ISSN 2529-9824

Artículo de Investigación

Estrategias de seguridad informática para mitigar vulnerabilidades en la red de en un sistema IoT agrícola en la provincia del Sumapaz en Colombia

Computer security strategies to mitigate vulnerabilities in the network of an agricultural IoT system in the province of Sumapaz in Colombia

Alexander Gordillo-Gaitán[1]: Universidad de Cundinamarca, Colombia.
agordillog@ucundinamarca.edu.co
Dayana Carolina Suárez-Quintero: Universidad de Cundinamarca, Colombia.
dayanacsuarez@ucundinamarca.edu.co
María Camila Castillo-Fernández: Universidad de Cundinamarca, Colombia.
mcamilacastillo@ucundinamarca.edu.co

Fecha de Recepción: 11/06/2024

Fecha de Aceptación: 04/09/2024

Fecha de Publicación: 28/01/2025

How to cite the article:

Gordillo-Gaitán, A., Suárez-Quintero, D. C. y Castillo-Fernández, M. C. (2025). Estrategias de seguridad informática para mitigar vulnerabilidades en la red de en un sistema IoT agrícola en la provincia del Sumapaz en Colombia [Computer security strategies to mitigate vulnerabilities in the network of an agricultural IoT system in the province of Sumapaz in Colombia]. *European Public & Social Innovation Review*, 10, 1-17. https://doi.org/10.31637/epsir-2025-1374

Resumen:
Introducción: El Internet de las Cosas ha abordado los desafíos de tecnificación agrícola y la adaptación para mejorar el uso de recursos como el agua y nutrientes de las plantas, impulsando el avance de esta tecnología dada su relevancia en la transición hacia la Industria 4.0. Este estudio plantea estrategias para mitigar vulnerabilidades de un sistema IoT agrícola de la provincia del Sumapaz en Colombia. **Metodología**: Se desarrolló en cinco fases, 1) Revisión de fuentes de información relacionadas con IoT. 2) Caracterización de las estrategias

[1] **Autor Correspondiente:** Alexander Gordillo-Gaitán. Universidad de Cundinamarca (Colombia).

consultadas. 3) Implementar los escenarios seleccionados en un ambiente Gray Box. 4) Plantear la estrategia de mitigación de las vulnerabilidades de los escenarios. 5) Validar la efectividad de cada estrategia a través de un análisis comparativo. **Resultados:** Creación de escenarios de hacking y posterior plantemamiento de estrategias de ciberseguriddad sobre la red y el servidor del sistema IoT. **Discusión**: La seguridad informática en sectores tecnológicamente emergentes o en transición a la industria 4.0 como el agrícola debe liderar un esfuerzo continuo y holístico que involucre a todos los actores. **Conclusiones**: Las estrategias mostraron mitigar el impacto de las vulnerabilidades contribuyendo a la disponibilidad, accesibilidad y confiabilidad del sistema IoT en la provincia del Sumapaz.

Palabras clave: Ciberseguridad IoT; Estrategias seguridad informática; Gray Box; Ethical Hacking; Internet de las Cosas; IoT en cultivos; Industria 4.0; Vulnerabilidades en IoT.

Abstract:
Introduction: The Internet of Things has addressed the challenges of agricultural technification and adaptation to improve the use of resources such as water and plant nutrients, driving the advancement of this technology given its relevance in the transition towards Industry 4.0. This study proposes strategies to mitigate vulnerabilities of an agricultural IoT system in the province of Sumapaz in Colombia. **Methodology:** It was developed in five phases: 1) Review of information sources related to IoT. 2) Characterization of the consulted strategies. 3) Implement the selected scenarios in a Gray Box environment. 4) Propose a strategy to mitigate the vulnerabilities of the scenarios. 5) Validate the effectiveness of each strategy through a comparative analysis. **Results:** Creation of hacking scenarios and subsequent proposal of cybersecurity strategies on the network and the server of the IoT system. **Discussion:** Information security in technologically emerging sectors or those transitioning to Industry 4.0, such as agriculture, must lead a continuous and holistic effort involving all stakeholders. **Conclusions:** Strategies were shown to mitigate the impact of vulnerabilities, contributing to the availability, accessibility, and reliability of the IoT system in the province of Sumapaz.

Keywords: IoT Cybersecurity; Information Security Strategies; Gray Box; Ethical Hacking; Internet of Things; IoT in Crops; Industry 4.0; IoT Vulnerabilities.

1. Introducción

La agricultura es la principal fuente de alimentación a nivel mundial y ha sido clave para el desarrollo de las civilizaciones. Según la Organización de las Naciones Unidas (ONU, 2019), se estima que la población mundial aumente 2.000 millones para el 2050, incrementando la demanda de alimentos y agua. Aunque podría parecer que la producción de alimentos debe aumentar para satisfacer el crecimiento poblacional, la Organización de las Naciones Unidas para la Agricultura y la Alimentación (FAO) afirma que no es necesario un incremento del 50% en la producción agrícola si se adoptan sistemas de producción más sostenibles. Para lograrlo, es esencial aprovechar al máximo la tecnología, la investigación y el desarrollo, promoviendo así los principios de la agricultura sostenible (Organización de las Naciones Unidas para la Alimentación y la Agricultura [ONUAA], 2018).

En el cambiante campo de la tecnología moderna el Internet de las Cosas (IoT, por sus siglas en inglés) ha capturado el interés de los usuarios y rediseñado industrias dado los muchos avances que ha generado a lo largo de su evolución. El IoT posee la habilidad de resolver problemáticas globales urgentes ofreciendo soluciones creativas que pueden reducir el impacto del avance tecnológico en el medio ambiente, incrementar la efectividad de los recursos y mejorar la calidad de vida en general (Singh y Singh, 2023). Como concepto, el IoT

se conoce como el conjunto de tecnologías emergentes, donde los sistemas, dispositivos y cosas están conectadas a través de Internet para recolectar, compartir y evaluar datos, sacando conclusiones o actuando por sí mismo (Sinha y Dhanalakshmi, 2022).

La Agricultura Inteligente ofrece un camino sustentable a través del uso de tecnologías de la información y comunicaciones en el ciclo físico-cibernético de la gestión del agro, con tecnologías como IoT, además cuenta con el enfoque de la agricultura de precisión que mejora la exactitud de las operaciones al dar a cada planta o animal lo que necesita para crecer apropiadamente reduciendo los desperdicios y la contaminación (Friha *et al*., 2021). En una revisión de Farooq *et al*. (2020) se videncia que el uso del IoT para diferentes aplicaciones en la agricultura el 16% se concentra en el monitoreo de la irrigación, 13% en monitoreo del suelo, el 12% en temperatura, 11% en monitoreo de humedad igual que en animales, el 5% en enfermedades y monitoreo del aire, el monitoreo del agua con el 7 % y por último el monitoreo de la fertilización con el 4%. Para la implementación de estos procesos en la agricultura inteligente existe la detección inteligente que se refiere a los sensores que se encargan del monitoreo de los factores necesarios en el sistema IoT agrícola, recolectando diferente información que puede ser usada en el análisis del estado del campo, y así contribuyendo al desarrollo del producto en cantidad y calidad (Said-Mohamed *et al*., 2021).

IoT se relaciona con las redes de sensores inalámbricas, la identificación de radiofrecuencia, cosas y redes donde sea y cuando sea, por eso es inevitable no tener problemas de ciberseguridad que deben ser resueltos para que los hackers no se aprovechen de los defectos y debilidades de los dispositivos y logren alterar la información o interrumpir el funcionamiento de los sistemas a través de la red global de IoT (Lu y Xu, 2019). Un aspecto critico de los desafíos que enfrenta IoT es la vulnerabilidad de los dispositivos en el despliegue de las redes 5G que se encuentra en desarrollo hoy en día, requiriendo estándares de seguridad específicos para asegurar la integridad y confidencialidad de los datos ya que 5G permite la transmisión de grandes volúmenes de información personal que pone en peligro la privacidad de los usuarios (Basurto-Guerrero y Guaña-Moya, 2023). Según Zainuddin *et al*. (2021) la disposición de confidencialidad de un sistema IoT se basa en el conocimiento de los riesgos de privacidad asociados con los dispositivos y servicios inteligentes que los rodean, el control individual sobre la recolección y procesamiento de datos sensibles por parte de estos dispositivos y el conocimiento y control sobre su uso y difusión por parte de terceros fuera de su ecosistema directo.

Las tecnologías utilizadas en la agricultura inteligente crean espacios vulnerables a ataques que perjudiquen el sistema productivo, como lo son ataques al flujo de los datos, a la red IoT y a los modelos de aprendizaje autónomo (Balaji *et al*., 2023). En la Tabla 1 se listan los tipos de ataques más comunes en sistemas IoT agrícolas, los dispositivos vulnerables y la capa de la arquitectura de tres capas que afecta directamente.

Tabla 1.

Ataques y dispositivos vulnerables en sistemas IoT agrícolas

Tipo de ataque	Dispositivos vulnerables	Capa objetivo
Ingeniería inversa	Sensores, drones	Percepción
Hombre en el medio	Sensores, dispositivos con comunicación M2M	Red
Suplantación de identidad	Router de WiFi, GPS	Red
Denegación de servicios	Puerta de enlace	Red
Inyección de datos falsos	Sensores, puerta de enlace, drones	Red y aplicación

Fuerza bruta para contraseñas	Router WiFi	Percepción y aplicación

Fuente: Balaji *et al*. (2023)

Dada la creciente necesidad de dar solución a los problemas de seguridad en IoT, en una revisión de 11 estudios Choo *et al*. (2021) dividieron la ciberseguridad estratégica en fases fundamentales que son: la clasificación, la detección, el análisis, el aseguramiento de la confidencialidad, integridad y disponibilidad de los datos. Varios métodos son implementados para garantizar que se consiga estratégicamente el aseguramiento de los sistemas en especial en IoT, como lo son los marcos con políticas de seguridad para la implementación de Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) que identifican oportunidades de negocio y crean valor organizacional, tomando como ejemplo el modelo el NIST CSF cuya implementación es en categorías con cuestiones técnicas, personas y procesos y cuenta con 5 funciones: 1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar; el OCTAVE Allegro que es el proceso de riesgos de seguridad informática con recursos limitados y cuenta con 4 funciones: 1. Establecer Dirección 2. Perfil de Activos 3. Identificar Amenazas 4. Mitigar amenazas; y también el Marco de referencia de seguridad Lubua que es la política de seguridad para asegurar la continuidad de negocios y se estructura en 7 categorías: 1. Seguridad de datos 2. Gobierno de servicios de red e Internet 3. Dispositivos usados por la compañía 4. Seguridad física 5. Reportes y manejo de incidentes 6. Monitoreo y Cumplimiento 7. Administración de políticas. (Espinosa-Garrido y Rosales-Roldan, 2022).

Dentro de los sistemas de la agricultura de precisión se conoce el concepto de Sistemas Físico-Cibernéticos (CPS, por sus siglas en ingles), que se conforma de la comunicación a través de la red de controladores con actuadores y sensores que actúan en un espacio discreto como un Sistema de Eventos Discretos (DES, por sus siglas en inglés) (Lima *et al*., 2018). En consecuencia, Oliveira *et al*. (2023) realizaron una clasificación de estrategias para DES en donde tuvieron en cuenta las características de la estrategia en sí misma, los tipos de ataques y el formalismo de modelado, concluyendo que con respecto a las investigaciones en estrategias el 61% se concentra en la protección en ataques pasivos, sin embargo, las relacionadas con ataques activos han tomado popularidad con una tendencia representativa. También el 73,8% abordan los modelos autómatas como las redes Petri. Por esto último, las estrategias algorítmicas son una tendencia entre aquellos que trabajan en el ámbito de la seguridad para la industria con sistemas robustos. En un mapeo sistemático Orozco Bonilla (2021) presenta algunas metodologías que evidencian un mejor nivel de protección de la información según una métrica como el Modelo entre Machine learning y Deep learning para detectar la intrusión con una exactitud del 99,9% de máquinas de vectores de soporte (SVM, por sus siglas en ingles), también está el lenguaje natural en la extracción de datos para determinar amenazas con un 83% de precisión y el modelo para seguimiento de intercambio de datos y medición del nivel de esfuerzo en ciberseguridad con un coeficiente de intercambio optimo.

En la agricultura inteligente con sistemas IoT usualmente los atacantes maliciosos se aprovechan de la pobre y descuidada configuración de los dispositivos y la red que no son considerados de importancia crítica para los agricultores, es por eso que profesionales en ciberseguridad que realizan auditorías externas siguen metodología de Hacking Ético con pruebas de penetración que sigue la estructura de reconocimiento, escaneo, hackeo, recolección de datos y elaboración del informe (Yaacoub *et al*., 2023).

A partir de la aplicación de los métodos mencionados cualquiera que sea la necesidad del agricultor, Sarowa *et al*. (2023) proponen unas cuantas estrategias de mitigación aplicadas en

agricultura inteligente como lo son la integración de Protocolo de Transferencia de Hipertexto (HTTP, por sus siglas en inglés) pero incorporado con Seguridad de la capa de transporte (TLS, por sus siglas en ingles) y encriptación en los datos que transmiten los sensores para mejorar la seguridad de la capa física y la comunicación con el servidor, también un sistema basado en detección de anomalías mediante el uso de algoritmos de aprendizaje automático que pueden reducir incidentes como malfuncionamiento de sensores, secuestro de sistemas de robots y drones, deformación de imágenes de cámaras e infiltración de datos, además de la adecuada autenticación y control de acceso para mejorar la seguridad de la capa de aplicación asegurándole a los usuarios saber quién es quién y quién está permitido dentro del sistema.

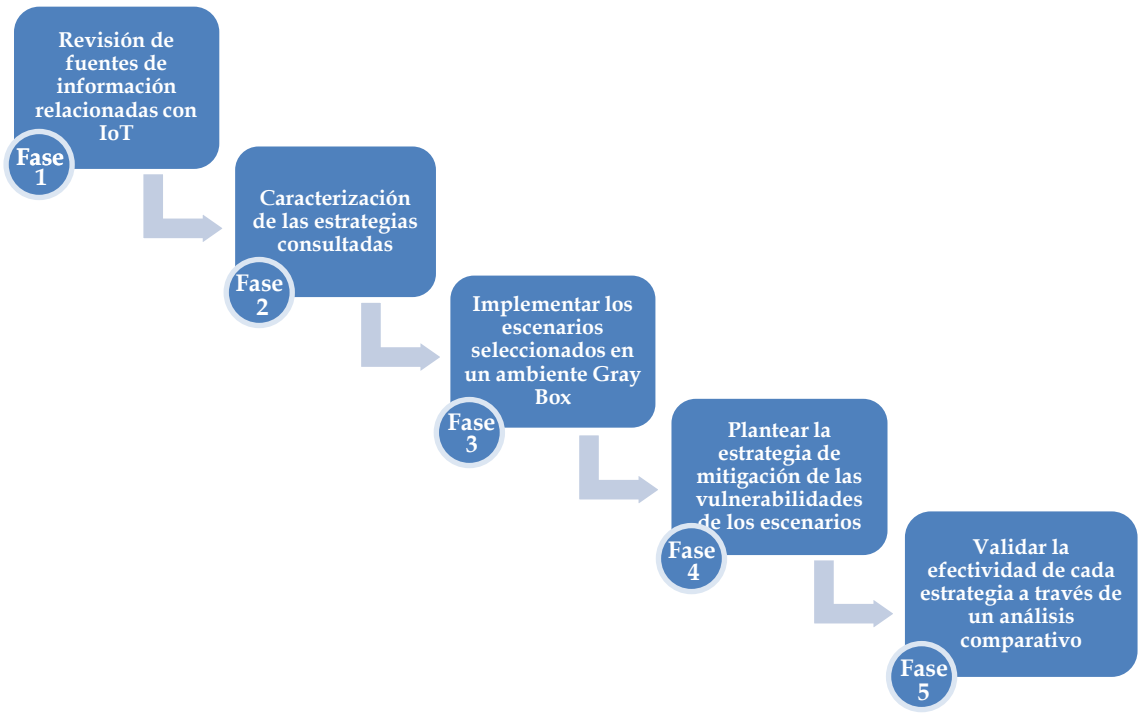
Dada la relevancia de la ciberseguridad en el IoT de los procesos agrícolas, metodologías de Ethical Hacking y la necesidad de generar conciencia de los retos y problemáticas que conllevan una transición tecnológica en países en desarrollo. Este enfoque incluye el planteamiento de escenarios de seguridad informática en sistemas IoT agrícolas con el fin de identificar y mitigar vulnerabilidades con información almacenada y en tránsito, desarrollar estrategias de seguridad informática para mitigar vulnerabilidades de la red y el servidor de un sistema IoT agrícola de la provincia del Sumapaz en Colombia.

2. Metodología

La metodología empleada para el proyecto fue cuantitativa con una muestra igual a la población de 43 dispositivos que componen el sistema IoT de un cultivo de café en la provincia del Sumapaz; el proyecto se estructura en cinco fases de trabajo descritas en la Figura 1:

Figura 1.

Metodología del proyecto



Fuente: Elaboración propia (2024).

2.1. Fase Uno: Revisión de fuentes de información relacionadas con IoT

Se realizó una revisión en artículos, documentos, bases de datos tales como Scopus, IEEE, Web of Science y Springer, además de otras fuentes gubernamentales y seguridad internacional que aportaron una mejor visibilidad de las vulnerabilidades y características desarrolladas en sistemas IoT, así como las principales estrategias que mitiguen efectos en la red y el servidor partiendo de las vulnerabilidades exploradas.

2.2. Fase Dos: Caracterización de las estrategias consultadas según su aplicabilidad y escalabilidad

Se clasificó la información obtenida al revisar fuentes de información discriminando por un máximo de 5 años la fecha de publicación y vulnerabilidades relacionadas con la arquitectura IoT; se realizó una caracterización que permitió seleccionar las estrategias con resultados más favorables en la mitigación de vulnerabilidades en entornos IoT. De esta forma se plantearon los criterios para los escenarios de hacking que representan el uso de dichas medidas de mitigación para su estudio.

2.3. Fase Tres: Implementar la simulación y el montaje de los escenarios seleccionados en un ambiente Gray Box

Al plantear los escenarios que representan una situación de debilidad sobre el estado del sistema, se realizó su implementación en un entorno Gray Box, el cual aporta un conocimiento parcial por parte del administrador del sistema, como sus direcciones IP, con el fin de llevar a cabo las pruebas, enfocadas a la red y el servidor del sistema IoT agrícola.

2.4. Fase Cuatro: Plantear la estrategia de mitigación de las vulnerabilidades de los escenarios

Al analizar la información proporcionada por las variables de estudio sobre los escenarios de hacking, se listan las vulnerabilidades encontradas y se plantean estrategias para mitigar, así como medidas de mejora del flujo de la red y de la seguridad del servidor.

2.5. Fase Cinco: Validar la efectividad de cada estrategia a través de un análisis comparativo

Se implementaron las estrategias y medidas de mejora propuestas para validar su eficacia y seguridad en el sistema. Finalmente, se replica las acciones de la fase 3 y se demuestra así la mitigación de las vulnerabilidades detectadas y la importancia del uso de la información adquirida previamente tras el estudio de este tipo de falencias y contramedidas en los sistemas IoT.

3. Resultados

Basado en los resultados de la exploración documental científica, técnica y tecnológica enfocado con sistemas IoT agrícolas, se propuso la implementación de los siguientes escenarios de pruebas se seguridad informática:

4.1. Primer Escenario: Ataque de Inyección SQL

En un periodo de 4 años, los ataques cibernéticos de inyección ocuparon el puesto tres entre los diez principales riesgos de seguridad con una tasa de incidencia máxima del 19%, entre estos encontrando la inyección SQL (Open Web Application Security Project [OWASP], 2022). Esta técnica puede ser utilizada para manipular las consultas SQL de una aplicación web lo que permite a los atacantes editar, ver o eliminar información de las bases de datos (Arteaga-Barragán y Balseca-Manzano, 2024). En el caso de IoT, que comparte una cantidad importante

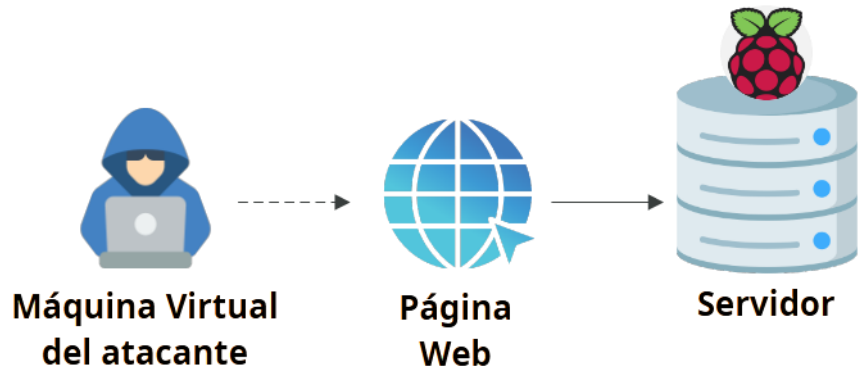
de datos a través de internet los ataques de inyección de código maliciosos en bases de datos relacionales son muy comunes (Quirumbay-Yagual *et al*., 2022). En el caso del sistema IoT agrícola descrito para este estudio se cuenta con el servicio web de gestión de base de datos MariaDB a través del navegador web y los datos de acceso del administrador. Se propone el primer escenario teniendo en cuenta un ambiente Gray Box que proporciona características del sistema como la dirección web de consulta a la base de datos. Este ataque se implementó haciendo uso de las herramientas, topología y metodología descritas en la Tabla 2:

Tabla 2.

Descripción, Herramientas, Topología y Metodología para el Ataque de Inyección SQL

<table>
<tr><td>Descripción</td><td colspan="2">Se ejecuta un ataque de inyección SQL a ciegas, que consiste en consultar a la base de datos valores de verdadero o falso y determinar la vulnerabilidad dependiendo de la respuesta con la herramienta sqlmap para la obtención de la tabla de usuarios y sus respectivas contraseñas.</td></tr>
<tr><td>Herramientas</td><td colspan="2">1. MariaDB, sistema de gestión de bases de datos relacionales.
2. Sqlmap, herramienta de software libre para automatizar ataques de Inyección SQL.
3. Virtual Box, software que ejecuta la máquina virtual.
4. Kali Linux, sistema operativo de la máquina atacante.</td></tr>
<tr><td>Topología</td><td colspan="2">La topología utilizada se puede apreciar en la Figura 2: Figura 2Figura 2.

Topología para el Ataque de Inyección SQL

Fuente: Elaboración propia (2024).</td></tr>
<tr><td rowspan="2">Metodología de Ethical Hacking descrita por (González-Pérez, 2023)</td><td>Fase de Reconocimiento</td><td>Primero se realiza la identificación de la dirección web del objetivo que se va a atacar. Esta nos permitirá acceder a la página de consulta de la base de datos insertando el enlace en la barra de búsqueda del navegador de la máquina del atacante, por ejemplo:
http://direcciónIP.php?id=número</td></tr>
<tr><td>Fase de Escaneo</td><td>Se envía un ID aleatorio en la URL para ver cómo se comporta la aplicación en circunstancias normales. Esto ayuda a establecer una base para el comportamiento esperado, por ejemplo, el</td></tr>
</table>

	número 2: http://direcciónIP.php?id=2 La respuesta debe ser positiva si el ID existe en la base de datos. Ahora para saber si la base de datos es susceptible al ataque se inserta una comilla simple (') después del número de ID, también se debe colocar un # al final de la consulta para comentar cualquier texto que el programa pueda agregar posteriormente. http://direcciónIP.php?id=2'# Si se produce un error o el comportamiento cambia, puede ser que la aplicación sea susceptible a la inyección SQL, así que se procede con el ataque con sqlmap.
Fase de Hacking	Para obtener las bases de datos del RDBMS se usa el comando <sqlmap -u direcciónIP.php?id=2 –dbs> El software lista los nombres de las bases de datos, posteriormente se identifica la que sea de interés. Para este caso es la única base de datos relacionada con el cultivo. Para conocer las tablas se usa el comando <sqlmap -u direcciónIP.php?id=2 –random-agent -level 5 -D [nombredelabd] --tables> Se despliega entonces la lista de tablas. Para ver las columnas de una tabla en específico se ejecuta el comando <sqlmap -u direcciónIP.php?id=2 –random-agent -level 5 -D [nombredelabd] -T [nombredelartabla] -columns> De nuevo se desplegará información, pero esta vez de la tabla seleccionada, como el nombre de las columnas y el tipo de variable. Como la tabla tiene una columna de usuarios y una de contraseñas, se pueden consultar de la siguiente forma <sqlmap -u direcciónIP.php?id=2 –random-agent -level 5 -D [nombredelabd] -T [nombredelartabla] -C [nombredelacolumna]> El software lista por última vez la columna consultada, visualizando entonces la lista de contraseñas que van asociadas relacionalmente a

los usuarios.

Fuente: Elaboración propia (2024).

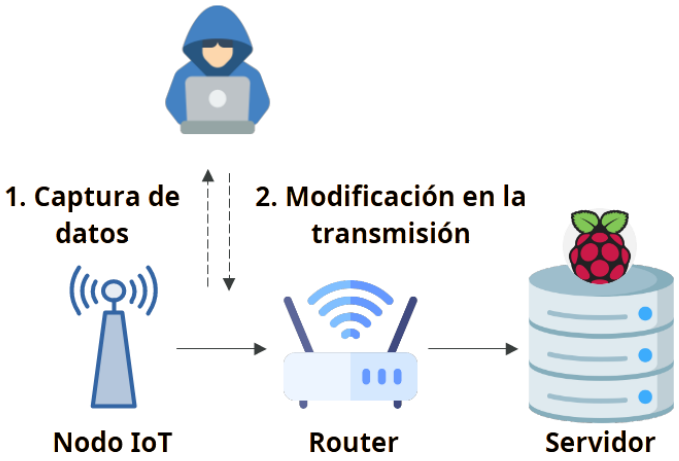
4.2. Segundo Escenario: Ataque Hombre en el Medio (MitM)

Como segundo escenario se seleccionó el ataque MitM, ello debido a que Bernaldo (2023) menciona como una de las técnicas de hacking más utilizadas entre los ataques de tipo intercepción de datos, situándose en el puesto catorce. Por otro lado, Grupo Atico34 (2023) menciona su influencia directa contra las bases de la seguridad informática, al contrarrestar la integridad y confidencialidad de los datos al ser interceptados y posteriormente modificados. Al ejecutarlo en un ambiente Gray Box, se dieron datos previos a su implementación, como la dirección IP prevista hacia la red del sistema, permitiendo así hacer uso de las herramientas, metodología y topología propuesta en la Tabla 3:

Tabla 3.

Descripción, Herramientas, Topología y Metodología para el Ataque Hombre en el Medio

Descripción	Ejecutar un ataque de Hombre en el Medio, ello en un ambiente compuesto por una conexión nodo hacia un router que transmite la información hacia el servidor. Este ataque se realiza específicamente entre la comunicación del Nodo y el router, donde se enfoca un ataque de tipo pasivo, obteniendo información transmitida entre estos dispositivos y de tipo activo, reteniendo los datos enviados, modificándolos y retransmitiéndolos hacia su destino
Herramientas	5. Nmap, herramienta para el análisis de la red. 6. Ettercap, herramienta para realizar el ataque de Hombre en el Medio. 7. Virtual Box, software que ejecuta la máquina virtual. 8. Kali Linux, sistema operativo de la máquina atacante. **9.** Wireshark, herramienta para realizar el ataque activo y comparar las alteraciones en los paquetes transmitidos.
Topología	La topología utilizada se puede apreciar en la Figura **3**: **Figura 3.** *Topología para el Ataque Hombre en el Medio*



Fuente: Elaboración propia (2024).

Metodología de Ethical Hacking descrita por (González-Pérez, 2023)	**Fase de Reconocimiento**	En esta fase se recolecta la información característica de la red IoT, como la asignación IP, la arquitectura utilizada, los protocolos de comunicación utilizados, los dominios DNS, etc. Para culminar esta fase, por medio de la herramienta Nmap se crea un listado de los dispositivos conectados a la red del sistema IoT, ello utilizando el comando: <nmap -sP [IP_Victima]> Donde [IP_Victima] hace referencia a la dirección de red del sistema seguida de su máscara de red.
	Fase de Escaneo	Por medio de la herramienta Nmap, se realiza un escaneo de puertos que permita identificar los puertos abiertos del sistema: <nmap -[IP_Victima]> Donde [IP_Victima] corresponde a la dirección IP asignada al dispositivo Nodo uno de los intermediarios para ejecutar el ataque. Esta información es adquirida como producto de la Fase de Reconocimiento.
	Fase de Hacking	Usando la herramienta Ettercap, se realizó una toma de los mensajes enviados entre el Nodo y el router con el fin de capturar los datos en ellos ejecutando un ataque pasivo, para ello se siguieron los pasos escritos a continuación: 1. Se da inicio al software Ettercap y se pulsa el menú "Aplicaciones". En el, se da click a "Kali Linux / Network

	Snooping / Poisoning / Ettercap-graphical". 2. Se selecciona la opción "Sniff / Unfied Sniffing". 3. Se utiliza la red conformada por el rango IP del sistema víctima. 4. Se selecciona "Hosts / Scan for Hosts" donde aparecerán los dispositivos conectados a ese rango de red. *5.* Por medio de "Add to TARGET1" se utiliza la IP del equipo víctima. *6.* Para hacer parte de la red atacada y evitar ser detectado se usa la opción "MITM / ARP Poisoning". Ello ejecutará la pantalla que integra "Sniff Remote Connections", se acepta para ejecutar "Start/Start Sniffing". 7. Se selecciona el equipo víctima y se ejecuta "ARP" que mostrará los equipos asignados al rango de la red 8. Por último, usando el comando: <sslstrip> Se convertirá la web segura en simple, lo que permite visualizar los datos encriptados. Para realizar el ataque activo, con el fin de capturar y modificar los paquetes transmitidos se implementa a Ettercap, la herramienta Wireshark. Retomando el estado del ataque pasivo: 1. Se selecciona la opción "Edit" del software Wireshark en el paquete donde se desea realizar la alteración y se realizan las respectivas modificaciones. 2. Una vez alterado, se utiliza "Save" y se da inicio en la herramienta Ettercap la opción "Plugins" 3. Se inicia la opción "Ettercap_ng" y se selecciona "Forward packets/ Manually specify packets to forward". Finalmente se seleccionan los paquetes modificados y se utiliza la opción "Forward".

Fuente: Elaboración propia (2024).

Al implementar los escenarios propuestos se obtuvo y sintetizó la información en la Tabla 4, donde se encuentran listadas las vulnerabilidades detectadas en cada uno de estos, una breve

descripción de las consecuencias de las debilidades en la seguridad y finalmente estrategias de mitigación que restauren la confidencialidad, integridad y disponibilidad de los datos expuestos en los ataques.

Tabla 4.

Resultados y Medidas de mitigación de los escenarios

Escenario		**Estrategias de mitigación**
Ataque de Inyección SQL		
Vulnerabilidad	**Descripción**	
Consulta y cambios a la base de datos por terceros	La inyección de código SQL depende en gran medida de la capacidad de un atacante para manipular las entradas de datos y funciones de la base de datos a través de una consulta web, logrando obtener información sensible y alterar la información de las tablas.	Aplicación de declaraciones preparadas y consultas parametrizadas. Utilizar procedimientos almacenados Establecer una lista de permitidos para definir entradas de usuario válidas, con las que la base de datos puede comprobar (y rechazar) las consultas Restringir el acceso de los usuarios a un nivel basado en funciones
Nula supervisión, validación y saneamiento de las entradas de usuario.	Dentro de la consulta se permite cualquier entrada de datos lo cual permite que las consultas sean inyectadas con código malicioso.	
Acceso con privilegios a todos los usuarios	Dentro de la base de datos cada usuario tiene el mismo nivel jerárquico por lo que puede realizar las mismas acciones que el administrador.	
Ataque Hombre en el Medio (Pasivo)		Cifrado de datos usando protocolos seguros como HTTPS. Implementación de métodos de autenticación seguros para comunicaciones Wi-Fi. Utilizar hashes para la verificación de los datos que son utilizados para la transmisión. Verificar los certificados SSL/TLS detectando su son válidos.
Vulnerabilidad	**Descripción**	
Cifrado de Datos	Al no utilizar un cifrado entre la comunicación de los dispositivos se puede fácilmente leer los datos transmitidos.	
Autenticación Débil	No implementar una autenticación o poseer una muy débil permite que cualquier dispositivo pueda acceder a la red y a sus datos.	
Carencias en los protocolos de transmisión	El uso de protocolos como HTTP involucra él envió de datos en texto plano, permitiendo una captura de datos más sencilla para cualquier atacante	
Configuración de red insegura	Uso de contraseñas por defecto o de configuraciones	

	predeterminadas permite accesos no autorizados.	Cambiar las configuraciones de los dispositivos por defecto y hacer uso de contraseñas con caracteres especiales, números y mayúsculas. Mantener el firmware del dispositivo Nodo y Router actualizado. Realizar monitorización de la red continuamente para la detección de anomalías en el sistema.
Ataque Hombre en el Medio (Activo)		
Vulnerabilidad	**Descripción**	
Falta de verificación de datos	La ausencia de una verificación de la integridad de los datos le permite al atacante realizar la modificación de estos alterando la veracidad de la información	
Suplantación de identidad	El atacante puede suplantar la identidad y redirigir el tráfico o acceder a datos importantes que son transmitidos	
No verificación de certificados	Al utilizar certificados como SSL/TLS permite que un atacante pueda hacer uso de credenciales falsos para la modificación del tráfico.	

Fuente: Elaboración propia (2024).

4. Discusión

La seguridad informática en sectores tecnológicamente emergentes o en transición a la industria 4.0 como el agrícola debe liderar un esfuerzo continuo y holístico que involucre a todos los actores. Los desarrolladores de sistemas IoT junto a la academia deben involucrar en sus diseños estándares reconocidos y prácticas de codificación seguras, además de la promoción de formación y capacitación. Los agricultores llegan a una brecha de retos y necesidades, no solo de conciencia, sino también educativas respecto a las amenazas, uso de contraseñas seguras y actualización del software.

Los protocolos ISO y TCP proporcionan un marco de referencia para normalizar la identificación de las vulnerabilidades y establecer estándares y controles de seguridad más precisos. La exploración de estas vulnerabilidades reveló que, a pesar de la diversidad de amenazas, existen patrones comunes que pueden ser mitigados mediante prácticas de seguridad bien establecidas.

Promover la educación en seguridad informática y establecer marcos normativos y regulatorios que garantices la protección de la confidencialidad, integridad y seguridad de los datos en la transición agrícola es una responsabilidad del gobierno y las entidades reguladoras.

El enfoque holístico de estrategias de ciberdefensa propuesto, que involucra la adopción de estándares, la implementación de prácticas de seguridad básicas, el uso de sistemas de detección y prevención, el cifrado de datos y la ofuscación, puede ayudar a mitigar las vulnerabilidades y proteger los cultivos de café del Sumapaz que le apuestan a la transición tecnológica.

5. Conclusiones

Las estrategias de seguridad informática de alcance transversal en el sistema IoT se constituye con el uso de controles y herramientas de seguridad tanto virtuales, enfocadas al software de los dispositivos; como físicas permitieron la creación de estrategias para la mitigación de las vulnerabilidades y amenazas en la red y el servidor del sistema IoT agrícola que implementan en cultivos de café en la provincia del Sumapaz.

Utilizar metodologías de Ethical Hacking para la ejecución de escenarios de pruebas de seguridad informática basados en un ambiente Gray Box, permitió que medidas de las variables se enfocaran a los efectos de la confidencialidad, integridad y disponibilidad de los datos transmitidos por la red y almacenados en el servidor.

En un enfoque de inversión de recursos, las vulnerabilidades con mayor impacto en la transmisión y almacenamiento de datos desde los nodos IoT al servidor de frontera, se mitigaron con la implementación de controles basados en mejoras de configuración y el uso de cifrado.

La transición a la industria 4.0 por parte de sectores económicos relacionados con la agricultura en la región del Sumapaz crea oportunidades de crecimiento regional con la mejora en la producción y calidad del café apoyado en sistemas IoT que integren estrategias de seguridad informática.

Los escenarios dispuestos en el proyecto son escalables y replicables en sistemas IoT que implementen las mismas tecnologías. Aun así, quedan por fuera otros vectores y superficies de ataque que no hicieron parte del alcance del proyecto, tales como ataques de interfaz, obtención de firmware, servicios remotos, transmisión a la nube, entre otras.

La seguridad informática de infraestructura IoT debe ser una mejora continua y holística que permita una gestión de vulnerabilidades oportuna en una región que le apuesta a la transformación digital y el fortalecimiento económico.

6. Referencias

Arteaga-Barragán, A., y Balseca-Manzano, J. (2024). Estrategias para identificar y mitigar vulnerabilidades de inyección SQL en aplicaciones móviles Android: Revisión bibliográfica. *593 Digital Publisher CEIT*, *9*(3), 71-83. https://doi.org/10.33386/593dp.2024.3.2300

Balaji, S. R. A., Rao, S. P. y Ranganathan, P. (2023). *Cybersecurity Challenges and Solutions in IoT-based Precision Farming Systems*. 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 237–246. https://doi.org/10.1109/UEMCON59035.2023.10316154

Basurto-Guerrero, M. O. y Guaña-Moya, J. (2023). Cybersecurity in 5G networks: challenges and solutions. *Revista VICTEC*, *4*(7). https://doi.org/10.61395/victec.v4i7.114

Bernaldo, M. (2023). *Las 15 técnicas de hacking más comunes*. https://bit.ly/3S0hblW

Choo, K. K. R., Gai, K., Chiaraviglio, L. y Yang, Q. (2021). A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Computers & Security*, 102, 102136. https://doi.org/10.1016/J.COSE.2020.102136

Espinosa-Garrido, C. B. y Rosales-Roldan, L. (2022). *Marco de Referencia de Ciberseguridad para Dispositivos de IoT Usando la Tecnología de IDS*, pp. 210–215. https://doi.org/10.54808/CICIC2022.01.210

Farooq, M. S., Riaz, S., Abid, A., Umer, T. y Zikria, Y. Bin. (2020). Role of IoT Technology in Agriculture: A Systematic Literature Review. *Electronics*, *9*(2), 319. https://doi.org/10.3390/electronics9020319

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L. y Wang, X. (2021). Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE/CAA Journal of Automatica Sinica*, *8*(4), 718-752. https://doi.org/10.1109/JAS.2021.1003925

González-Pérez, P. (2023). *Ethical Hacking: Teoría y práctica para la realización de un pentesting* (3ª ed.). OxWORD.

Grupo Atico34. (2023). *Confidencialidad, integridad y disponibilidad (Tríada CID)*. https://bit.ly/45WQR1U

Lima, P. M., Carvalho, L. K., y Moreira, M. V. (2018). Detectable and Undetectable Network Attack Security of Cyber-physical Systems. *IFAC-PapersOnLine*, *51*(7), 179-185. https://doi.org/10.1016/j.ifacol.2018.06.298

Lu, Y. y Xu, L. Da. (2019). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Oliveira, S., Leal, A. B., Teixeira, M. y Lopes, Y. K. (2023). A classification of cybersecurity strategies in the context of Discrete Event Systems. *Annual Reviews in Control*, 56, 100907. https://doi.org/10.1016/j.arcontrol.2023.100907

Open Web Application Security Project. (2022). *OWASP Top 10 - 2021*. https://owasp.org/Top10/

Organización de las Naciones Unidas para la Alimentación y la Agricultura. (2018). *More people, more food, worse water? A global review of water pollution from agriculture*. https://bit.ly/4cFEN7s

Organización de las Naciones Unidas. (2019). *World population prospects 2019: Highlights*. https://bit.ly/45K0yjS

Orozco-Bonilla, C. A. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático* [Tesis de grado]. Universidad Politécnica Salesiana.

Quirumbay-Yagual, D. I., Castillo-Yagual, C., y Coronel-Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE*, *9*(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671

Said-Mohamed, E., Belal, A. A., Kotb Abd-Elmabod, S., El-Shirbeny, M. A., Gad, A. y Zahran, M. B. (2021). Smart farming for improving agricultural management. *The Egyptian Journal of Remote Sensing and Space Science*, *24*(3), 971-981. https://doi.org/10.1016/j.ejrs.2021.08.007

Sarowa, S., Kumar, V., Bhanot, B. y Kumar, M. (2023). *Enhancement of Security Posture in Smart Farming: Challenges and Proposed Solution*. Conferencia Internacional sobre Tecnologías de Inteligencia de Dispositivos, Computación y Comunicación (DICCT), 1-5. https://doi.org/10.1109/DICCT56244.2023.10110208

Singh, G. y Singh, J. (2023). *Transformative Potential of IoT for Developing Smart Agriculture System: A Systematic Review*. 4th International Conference on Communication, Computing and Industry 6.0 (C216), 1-6. https://doi.org/10.1109/C2I659362.2023.10430789

Sinha, B. B., y Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, 126, 169-184. https://doi.org/10.1016/j.future.2021.08.006

Yaacoub, J.-P. A., Noura, H. N., Salman, O., y Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, 3, 280-308. https://doi.org/10.1016/j.iotcps.2023.04.002

Zainuddin, N., Daud, M., Ahmad, S., Maslizan, M. y Abdullah, S. A. L. (2021). *A Study on Privacy Issues in Internet of Things (IoT)*. 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 96–100. https://doi.org/10.1109/CSP51677.2021.9357592

CONTRIBUCIONES DE AUTORES/AS, FINANCIACIÓN Y AGRADECIMIENTOS

Contribuciones de los/as autores/as:

Conceptualización: Gordillo-Gaitan, Alexander; **Software:** Suárez-Quintero, Dayana; Castillo-Fernández, María Camila **Validación:** Gordillo-Gaitan, Alexander; **Análisis formal:** Gordillo-Gaitan, Alexander; Suárez-Quintero, Dayana; Castillo-Fernández, María Camila; **Curación de datos:** Suárez-Quintero, Dayana; Castillo-Fernández, María Camila**; Redacción-Preparación del borrador original:** Suárez-Quintero, Dayana; Castillo-Fernández, María Camila; **Redacción-Re- visión y Edición:** Gordillo-Gaitan, Alexander; **Visualización:** Gordillo-Gaitan, Alexander; **Supervisión:** Gordillo-Gaitan, Alexander; **Administración de proyectos:** Gordillo-Gaitan, Alexander; **Todos los/as autores/as han leído y aceptado la versión publicada del manuscrito:** Gordillo-Gaitan, Alexander; Suárez-Quintero, Dayana; Castillo-Fernández, María Camila.

Financiación: Esta investigación recibió financiación de la Universidad de Cundinamarca.

AUTORES:

Alexander Gordillo-Gaitán:
Universidad de Cundinamarca.

Ingeniero electrónico, Magister en Ingeniería Electrónica con énfasis en Telecomunicaciones, con experiencia de 6 años como docente universitario e investigador líder en proyectos de telecomunicaciones, educación, ciberseguridad y seguridad informática en la Universidad de Cundinamarca y la Corporación Universitaria Minuto de Dios – UNIMINUTO, certificado como auditor, implementador y ejecutor de la norma ISO/IEC 27001, Ethical Hacking Certified Associate (EHCA).
agordillog@ucundinamarca.edu.co

Índice H: 2
Orcid ID: https://orcid.org/0000-0002-4757-6950
Google Scholar: https://scholar.google.es/citations?user=qEs6yEsAAAAJ&hl=es
ResearchGate: https://www.researchgate.net/profile/Alexander-Gordillo-Gaitan

Dayana Carolina Suárez-Quintero:
Universidad de Cundinamarca.

Estudiante de Ingeniería Electrónica y auxiliar de investigación para el proyecto de investigación "Estrategia de ciberseguridad para sistema IoT de medición de variables ambientales y su efecto en la roya del café (Hemileia Vastatrix) en cultivos de la provincia del Sumapaz (Cundinamarca – Colombia)"
dayanacsuarez@ucundinamarca.edu.co

Orcid ID: https://orcid.org/0009-0001-8208-7888
ReserchGate: https://www.researchgate.net/profile/Dayana-Suarez-Quintero

María Camila Castillo-Fernández:
Universidad de Cundinamarca.

Estudiante de Ingeniería Electrónica y auxiliar de investigación para el proyecto de investigación "Estrategia de ciberseguridad para sistema IoT de medición de variables ambientales y su efecto en la roya del café (Hemileia Vastatrix) en cultivos de la provincia del Sumapaz (Cundinamarca – Colombia)"
mcamilacastillo@ucundinamarca.edu.co

Orcid ID: https://orcid.org/0009-0003-3280-4695
ReserchGate: https://www.researchgate.net/profile/Maria-Castillo-166