://bdspeedytech.com/index.php?route=product/product&product_id=3627

Bracho, C. (2017a). *Auditoría de seguridad informática dirigida al gobierno autónomo descentralizado del cantón Mira basado en el estándar cobitv5, siguiendo la metodología osstmmv3*. http://repositorio.utn.edu.ec/handle/123456789/6878

Bracho, C. (2017b). *Auditoría de seguridad informática dirigida al gobierno autónomo descentralizado del cantón Mira basado en el estándar cobitv5, siguiendo la metodología osstmmv3*. http://repositorio.utn.edu.ec/handle/123456789/6878

Burbano García, J. L. (2014). *Red WSN para el control y monitoreo de una sistema de riego por goteo de una plantación de fresas en la granja experimental Yuyucocha – UTN.Red WSN para el control y monitoreo de una sistema de riego por goteo de una plantación de fresas en la granja experimental Yuyucocha – UTN.* http://repositorio.utn.edu.ec/handle/123456789/3526

Bustamante Sánchez, R. (2011). *Seguridad en redes*. https://repository.uaeh.edu.mx/bitstream/handle/123456789/10537

Campos, E. (2020). *Arquitectura IOT de bajo costo para redes de sensores*. https://repositorio.usm.cl/handle/11673/49644

Canales, M., & Bordachar, M. (2021). *Protección de datos personales en Ecuador: El momento es ahora | Derechos Digitales*. Derechos Digitales. https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

Carrión, E., & Maya, E. (2016). *Sistema de monitoreo de monóxido de carbono mediante una red de sensores inalámbricos y una plataforma como servicio en la nube para una residencia*. http://repositorio.utn.edu.ec/handle/123456789/7063

Carrizo-Díaz, C., & Vargas-Lombardo, M. (2017). Estándar, seguridad, vulnerabilidades y riesgos para la automatización del hogar. *Revista de Iniciación Científica*, *3*(1), 21–26. https://revistas.utp.ac.pa/index.php/ric/article/view/1694/html

Cedro, V., Sócrates, R., Muñoz Barragán, N., Felipe, A., Álvarez, T., Bestier, J., & Bejarano, P. (2018). Red de sensores inalámbricos para el monitoreo de variables microclimáticas en el Relicto Vegetal Cedro Rosado. *Scientia et Technica*, *23*(4), 501–510. https://doi.org/10.22517/23447214.16471

Celis, A., & Arévalo, L. (2018). *Diseño y planificación de un procedimiento de análisis, configuración y monitoreo de vacunas digitales para el sistema de prevención de instrusos ubicado en el Datacenter Santa Mónica ETB*. http://polux.unipiloto.edu.co:8080/00004474.pdf

Cevallos García, R. M., Melgar Jara, J. C., & Espol. (2016). *Diseño del despliegue de redes de sensores para el monitoreo de un centro comercial en la ciudad de Guayaquil*. http://www.dspace.espol.edu.ec/handle/123456789/37276

Cuadros, C. G., Veliz, V. F., Veloz, J. L., & Cruz, M. del R. (2022). Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicaciones. *Serie Científica de La Universidad de Las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 15, Nº. 1, 2022 (Ejemplar Dedicado a: Enero), Págs. 40-53*, *15*(1), 40–53. https://dialnet.unirioja.es/servlet/articulo?codigo=8590601&info=resumen&idioma=SPA

Cuzme Rodríguez, F. G. (2015). El Internet de las cosas y las consideraciones de seguridad. *Pontificia Universidad Católica Del Ecuador*. http://repositorio.puce.edu.ec:80/handle/22000/8492

CVSS. (2023a). *Common Vulnerability Scoring System SIG*. https://www.first.org/cvss/

CVSS. (2023b). *Common Vulnerability Scoring System SIG*. https://www.first.org/cvss/

Diaz, A., Sanchez, P., Bravo, I., Palomar, E., Gardel, A., & Lázaro, J. L. (2016). Simulation of Attacks for Security in Wireless Sensor Network. *Sensors 2016, Vol. 16, Page 1932*, *16*(11), 1932. https://doi.org/10.3390/S16111932

Domínguez, A. (2020). *Diseño de una red de sensores inalámbricos LPWAN para el monitoreo de cultivos y materia orgánica en la granja experimental La Pradera de la Universidad Técnica del Norte*. http://repositorio.utn.edu.ec/handle/123456789/10297

Egas, C., & Gil-Castiñeira, F. (2020). Revisión de requisitos, protocolos y desafíos en LWSN. *MASKAY*, *11*(1), 13–21. https://doi.org/10.24133/maskay.v11i1.1728

Enríquez Burgos, V. E. (2018). *Diseño de una red inalámbrica para una WSN de un sistema de alerta temprana de incendios para el bosque protector Guayabillas*. http://repositorio.utn.edu.ec/handle/123456789/8608

Escalante Uicab, F. J. (2019). Redes inalámbricas de sensores: aplicaciones, protocolos de enrutamiento y seguridad. In *Exploraciones, intercambios y relaciones entre el diseño y la tecnología*. Universidad de Quintana Roo. https://doi.org/10.16/CSS/JQUERY.DATATABLES.MIN.CSS

Farahani, S. (2008). ZigBee and IEEE 802.15.4 Protocol Layers. *ZigBee Wireless Networks and Transceivers*, 33–135. https://doi.org/10.1016/B978-0-7506-8393-7.00003-0

Fuertes, A. (2014). *Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad*. https://reunir.unir.net/handle/123456789/2331

Gélvez-Rodríguez, L. F., & Santos-Jaimes, L. M. (2020). Internet de las Cosas: una revisión sobre los retos de seguridad y sus contramedidas. *Revista Ingenio*, *17*(1), 56–64. https://doi.org/10.22463/2011642X.2370

Gencer, K., & Başçiftçi, F. (2021). The fuzzy common vulnerability scoring system (F-CVSS) based on a least squares approach with fuzzy logistic regression. *Egyptian Informatics Journal*, *22*(2), 145–153. https://doi.org/10.1016/J.EIJ.2020.07.001

GlobalSec. (2021). *Guía para gestionar pruebas de penetración (Ethical hacking) – GLOBALSEC PERÚ*. https://globalsecperu.com/guia-para-gestionar-pruebas-de-penetracion-ethical-hacking/

Gómez, A. (2017). Enciclopedia de la Seguridad Informática. 2ª edición - Álvaro Gómez Vieites - Google Libros. In *E*. RAMA. https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Gordillo, C. (2021). *Red de sensores inalámbricos bajo protocolo lora y gestión de procesos para la analítica de datos mediante meta sistema operativo para monitoreo ambiental en invernaderos*. http://repositorio.utn.edu.ec/handle/123456789/11887

Gordón, D., & Pacheco, R. (2018). Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior. *ReCIBE*. https://www.redalyc.org/articulo.oa?id=512255650001

Guato, K. (2018). *Análisis de las redes de sensores inalámbricos en la agricultura de precisión en el Ecuador*.

Guayas, B. (2018). *Auditoria de seguridad informática a la empresa BANAGINA S.A, ubicada en la provincia de El Oro, parroquia El Cambio.* http://repositorio.utmachala.edu.ec/handle/48000/12822

Gutiérrez-Portela, F., Almenares-Mendoza, F., Calderón-Benavides, L., & Romero-Riaño, E. (2021a). Prospectiva de seguridad de las redes de sensores inalámbricos. *Revista UIS Ingenierías*, *20*(3). https://doi.org/10.18273/REVUIN.V20N3-2021014

Gutiérrez-Portela, F., Almenares-Mendoza, F., Calderón-Benavides, L., & Romero-Riaño, E. (2021b). Prospectiva de seguridad de las redes de sensores inalámbricos. *Revista UIS Ingenierías*, *20*(3). https://doi.org/10.18273/REVUIN.V20N3-2021014

Ingeniería MCI Ltda. (2021). *¿Qué es XBee? XBee.cl - Comunicación Inalámbrica para Tus Proyectos*. https://xbee.cl/que-es-xbee/

Intriago Velásquez, G. A., & Cevallos Ulloa, H. I. (2015). *Diseño e implementación de un sistema domótico de radiofrecuencia para brindar*

gestión de networking, seguridad y confort usando los protocolos z-wave y zigbee. Espol. http://www.dspace.espol.edu.ec/handle/123456789/30126

Khanji, S., Iqbal, F., & Hung, P. (2019). ZigBee Security Vulnerabilities: Exploration and Evaluating. *2019 10th International Conference on Information and Communication Systems (ICICS)*, 52–57. https://doi.org/10.1109/IACS.2019.8809115

Kumar, M., Mohanraj, V., Suresh, Y., Senthilkumar, J., & Nagalalli, G. (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. *Journal of Ambient Intelligence and Humanized Computing*, *12*(5), 5287–5295. https://doi.org/10.1007/S12652-020-02007-W

Lascano Swoboda, J. L. (2017). *Diseño de un sistema prototipo para el control de robos vehiculares en la ciudad de Quito mediante tecnología con redes de sensores inalámbricos y un sistema de control central*. https://repositorioslatinoamericanos.uchile.cl/handle/2250/2793824

León Gudiño, M. W. (2017). *Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología Offensive Security Professional Training and Tools For Security Specialists y planteamiento de políticas de seguridad basadas en la norma ISO/IEC 27001*. http://repositorio.utn.edu.ec/handle/123456789/6975

López, A. (2021). *Qué ataques existen en las redes y cómo evitarlo protegiéndonos*. https://www.redeszone.net/tutoriales/seguridad/listado-completo-ataques-redes-como-evitarlos/

Lopez, J. E. G., Chavez, J. C., & Sanchez, A. K. J. (2017). Modelado de una red de sensores y actuadores inalámbrica para aplicaciones en agricultura de precisión. *2017 IEEE Mexican Humanitarian Technology Conference, MHTC 2017*, 109–116. https://doi.org/10.1109/MHTC.2017.7926210

Martínez, R. (2017). *Retos tecnológicos en la iot en el ámbito de las redes de sensores*. https://dialnet.unirioja.es/servlet/tesis?codigo=202921&info=resumen&idioma=SPA

Mbarek, B., & Meddeb, A. (2016). Energy efficient security protocols for wireless sensor networks : SPINS vs TinySec. *2016 International Symposium on*

Networks, Computers and Communications, ISNCC 2016. https://doi.org/10.1109/ISNCC.2016.7746117

Mejía, M. (2019). *Implementación de técnicas de seguridad informática para garantizar los principios de integridad, confidencialidad y disponibilidad de la información a un sistema de radiolocalización híbrido*. https://repository.upb.edu.co/handle/20.500.11912/4682

Mendoza, E., Fuentes, P., Benítez, I., Reina, D., & Núñez, J. (2020). Red de sensores inalámbricos multisalto para sistemas domóticos de bajo costo y área extendida. *Revista Iberoamericana de Automática e Informática Industrial*, *17*(4), 412–423. https://doi.org/10.4995/RIAI.2020.12301

MeteoSur. (2020). *Nuevo sistema de sensores inalámbricos hace posible el monitoreo en tiempo real para la agricultura por ambientes | MeteoSur*. https://www.meteosur.com/node/18

MITRE Corporation. (2022). *MITRE ATT&CK®*. https://attack.mitre.org/

Mohammadi, S., & Jadidoleslamy, H. (2011). A Comparison of Link Layer Attacks on Wireless Sensor Networks. *International Journal on Applications of Graph Theory In Wireless Ad Hoc Networks And Sensor Networks*, *3*(1), 35–56. https://doi.org/10.5121/jgraphhoc.2011.3103

Mordor Intelligence. (2023). *Pronóstico del mercado de la red de sensores inalámbricos (2022 - 27) | Tamaño de la industria, tendencias*. https://www.mordorintelligence.com/es/industry-reports/wireless-sensor-networks-market

Muñoz, A., & Mayorga, S. (2017). *Pentesting sobre aplicaciones web basado en la metodología OWASP utilizando SBC de bajo costo*. http://repositorio.unicauca.edu.co:8080/xmlui/handle/123456789/1773

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

NIST. (2002). *NIST SP 800-30 | NIST*. https://www.nist.gov/privacy-framework/nist-sp-800-30

Nordic. (2016). *Enhanced ShockBurst User Guide*. Nordic Semiconductor. https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.sdk5.v11.0.0%2Fesb_users_guide.html

Oreku, G. S., & Pazynyuk, T. (2015). Security in wireless sensor networks. *Security in Wireless Sensor Networks*, 1–87. https://doi.org/10.1007/978-3-319-21269-2

Otero Dans, A. (2021). *Herramienta de auditoría de seguridad en redes inalámbricas para pequeñas empresas*. https://ruc.udc.es/dspace/handle/2183/29830

OWASP Fundation. (2017). *Estándar de Verificación de Seguridad en Aplicaciones 3.0.1*.

Park, K. J., Zheng, R., & Liu, X. (2012). Cyber-physical systems: Milestones and research challenges. *Computer Communications*, *36*(1), 1–7. https://doi.org/10.1016/J.COMCOM.2012.09.006

Pomachagua, J. (2021). *Desarrollo de un sistema de auditoría de equipos de seguridad de redes*. Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/19072

Pule Méndez, D. C. (2017). *Diseño de un radio enlace inalámbrico de alta disponibilidad para el transporte de información recolectada a través de una WSN (red de sensores inalámbricos) de un sistema de alerta temprana de incendios forestales*. http://repositorio.utn.edu.ec/handle/123456789/6896

Ramírez Gómez, J., Fernando, H., Montoya, V., & León Henao, Á. (2019). Implementación del ataque Wormhole en redes de sensores inalámbricos con dispositivos XBee S2C. *Revista Colombiana de Computación*, *20*(1), 41–58. https://doi.org/10.29375/25392115.3606

Constitución de la República del Ecuador 2008, (2008) (testimony of Registro Oficial). www.lexis.com.ec

Romero, M. I., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., Álava, E., Galo, C., Parrales, R., Christian, A., Álava, J., Ángel, M., Murillo Quimiz, L., Adriana, M., & Merino, C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidadesDES* (1st ed.). Editorial Área de Innovación y Desarrollo S.L. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Rueda, J. S., & Talavera, J. (2017). Similitudes y diferencias entre Redes de Sensores Inalámbricas e Internet de las Cosas: Hacia una postura clarificadora. *Revista Colombiana de Computación, ISSN 1657-2831, ISSN-*

e 2539-2115, Vol. 18, Nº. 2, 2017, Págs. 58-74, *18*(2), 58–74. https://doi.org/10.29375/25392115.3218

Sajjad, S. M., & Yousaf, M. (2014). Security analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT). *Conference Proceedings - 2014 Conference on Information Assurance and Cyber Security, CIACS 2014*, 9–14. https://doi.org/10.1109/CIACS.2014.6861324

Santos Benavides, P. G., & Jurado Lozada, M. A. (2019). *Red inalámbrica de sensores (WSN) de monitoreo de la calidad del agua para estanques de truchas*. Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería Electrónica y Comunicaciones. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/29894

Sharma, S., Yadav, A., Panchal, M., & Vyavahare, P. D. (2019). Classification of Security Attacks in WSNs and Possible Countermeasures: A Survey. *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, *2019-December*. https://doi.org/10.1109/ANTS47819.2019.9118119

Sisteseg Consulting Services. (2018). *Metodología de análisis de riesgo según ISO 27005:2018 e ISO 31000:2018*. https://sisteseg.com/blog/wp-content/uploads/2018/11/Metodologia-para-Gesti%C3%B3n-de-Riesgos-V-1.0.pdf

Soluciones Keller. (2021). *Tecnología LoRA y LoRAWAN - Catsensors*. https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan

Tambaco Suarez, E. O. (2015). *IPV6 en una red WSN para el monitoreo remoto de cultivos en la Granja La Pradera de la Universidad Técnica del Norte.* http://repositorio.utn.edu.ec/handle/123456789/4471

Tawalbeh, A., Hashish, S., Tawalbeh, L., & Aldairi, A. (2017). Security in Wireless Sensor Networks Using Lightweight Cryptography". *Journal of Information Assurance and Security*, 118–123. https://www.researchgate.net/publication/320408314_Security_in_Wireless_Sensor_Networks_Using_Lightweight_Cryptography

Tejedor Doria, J. A. (2020). *Pentesting IoT device: smart doorlock*.

Tejedor, J. A. (2020). *Pentesting IoT device: smart doorlock*.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230–244. https://doi.org/10.23857/pc.v3i4.809

Torrijos, H. (2021). *Auditoría en seguridad sobre una API aplicada a un entorno IoT*.

Trend Micro Incorporated. (2022). *¿Qué es seguridad de red?* https://www.trendmicro.com/es_es/what-is/network-security.html

Universidad Internacional de Valencia. (2017). *Rfid: qué es y cómo funciona | VIU*. https://www.universidadviu.com/pe/actualidad/nuestros-expertos/rfid-que-es-y-como-funciona

Valencia, L., Guarda, T., Patricio, G., Arias, L., & Ninahualpa Quiña, G. (2019). *Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía*.

Vásquez, A. (2021). *Auditoría de seguridad e investigación de protocolos IoT (Thread y Zigbee)*. https://nootropico.li/files/tfg/TFG_IoT_ZigbeeThread.pdf

Wireshark. (2023). *Wireshark · Go Deep.* https://www.wireshark.org/

Yang, B. (2009). Study on security of wireless sensor network based on ZigBee standard. *CIS 2009 - 2009 International Conference on Computational Intelligence and Security*, *2*, 426–430. https://doi.org/10.1109/CIS.2009.208

Anexos

Anexo 1. Código Fuente

a) Nodo coordinador

```
#include <Wire.h>      // libreria de comunicacion por I2C
#include <LCD.h>      // libreria para funciones de LCD
#include <LiquidCrystal_I2C.h>    // libreria para LCD por I2C
#include <SoftwareSerial.h>
LiquidCrystal_I2C lcd (0x27, 2, 1, 0, 4, 5, 6, 7); // DIR, E, RW, RS, D4, D5, D6, D7
#define boton A0
#define lcdLoading 0
#define lcdInfo 1
//#define DEBUG(a) Serial.println(a);
const int pinRx = 2;
const int pinTx = 3;
int select;
String data;
int a;
SoftwareSerial xbee(pinRx, pinTx);

bool xb1Presence = false;
bool xb2Presence = false;
bool xb3Presence = false;

int dataXB11 = 0, dataXB12 = 0, dataXB13 = 0;
int dataXB21 = 0, dataXB22 = 0, dataXB23 = 0;
int dataXB31 = 0, dataXB32 = 0, dataXB33 = 0;

float xb1Temp = 0;
float xb2Temp = 0;
float xb3Temp = 0;

unsigned long offLineInterval = 10000;
unsigned long xb1LastUpdate = 0;
unsigned long xb2LastUpdate = 0;
unsigned long xb3LastUpdate = 0;

bool xb1OffLine = true;
bool xb2OffLine = true;
bool xb3OffLine = true;

int xb1LastState = xb1OffLine;
int xb2LastState = xb2OffLine;
int xb3LastState = xb2OffLine;

unsigned int diInterval = 500;
unsigned long diPreviousMillis = 0;
unsigned int lInterval = 5000;
unsigned long lPreviousMillis = 0;

int stateDisplay = lcdLoading;

uint8_t degree[8] = { 140,146,146,140,128,128,128,128 };
```

```
void setup() {
  Serial.begin(9600);
  xbee.begin(9600);
  pinMode(8,INPUT);
  pinMode(A0,INPUT);
  lcd.setBacklightPin(3,POSITIVE);
  lcd.setBacklight(HIGH);
  lcd.begin(20, 4);
  lcd.createChar(0, degree);
}

void loop() {
  Serial.println(digitalRead(boton));
  if(digitalRead(boton)==HIGH){delay(100);a++;}
  if(a == 2){delay(10);a=0;}
  listenSlaves();
  getTemperature();
  displayInfo();
  slaveStatus();
}

void listenSlaves() {
  int dataNumber = xbee.available();
  if (dataNumber >= 25)
  {
    byte init = xbee.read();
    if (init == 0x7E) {
      discardData(10);
      byte identifier = xbee.read();
      if (identifier == 0x70)
      {
        xb1Presence = true;
        discardData(7);
        dataXB11 = xbee.read();
        dataXB12 = xbee.read();
        discardData(1);
        dataXB13 = xbee.read();
        xb1OffLine = false;
        xb1LastUpdate = millis();
      }
      else if (identifier == 0x5E)
      {
        xb2Presence = true;
        discardData(7);
        dataXB21 = xbee.read();
        dataXB22 = xbee.read();
        discardData(1);
        dataXB23 = xbee.read();
        xb2OffLine = false;
        xb2LastUpdate = millis();
      }
      else if (identifier == 0x71)
      {
        xb3Presence = true;
```

```
        discardData(7);
        dataXB31 = xbee.read();
        dataXB32 = xbee.read();
        discardData(1);
        dataXB33 = xbee.read();Serial.println(dataXB33);
        if(dataXB33 == 255){select++;delay(1000);}
        xb3OffLine = false;
        xb3LastUpdate = millis();
      }
    }
  }
}
void discardData(int jump) {
  int _jump = jump;
  for (int i = 0; i < _jump; i++)
  {
    byte discarded = xbee.read();
  }
}
void getTemperature() {
  if (xb1Presence)
  {
    if(a==0){
      dataXB11 *= 256;
      float mv = dataXB11 + dataXB12;
      mv *= 3.22;
      xb1Temp = mv/25;
      xb1Presence = false;
      //Serial.println(xb1Temp);
    }
    if(a==1){
      dataXB11 *= 256;
      float mv = dataXB11 + dataXB12;
      xb1Temp = (mv*100)/1023;
      xb1Presence = false;
      //Serial.println(xb1Temp);
    }
  }
  else if (xb2Presence)
  {
    dataXB21 *= 256;
    float mv = dataXB21 + dataXB22;
    mv *= 3.22;
    xb2Temp = mv/25;
    xb2Presence = false;
    //Serial.println(xb2Temp);
  }
  else if (xb3Presence)
  {
    dataXB31 *= 256;
    float mv = dataXB31 + dataXB32;
    mv *= 3.22;
    xb3Temp = mv/25;
    xb3Presence = false;
    //Serial.println(xb2Temp);
```

```
  }
}
void displayInfo() {
  unsigned long currentMillis = millis();
  if (stateDisplay == lcdLoading)
  {
    displayLoading();
    if ((currentMillis - lPreviousMillis) >= (lInterval))
    {
      stateDisplay = lcdInfo;
      cleanDisplay();
    }
  }
  else if (stateDisplay == lcdInfo)
  {
    if ((currentMillis - diPreviousMillis) >= (diInterval))
    {
      diPreviousMillis = currentMillis;
      displayTemperatures();
    }
  }
}
void slaveStatus() {
  unsigned long currentMillis = millis();
    if (!xb1OffLine)
    {
      if ((currentMillis - xb1LastUpdate) >= (offLineInterval))
        xb1OffLine = true;
    }
    if (!xb2OffLine)
    {
      if ((currentMillis - xb2LastUpdate) >= (offLineInterval))
        xb2OffLine = true;
    }
}
void displayLoading() {
  lcd.setCursor(4, 0); lcd.print("");
  lcd.setCursor(2, 1); lcd.print("Redes de Sesores");
 lcd.setCursor(6, 2); lcd.print("con Xbee");
  lcd.setCursor(4, 3); lcd.print("");
}
void displayTemperatures() {
  if (select==0 ||select==1 ||select==2){
  if (xb1LastState != xb1OffLine || xb2LastState != xb2OffLine)
    cleanDisplay();
  lcd.setCursor(6, 0); lcd.print("XBee s01");
  if(a==0){lcd.setCursor(0, 1); lcd.print("T= ");}
  if(a==1){lcd.setCursor(0, 1); lcd.print("CO2: ");}
  if (select==0){
    lcd.print(xb1Temp);
  }
  if (select==1){
    lcd.print(random(0,200));
  }
  if (select==2){
```

```
    lcd.clear();
  }
  if (select==3){
    select=0;
  }
  if(a==0){lcd.write(byte(0)); lcd.print("C");}
  if(a==1){lcd.print("%");}
  if (!xb1OffLine) {
    lcd.print(" On line");
    if (xb1LastState != xb1OffLine)
      xb1LastState = xb1OffLine;
  }
  else if (xb1OffLine) {
    lcd.print(" Off line");
    if (xb1LastState != xb1OffLine)
      xb1LastState = xb1OffLine;
  }
  lcd.setCursor(6, 2); lcd.print("XBee s02");
  lcd.setCursor(0, 3); lcd.print("T= ");
  if (select==0){
    lcd.print(xb2Temp);
  }
  if (select==1){
    lcd.print(random(0,200));
  }
  if (select==2){
    lcd.clear();
  }
  if (select==3){
    select = 0;
  }
  lcd.write(byte(0)); lcd.print("C");
  if (!xb2OffLine) {
    lcd.print(" On line");
    if (xb2LastState != xb2OffLine)
      xb2LastState = xb2OffLine;
  }
  else if (xb2OffLine) {
    lcd.print(" Off line");
    if (xb2LastState != xb2OffLine)
      xb2LastState = xb2OffLine;
  }
  }
}
void cleanDisplay() {
  lcd.clear();
}
```

b) Nodo atacante

```
#include <Wire.h>      // libreria de comunicacion por I2C
#include <LCD.h>       // libreria para funciones de LCD
#include <LiquidCrystal_I2C.h>    // libreria para LCD por I2C
#include <SoftwareSerial.h>
LiquidCrystal_I2C lcd (0x27, 2, 1, 0, 4, 5, 6, 7); // DIR, E, RW, RS, D4, D5, D6, D7
```

```
#define lcdLoading 0
#define lcdInfo 1
//#define DEBUG(a) Serial.println(a);
const int pinRx = 2;
const int pinTx = 3;
int select;
String data;
SoftwareSerial xbee(pinRx, pinTx);

bool xb1Presence = false;
bool xb2Presence = false;
bool xb3Presence = false;

int dataXB11 = 0, dataXB12 = 0, dataXB13 = 0;
int dataXB21 = 0, dataXB22 = 0, dataXB23 = 0;
int dataXB31 = 0, dataXB32 = 0, dataXB33 = 0;

float xb1Temp = 0;
float xb2Temp = 0;
float xb3Temp = 0;

unsigned long offLineInterval = 10000;
unsigned long xb1LastUpdate = 0;
unsigned long xb2LastUpdate = 0;
unsigned long xb3LastUpdate = 0;

bool xb1OffLine = true;
bool xb2OffLine = true;
bool xb3OffLine = true;

int xb1LastState = xb1OffLine;
int xb2LastState = xb2OffLine;
int xb3LastState = xb2OffLine;

unsigned int diInterval = 500;
unsigned long diPreviousMillis = 0;
unsigned int lInterval = 5000;
unsigned long lPreviousMillis = 0;

int stateDisplay = lcdLoading;

uint8_t degree[8] = { 140,146,146,140,128,128,128,128 };

void setup() {
  Serial.begin(9600);
  xbee.begin(9600);
  pinMode(8,INPUT);
  lcd.setBacklightPin(3,POSITIVE);
  lcd.setBacklight(HIGH);
  lcd.begin(20, 4);
  lcd.createChar(0, degree);
}
```

```
void loop() {
  displayLoading();
}
void listenSlaves() {
  int dataNumber = xbee.available();
  if (dataNumber >= 25)
  {
    byte init = xbee.read();
    if (init == 0x7E) {
      discardData(10);
      byte identifier = xbee.read();
      if (identifier == 0x70)
      {
        xb1Presence = true;
        discardData(7);
        dataXB11 = xbee.read();
        dataXB12 = xbee.read();
        discardData(1);
        dataXB13 = xbee.read();
        xb1OffLine = false;
        xb1LastUpdate = millis();
      }
      else if (identifier == 0x5E)
      {
        xb2Presence = true;
        discardData(7);
        dataXB21 = xbee.read();
        dataXB22 = xbee.read();
        discardData(1);
        dataXB23 = xbee.read();
        xb2OffLine = false;
        xb2LastUpdate = millis();
      }
      else if (identifier == 0x71)
      {
        xb3Presence = true;
        discardData(7);
        dataXB31 = xbee.read();
        dataXB32 = xbee.read();
        discardData(1);
        dataXB33 = xbee.read();Serial.println(dataXB33);
        if(dataXB33 == 255){select++;delay(1000);}
        xb3OffLine = false;
        xb3LastUpdate = millis();
      }
    }
  }
}
void discardData(int jump) {
  int _jump = jump;
  for (int i = 0; i < _jump; i++)
  {
    byte discarded = xbee.read();
  }
}
```

```
void getTemperature() {
  if (xb1Presence)
  {
    dataXB11 *= 256;
    float mv = dataXB11 + dataXB12;
    mv *= 3.22;
    xb1Temp = mv/25;
    xb1Presence = false;
    //Serial.println(xb1Temp);
  }
  else if (xb2Presence)
  {
    dataXB21 *= 256;
    float mv = dataXB21 + dataXB22;
    mv *= 3.22;
    xb2Temp = mv/25;

    xb2Presence = false;
    //Serial.println(xb2Temp);
  }
  else if (xb3Presence)
  {
    dataXB31 *= 256;
    float mv = dataXB31 + dataXB32;
    mv *= 3.22;
    xb3Temp = mv/25;
    xb3Presence = false;
    //Serial.println(xb2Temp);
  }
}
void displayInfo() {
  unsigned long currentMillis = millis();
  if (stateDisplay == lcdLoading)
  {
    displayLoading();
    if ((currentMillis - lPreviousMillis) >= (lInterval))
    {
      stateDisplay = lcdInfo;
      cleanDisplay();
    }
  }
  else if (stateDisplay == lcdInfo)
  {
    if ((currentMillis - diPreviousMillis) >= (diInterval))
    {
      diPreviousMillis = currentMillis;
      displayTemperatures();
    }
  }
}
void slaveStatus() {
  unsigned long currentMillis = millis();
    if (!xb1OffLine)
    {
      if ((currentMillis - xb1LastUpdate) >= (offLineInterval))
```

```
        xb1OffLine = true;
    }
    if (!xb2OffLine)
    {
      if ((currentMillis - xb2LastUpdate) >= (offLineInterval))
        xb2OffLine = true;
    }
}
void displayLoading() {
  lcd.setCursor(3, 0); lcd.print("ATACAR SISTEMA");
  lcd.setCursor(2, 1); lcd.print("");
 lcd.setCursor(2, 2); lcd.print("1. Datos Erroneos");
  lcd.setCursor(4, 3); lcd.print("2. Limpiar");
}
void displayTemperatures() {
  if (select==0 ||select==1 ||select==2){
  if (xb1LastState != xb1OffLine || xb2LastState != xb2OffLine)
    cleanDisplay();
  lcd.setCursor(6, 0); lcd.print("XBee s01");
  lcd.setCursor(0, 1); lcd.print("T= ");
  if (select==0){
    lcd.print(xb1Temp);
  }
  if (select==1){
    lcd.print(random(0,200));
  }
  if (select==2){
    lcd.clear();
  }
  if (select==3){
    select=0;
  }
  lcd.write(byte(0)); lcd.print("C");
  if (!xb1OffLine) {
    lcd.print(" On line");
    if (xb1LastState != xb1OffLine)
      xb1LastState = xb1OffLine;
  }
  else if (xb1OffLine) {
    lcd.print(" Off line");
    if (xb1LastState != xb1OffLine)
      xb1LastState = xb1OffLine;
  }
  lcd.setCursor(6, 2); lcd.print("XBee s02");
  lcd.setCursor(0, 3); lcd.print("T= ");
  if (select==0){
    lcd.print(xb2Temp);
  }
  if (select==1){
    lcd.print(random(0,200));
  }
  if (select==2){
    lcd.clear();
  }
  if (select==3){
```

```
    select = 0;
   }
   lcd.write(byte(0)); lcd.print("C");
   if (!xb2OffLine) {
    lcd.print(" On line");
    if (xb2LastState != xb2OffLine)
      xb2LastState = xb2OffLine;
   }
   else if (xb2OffLine) {
    lcd.print(" Off line");
    if (xb2LastState != xb2OffLine)
      xb2LastState = xb2OffLine;
   }
   }
}
void cleanDisplay() {
  lcd.clear();
}
```

Anexo 2. Guía de usuario Auditor

GUÍA DE USUARIO AUDITOR

Aplicación de Metodología de Auditoría de seguridad para redes de sensores inalámbricos

Elaborado por: Oñate Kevin

Revisado por: Ing. Fabián Cuzme Rodríguez

2023

CONTENIDO

Pág.

INTRODUCCIÓN

El método de auditoría de seguridad en redes de sensores inalámbricas propuesto se basa en los parámetros de Offensive Security y en algunos aspectos de OWSAP a modo complementario. El método de auditoría propuesto considera que existe una red inalámbrica de sensores que requiere ser evaluada en términos de seguridad. De igual manera, es preciso definir el equipo de auditoría y los respectivos roles que serán asignados para cada una de las fases.

Esta metodología se compone de seis fases: i) recolección de la información, ii) análisis de vulnerabilidades, iii) definición de objetivos secundarios, iv) ataques, v) análisis de resultados y vi) análisis final y documentación.

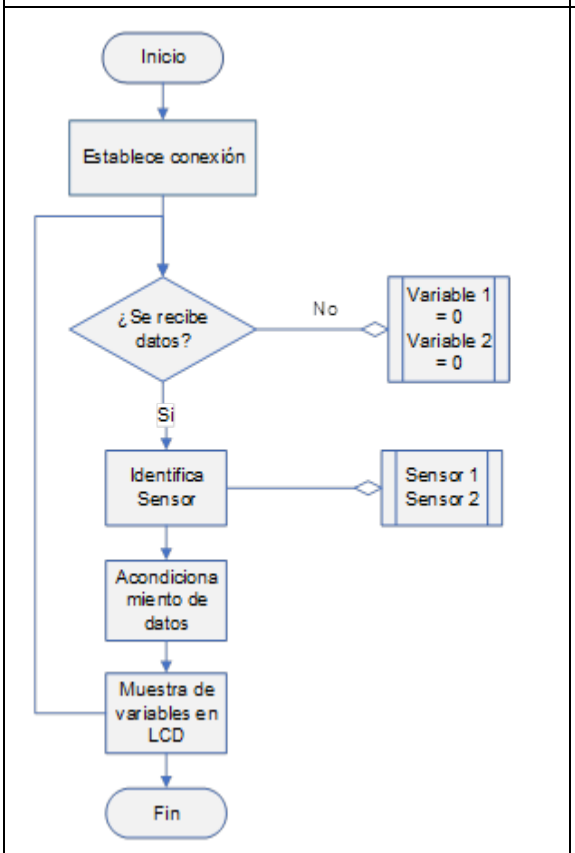
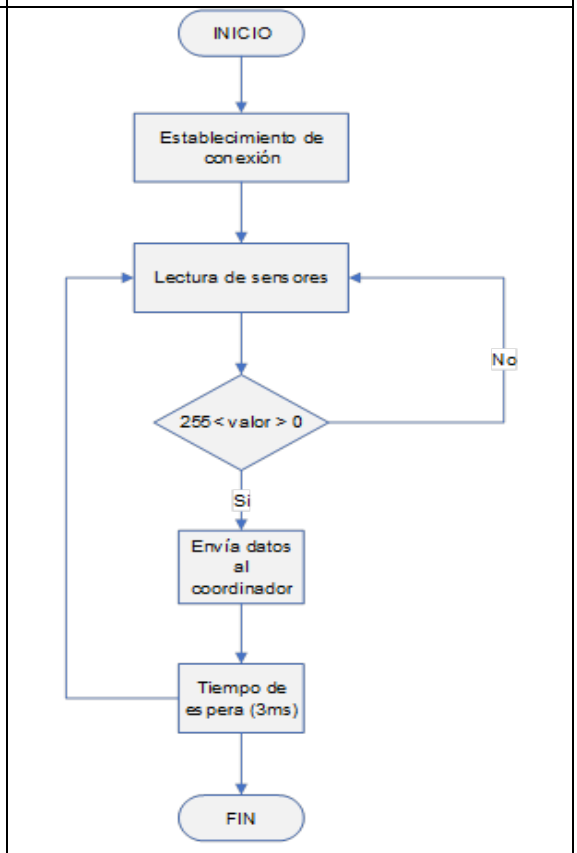
METODOLOGÍA DE AUDITORÍA DE SEGURIDAD PARA "RED DE SENSORES INALÁMBRICOS"

Fase 1. RECOPILACIÓN DE INFORMACIÓN

Para iniciar el proceso de auditoría, es preciso obtener toda la información del sistema a evaluar para llevar a cabo un diagnóstico adecuado. Así, las actividades a desarrollar son la siguientes:

a. Situación actual

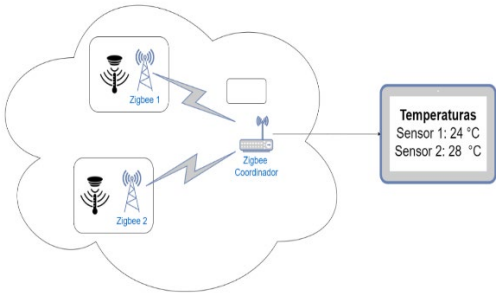
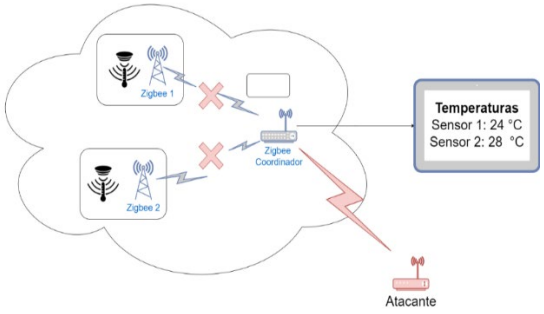
En esta etapa es necesario identificar y presentar flujos de proceso de nodo coordinador, sensor y topología de la red. Esta actividad considera la configuración de la red y de los puertos respectivos. Se realiza una verificación de la recepción, consolidación de datos y se presentan los niveles arrojados por los sensores, dependiendo de la naturaleza de su medición.

Funcionamiento nodo coordinador	Funcionamiento nodos sensores
	

b. Planeación de ataques

Se define el alcance de los ataques y se determina su flujo en función de la naturaleza de los sensores. El flujo de ataque inicia con una lectura de tramas utilizando herramienta Zboss. Posteriormente, se realiza una lectura de paquetes capturados con el programa Wireshark; se identifica la dirección del nodo coordinador PAN ID y se ejecuta el ataque en particular implementado, mientras que en segundo lugar se utiliza ataque de fuerza bruta.

Cabe mencionar que también es importante la selección del evaluador responsable de la ejecución del ataque y para la coordinación se debe determinar herramientas como ZBOSS Sniffer, WireShark y Zigbee-emulador CC, depurador, programador USB. Los ataques que se toman en cuenta pueden ser de confidencialidad, integridad y disponibilidad. Además, se debe planificar los ataques, donde se describe las actividades, tiempos o duración, recursos y responsable.

Topología de WSN sin ataque	Topología ataque a WSN
	

Fase 2. ANÁLISIS DE VULNERABILIDADES

Para continuar con el análisis de las vulnerabilidades, se utilizan criterios establecidos en la metodología NIST SP 800-30.

a. Preparación para evaluación de riesgos.

Esta actividad consiste en la determinación del alcance de la identificación del nivel de riesgos evidenciado con cada ataque planificado y los métodos para implementarla. Se sugiere una matriz de riesgo, probabilidades, magnitud del impacto, escala de riesgos y acciones a implementar.

b. Realización de la evaluación de riesgos.

Una vez determinado el alcance de la evaluación de riesgos debe ejecutarse. Para ello, se realiza la matriz fuente de amenaza:

Matriz fuente de amenaza

Activo	Ataque	Vulnerabilidad	Fuente de amenaza
Red de sensores inalámbricos	Confidencialidad Integridad Disponibilidad	Indicar tipo de vulnerabilidad	Indicar origen de la amenaza

Posteriormente, se elabora la matriz de evaluación de riesgo:

Matriz evaluación de riesgo

Activo	Ataque	Vulnerabilidad	Probabilidad de amenaza	Impacto	Valoración de riesgo
Red de sensores inalámbricos	Confidencialidad Integridad Disponibilidad				

Valor entre 51 y 100: Riesgo elevado

Valor entre 25 y 50: Riesgo moderado

Valor entre 0 y 24: Riesgo bajo

c. Comunicar y compartir información de evaluación del riesgo

Es preciso realizar la comunicación de la evaluación de riesgos observadas. Se indicará el tipo de vulnerabilidad asociado al tipo de ataque, y se señalarán las probabilidades de ocurrencia de la amenaza, el nivel de impacto y la valoración global del riesgo.

d. Mantenimiento.

Con base en el estándar ISO/IEC 27002 se establecen los lineamientos para llevar a cabo el mantenimiento en atención a las vulnerabilidades detectadas. Se considerarán los controles físicos a aplicar en sensores, las propiedades de la información respecto de la seguridad, el personal necesario para llevarlo a cabo (talento humano) y la tecnología.

Se elaborará la siguiente propuesta de matriz de control de riesgo.

Matriz control de riesgo

Tipo de control	Información	Seguridad	Capacidad operacional	Dominio de seguridad	Frecuencia
Preventivo					
Detectivo					
Correctivo					

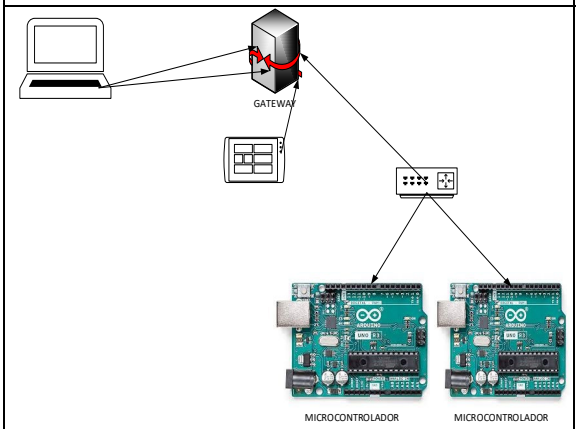
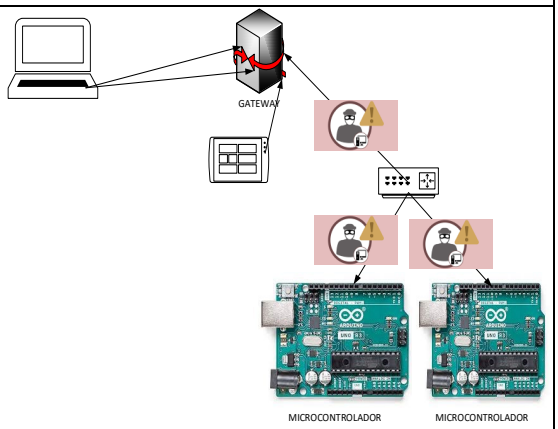
Fase 3. DEFINICIÓN DE OBJETIVOS SECUNDARIOS

En esta fase se prepara el proceso de definición de los objetivos específicos que son propio del proyecto y los objetivos secundarios del análisis de vulnerabilidades.

a. **Objetivo específico:** Se determinará la herramienta y equipo encargado de llevar a cabo esta fase y los responsables.
b. **Objetivos secundarios:** Se sugiere el uso de la metodología OWASP para seleccionar los ataques o técnicas más adecuados. Por último, se establece aspectos relacionados con la elaboración del informe.

Fase 4. ATAQUES

a. Se diseña la red en la arquitectura del modelo de red y topología de red de sensores atacada. Véase el ejemplo a continuación:

Arquitectura modelo de red	*Topología de red para evaluación*
	

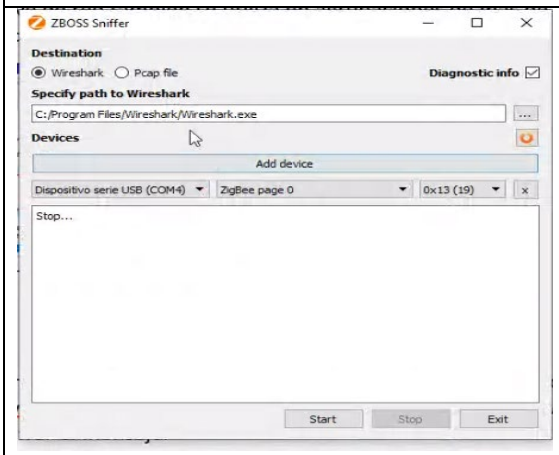
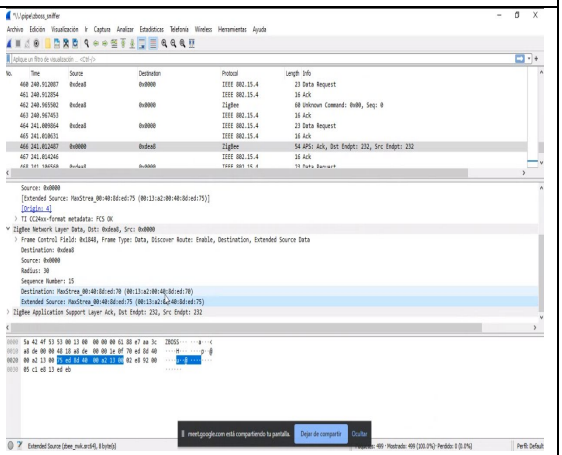
b. Se llevan a cabo los ataques determinados, que pueden ser de confidencialidad, de integridad o disponibilidad.

Ataque de confidencialidad

El proceso de ataque de confidencialidad se aprecia en el siguiente diagrama:

Diagrama de secuencia para ataque de confidencialidad

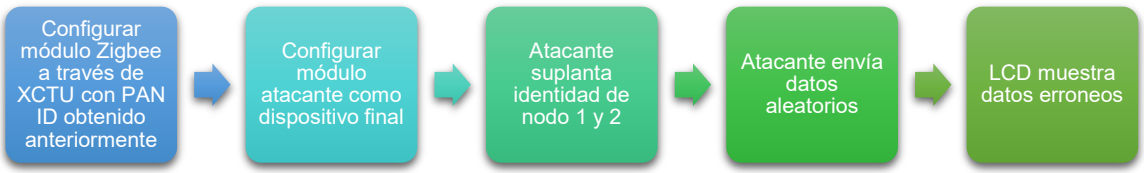
- Escanear los canales de la capa de la red con Zboss, este se conecta a la antena. En la interfaz Zboss se selecciona el puerto serial al que se conecte la antena y decodificador zigbee.
- Realizar varias pruebas hasta identificar el canal de comunicación.
- Uso de Wireshark para capturar las tramas de coordinador y clientes
- Se identifica PAN ID de la red, con esto se realiza el resto de ataques.

Ataque de confidencialidad	Captura de paquetes (tramas)
	

Ataque de integridad

El proceso de ataque de integridad se aprecia en el siguiente diagrama:

Diagrama de secuencia para ataque de integridad

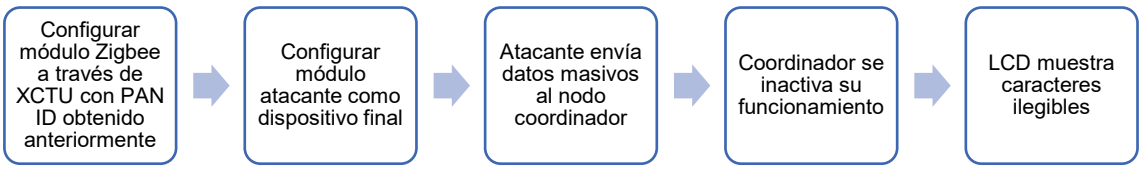


- Configurar el módulo atacante Zigbee, utilizando el programa XCTU.
- El atacante realiza suplantación de identidad en nodo 1 – 2, modificando y enviando los datos.
- Considerar PAN ID del primer ataque.
- Leer el puerto digital y recibe datos aleatorios del Arduino atacante.
- La pantalla LCD del nodo coordinador se presenta información equivocada.

Ataque de disponibilidad

El proceso de ataque de integridad se aprecia en el siguiente diagrama:

Diagrama de secuencia para ataque de disponibilidad



- Considerar técnica intrusiva como denegación de servicio (DoS).
- Configurar el módulo atacante Zigbee, utilizando el programa XCTU.
- Atacante envía datos masivos al nodo coordinador.
- Considerar PAN ID del primer ataque.
- Se presenta inactividad del nodo coordinador
- El Arduino envía datos aleatorios al nodo 1 y 2.
- En la pantalla LCD se presentan caracteres especiales que no se visualizan.

Fase 5. ANÁLISIS DE RESULTADOS

En esta fase de la metodología deben presentarse los hallazgos de las vulnerabilidades encontradas para cada escenario valorado, lo cual se lleva a cabo mediante la comparación de métricas mediante CVSS.

a. Presentación de hallazgos

Para cada escenario valorado se indicarán de forma particular sus alcances y los hallazgos identificados, entre los cuales pueden destacar la

manipulación de datos, denegación de servicios captura de paquetes, entre otros.

b. Determinación método comparativo

Se propone el método de cálculo de gravedad de vulnerabilidades CVSS (*Common Vulnerability Score System*). Este corresponde a un cálculo para transformar fórmulas simples en índices de gravedad de las vulnerabilidades identificadas mediante la observación de las métricas que son de carácter estándar.

Escala de calificación CVSS

Calificación (C)	Escala
0	Nulo
1 – 3,9	Bajo
4 – 6,9	Medio
7 – 8,9	Alto
9 - 10	Muy Alto

c. Determinación de la métrica

Pueden ser básicas o temporales. Las métricas básicas corresponden a las características constantes del entorno de usuario. Las métricas temporales son variables que reflejan vulnerabilidades y que cambian con el tiempo.

Básicas	Temporales
• Explotabilidad: métricas en torno a la facilidad y otros aspectos técnicos de explotación. Entre estas se encuentran: i) vector de acceso a red de sensores ii) complejidad de acceso y iii) autenticación. • Impacto: refiere a las métricas que analizan las consecuencias de un impacto directo. Entre estas se encuentran: I) confidencialidad, ii) integridad, iii) disponibilidad y iv) impacto de reconocimiento de puertos.	• Explotabilidad • Confiabilidad • Fiabilidad del informe de vulnerabilidad y facilidad de solución

d. Comparación de pruebas intrusivas

Es preciso realizar una comparación de las distintas pruebas intrusivas mediante el criterio de las ventajas o desventajas que estas representan.

Sniffing	
Ventajas	**Desventajas**
• Permite controlar tráfico • No requiere de conocimientos sofisticados • Posibilita cambios en la seguridad • Captura contraseñas y nombres de usuario	• Requiere de conocimiento previo

Phishing	
Ventajas	**Desventajas**
• No requiere conocimientos sofisticados • Permite identificar mensajes no deseados o información confidencial • Entre otras	• No permite identificar vulnerabilidades técnicas

Modificación de datos	
Ventajas	**Desventajas**
• Prueba con costo menor • Presentación sencilla de información • Entre otras	• Puede ocasionar cuellos de botella

Denegación de servicio (DoS)	
Ventajas	**Desventajas**
• Permite presentar información de manera sencilla • Permite identificar la información cambiada e implementar medidas • Coadyuva a identificar paquetes alterados • Entre otras	• Requiere de conocimientos previos

e. Análisis de seguridad de trabajos existentes

Este paso corresponde al análisis comparativo de la seguridad y vulnerabilidad en trabajos previos realizados. Permite generar el conocimiento sobre el estado del arte en torno a la seguridad en redes de sensores inalámbricas.

Matriz Análisis de seguridad de trabajos existentes

Trabajos	Tipo de seguridad	Vulnerabilidades

f. Comparativa

Se lleva a cabo a continuación la comparación de las pruebas intrusivas empleadas para los ataques en la red. Se sugiere el uso de las técnicas:

Técnicas intrusivas

Luego de elabora una matriz comparativa de técnicas intrusivas, considerando que el puntaje (P), este debe sumar un total de 1,00. En la

calificación (C) se otorga puntuación según la escala de calificación CVSS. El total de cada técnica se obtiene de la multiplicación entre P y C. Para identificar la técnica más adecuada se debe sumar los totales de cada parámetro y seleccionar la que posea mayor puntuación.

Matriz comparativa de técnicas intrusivas

Parámetro	P	Suplantación de identidad		DoS		Sniffing		Modificación de datos		Nombre de técnicas	
		C	T	C	T	C	T	C	T	C	T
Vector de Acceso a red de sensores	0,10		Multiplicar								
Complejidad de Acceso a red de sensores	0,10										
Autenticación	0,09										
Confidencialidad	0,09			Sumar							
Integridad	0,09										
Disponibilidad	0,09										
Explotabilidad	0,09										
Confiabilidad	0,09										
Impacto en Reconocimiento de Puertos	0,10					Mayor puntaje					
Facilidad de Solución	0,08										
Fiabilidad del Informe de Vulnerabilidad	0,08										
Total	1,00		**6,04**		**6,58**		**8,65**		**6,04**		**0,00**

FASE 6. PRESENTACIÓN DE EVIDENCIA

Esta fase corresponde a la etapa final de la auditoría realizada; en ella se realiza el análisis final y se elabora toda la documentación necesaria, en donde se detalla la evidencia recopilada y todo el diseño de auditoría llevado a cabo en el proyecto.

a. Presentación de evidencias

La presentación de evidencias debe considerar una descripción detallada del escenario, los ataques, las técnicas de ataque utilizadas y las vulnerabilidades encontradas. Se sugiere completar una matriz como la siguiente:

Matriz de evidencias

Escenario	Ataque	Técnica de ataque	Vulnerabilidad detectada
Escenario 1	Confidencialidad	Sniffing	Vulnerabilidad 1, 2, …n
	Integridad	Phishing Modificación de datos	…
	Disponibilidad	DoS	
	…	…	…
Escenario 2	…	…	…
Escenario n…	…	…	…

b. Informe de auditoría

El informe de la auditoría deberá ser la documentación final detallada en donde conste el proceso completo llevado a cabo, con datos generales, metodología de auditoría, resultados y recomendaciones en atención a dichos resultados. Así, se presentará:

Datos generales

Los datos generales registrarán todas las generalidades de la auditoría realizada. Se incluirá:

- **Objetivo de auditoría:** define la finalidad que tuvo la auditoría.
- **Alcance de auditoría:** define los procesos, escenarios y aspectos que se evaluaron dentro de la auditoría. Se detallarán los datos de los softwares utilizados, la identificación de vulnerabilidades buscadas, el tipo de red inalámbrica y sensores, herramientas (como ZBOSS Sniffer, WireShark, entre otras). Se definirán los ataques y las técnicas intrusivas para llevarlos a cabo.

Metodología

En este apartado se describirá el método mediante el cual se realizó la auditoría, los aspectos que fueron evaluados y el proceso y control mediante el cual fueron realizados. Incluirá:

- **Método:** se describirá el método utilizado. Se sugiere aquí la presente metodología de visualización de panorama y verificación de documentos, que consta de la revisión del funcionamiento de los equipos y software. La verificación deberá realizarse mediante el análisis de fuentes secundarias de información.
- **Aspectos evaluados:** se detallará cada variable en estudio, sus métricas, el tipo de vulnerabilidad que se quiere observar, los ataques y las técnicas de ataque en los distintos escenarios determinados.

- **Proceso:** Se describirá claramente el proceso llevado a cabo en un diagrama de flujo o similar.
- **Manejo:** se detallarán los mecanismos establecidos para la realización de la auditoría y su control.

Hallazgos

En este apartado del informe es preciso incluir los hallazgos identificados. Se detallará con claridad el momento, tipo de ataque y vulnerabilidad. De igual manera, serán indicados todos los hallazgos positivos y negativos.

- Aspectos positivos: corresponde a todas las observaciones realizadas que dan cuenta de una adecuada seguridad de la red ante ataques intrusivos. Se detallan todos los parámetros bajo los que se realizaron estas observaciones.
- Aspectos negativos: Se detallan todos los problemas de seguridad identificados y los parámetros bajo los que fueron constatados.

Recomendaciones

Finalmente, las recomendaciones serán indicadas en este apartado, y estarán en línea con los hallazgos identificados. Corresponden a todas las modificaciones y/o medidas que pueden ser establecidas para mitigar riesgos de ataques y vulnerabilidades. Es importante considerar normas como NIST, OWASP y MITRE.

Matriz de medidas

Vulnerabilidades	Ataques	Medidas

Anexo 3. Formato de informe de auditoría

INFORME DE AUDITORÍA DE SEGURIDAD EN REDES DE SENSORES INALÁMBRICAS	
Nro. de auditoría	
Fecha	
Institución o proyecto auditado	
Responsable de proyecto auditado	
Responsable de equipo auditor	
Equipo auditor	
Nombre 1	
Nombre 2	
Nombre n…	
Datos generales	
Hora de comienzo	
Objetivo de auditoría	
Alcance de auditoría	
Metodología de auditoría	
Método	
Aspectos evaluados	

<table>
<tr><td></td><td></td></tr>
<tr><td>Proceso</td><td></td></tr>
<tr><td>Manejo</td><td></td></tr>
<tr><td colspan="2">Hallazgos</td></tr>
<tr><td>Matriz de evidencias</td><td>
<table>
<tr><th>Escenario</th><th>Ataque</th><th>Técnica de ataque</th><th>Herramientas utilizadas</th><th>Vulnerabilidad detectada</th></tr>
<tr><td>Escenario 1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>E2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>En…</td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Hallazgos positivos y negativos</td><td>
<table>
<tr><th>Aspectos</th><th>Descripción</th></tr>
<tr><td>Negativos</td><td>•
•</td></tr>
<tr><td>Positivos</td><td>•
•</td></tr>
</table>
</td></tr>
<tr><td>Recomendaciones</td><td>
<table>
<tr><th>Vulnerabilidad</th><th>Ataque</th><th>Medidas</th></tr>
<tr><td>Vulnerabilidad 1</td><td></td><td></td></tr>
<tr><td>V2</td><td></td><td></td></tr>
<tr><td>Vn…</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Firma de responsables</td><td>_____
Responsable 1</td><td>_____
Responsable 2</td></tr>
</table>