

**IMPLEMENTACIÓN DE PRUEBAS DE PENETRACIÓN Y
EVALUACIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA
OSSTMM EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E
CXAYUCE JXUT, TORIBÍO, CAUCA, DURANTE EL SEMESTRE DE
2025.**

EDINSON MESTIZO Y DARLY TENORIO

CORPORACION UNIVERSITARIA COMFACAUCA UNICOMFACAUCA

INGENIERÍA DE SISTEMAS

SANTANDER DE QUILICHAO

10 DE MARZO DE 2025

**IMPLEMENTACIÓN DE PRUEBAS DE PENETRACIÓN Y EVALUACIÓN DE
SEGURIDAD MEDIANTE LA METODOLOGÍA OSSTMM EN LA
INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E CXAYUCE JXUT TORIBIO
CAUCA.**

**PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE
INGENIERÍA DE SISTEMAS**

GIOVANI ANTONIO VILLALBA VERGARA

CORPORACION UNIVERSITARIA COMFACAUCA UNICOMFACAUCA

INGENIERÍA DE SISTEMAS

SANTANDER DE QUILICHAO

10 DE MARZO DE 2025

Tabla de contenido

1. RESUMEN.....	11
2. INTRODUCCIÓN	12
3. FORMULACIÓN DEL PROBLEMA	15
4. JUSTIFICACIÓN.....	17
5. OBJETIVOS.....	20
5.1. Objetivo General	20
5.2. Objetivo Específico.....	20
6. METODOLOGÍA.....	22
6.1. Tipo de estudio	22
6.2. Fases del trabajo	23
6.2.1. Fase interacciones previas al compromiso	23
6.2.2. Fase recolección de información	23
6.3. Fase de análisis de vulnerabilidades	24
6.3.1. Instrumentos O Herramientas Utilizadas	25
6.4. Alcances Y Limitaciones.....	28
6.4.1. Alcance	28
6.5. Fase de intervención	31
6.5.1. El procedimiento metodológico se desarrolló en las siguientes fases:	31

6.6. Informe de Hallazgos y Evaluación de Vulnerabilidades	33
6.6.1. Metodología de Evaluación	33
6.6.2. La metodología aplicada se estructuró en las siguientes fases:.....	33
6.7. Metodología de Presentación de Hallazgos	34
6.8. Metodología propuesta de mejora y plan de acción	35
7. MARCO TEÓRICO	37
8. MARCO CONTEXTUAL.....	41
9. MARCO LEGAL	42
9.1. Normativa Internacional	42
9.1.1. Estándar ISO/IEC 27001	42
9.1.2. Convenio de Budapest sobre Ciberdelincuencia	42
9.1.3 Convenio 108 del Consejo de Europa para la protección de las personas con respecto	43
9.2 NORMATIVA NACIONAL	43
9.2.1 Ley 1273 de 2009 Delitos Informáticos	45
10. ANTECEDENTES.....	46
10.1. Convenio 108 del Consejo de Europa para la protección de datos personal	48
10.2. Normativa Nacional	49
10.2.1. Ley 1273 de 2009 Delitos Informáticos.....	50
11. CAPÍTULO 1.	51

11.1 Identificar los activos críticos de la infraestructura tecnológica de la E.S.E Cxayuce	51
11.2. Para hacer el inventario, se utilizaron las siguientes herramientas	61
11.3. Procedimientos Aplicados	63
12. CAPÍTULO 2	64
12.1 Realizar un análisis de vulnerabilidades en la infraestructura tecnológica, ...	64
12.1.1. Metodología del análisis de vulnerabilidades	64
12.1.2. Herramientas utilizadas	65
12.1.3. Resultados preliminares.....	78
13. CAPÍTULO 3	80
13.1. Implementar la metodología OSSTMM (Open Source Security Testing Methodology	80
13.2. Metodología OSSTMM	80
13.3. Aplicación en la E.S.E. Cxayuce Jxut.....	80
14. CAPÍTULO 4	82
14.1. Evaluar el nivel de exposición y posibles riesgos asociados a cada vulnerabilidad	82
14.2. Aplicación de los Risk Assessment Values (RAVs)	83
15. CAPÍTULO 5	88
15.1. Generar un informe detallado que presente los hallazgos del test de penetración.	88
15.2. Metodología de Evaluación	89

15.3. Metodología de presentación de hallazgos a la E.S.E CXAYUCE JXUT.	90
15.3.1. Presentación de análisis de vulnerabilidades con Nessus.....	90
15.3.2. Descripción de hallazgo	96
15.3.3. Matriz de riesgo de la E.S.E CXAYUCE JXUT Toribio	98
15.3. Análisis comparativo del informe del pentesting en la E.S.E CXAYUCE JXUT	99
 16. CAPÍTULO 6	 103
 16.1. Establecer un plan de acción con propuestas de mejora para incrementar	 103
16.2. Acciones correctivas para la seguridad informática	103
16.3 Acciones Estratégicas para la seguridad informática	105
 17. RESULTADOS ALCANZADOS	 108
17.1. Identificación de activos críticos	108
17.2. Análisis exhaustivo de vulnerabilidades	108
17.3. Aplicación estructurada de la metodología OSSTMM	112
17.4. Evaluación del nivel de exposición y riesgos.....	113
17.4.1. Mapa integral de vulnerabilidades priorizadas	114
17.4.2. Indicadores cuantitativos de exposición mediante RAVs.....	114
17.4.5. Generación de un informe técnico con hallazgos y recomendaciones.	115
17.5. Diseño de un plan de acción para la mejora de la seguridad	117
 18. TRABAJOS FUTUROS	 119

19. RECOMENDACIONES	121
20. CONCLUSIONES.....	124
21. BIBLIOGRAFÍA.....	126
22. ANEXOS.....	130

Lista de Tablas

Tabla 1	Plan de actividades metodológicas para la aplicación de OSSTMM	29
Tabla 2	Detalle de Equipos de Cómputo y Software de la E.S.E. CXAYUCE JXUT	53
Tabla 3	Inventario de equipos de cómputo de la E.S.E. CXAYUCE JXUT	59
Tabla 4	Herramientas utilizadas en el test de penetración y su función principal.	72
Tabla 5	Explicación de los apartados de las métricas RAV (OSSTMM v3).....	84
Tabla 6	Clasificación de vulnerabilidades por nivel de riesgo en el servidor.....	91
Tabla 7	Clasificación de vulnerabilidades por nivel de riesgo en Contratación.....	91
Tabla 8	Clasificación de vulnerabilidades por nivel de riesgo en Cartera.....	93
Tabla 9	Clasificación de vulnerabilidades por nivel de riesgo en Contador.....	94
Tabla 10	Clasificación de hallazgos del test de penetración en la E.S.E Cxayuce Jxut ..	96
Tabla 11	Plan de acciones correctivas para la mitigación de vulnerabilidades	104
Tabla 12	Estrategias de fortalecimiento en ciberseguridad para	106

Lista de Ilustraciones

Ilustración 1 Distribución de tipo de ataque en sector salud.....	14
Ilustración 2 Respuesta de la propuesta presentada.	52
Ilustración 3 Instalación de Nmap.....	61
Ilustración 4 Escaneo activo de la red con Nmap en Kali Linux	62
Ilustración 5 áreas de trabajo.....	65
Ilustración 6 Distribución del tiempo de experiencia del personal en la institución.....	66
Ilustración 7 Frecuencia de cambio de contraseñas de acceso a los sistemas	66
Ilustración 8 Uso de la misma contraseña en múltiples sistemas o servicios.....	67
Ilustración 9 Conocimiento del personal sobre la existencia de una política de	67
Ilustración 10 Inducción recibida sobre el uso seguro de los sistemas informáticos.....	68
Ilustración 11 Recepción de correos sospechosos solicitando contraseñas o datos	69
Ilustración 12 Percepción del nivel de exposición de la institución frente a ataques	70
Ilustración 13 Participación en capacitaciones o talleres de seguridad informática	70
Ilustración 14 Conocimiento del procedimiento para reportar incidentes de seguridad .	71
Ilustración 15 Resultados del escaneo de vulnerabilidades con Nessus Essentials.	73
Ilustración 16 Resultados del escaneo de puertos y servicios con Nmap en el host	74
Ilustración 17 Registros A y MX obtenidos durante el análisis de subdominio.	75
Ilustración 18 Escaneo de puertos abiertos con Netcat en el host 192.168.0.247.....	75
Ilustración 19 Escaneo masivo de puertos con Masscan en el host 192.168.0.22.	76
Ilustración 20 Extracción de usuarios a partir de metadatos con FOCA.....	76
Ilustración 21 Visualización de relaciones y entidades con Maltego para la E.S.E.....	77
Ilustración 22 Calculadora RAV área SERVIDOR.....	87

Ilustración 23	Matriz de riesgo.....	99
Ilustración 24	clasificación de vulnerabilidades Nessus en el servidor	109
Ilustración 25	Vulnerabilidades por activos	110
Ilustración 26	Entrada hacia las instalaciones de la E.S.E. Cxayuce Jxut	130
Ilustración 27	Área de archivo y historias clínicas.....	130
Ilustración 28	Punto de distribución de red con cableado expuesto.....	131
Ilustración 29	cronograma de actividades	133
Ilustración 30	Constancia de cumplimiento de actividades del proyecto	134

1. Resumen

El aumento de ciberataques en el sector salud representa un riesgo significativo para la protección de datos sensibles y la continuidad de los servicios médicos. Este estudio evalúa la seguridad de la infraestructura tecnológica de la E.S.E. Cxayuce Jxut en Toribío, Cauca, mediante un test de penetración basado en la metodología OSSTMM, con el objetivo de estimar su nivel de seguridad y proponer estrategias de mejora.

El análisis comienza con la identificación de activos críticos a través de un inventario detallado de sistemas, redes y dispositivos. Luego, se realiza un análisis de vulnerabilidades con herramientas automatizadas y técnicas manuales para detectar debilidades explotables. La aplicación estructurada de OSSTMM evalúa redes, sistemas, servicios y aplicaciones, proporcionando un diagnóstico preciso del estado de seguridad.

Los hallazgos se presentan en un informe que categoriza los riesgos y ofrece recomendaciones para su mitigación. Además, se diseña un plan de acción con políticas de seguridad, controles técnicos y procedimientos de respuesta ante incidentes, fortaleciendo la resiliencia de la institución frente a ataques cibernéticos.

Este estudio optimiza la seguridad hospitalaria, protege la información crítica, fortalece la capacidad técnica del personal y garantiza la continuidad operativa de la E.S.E. Cxayuce Jxut, beneficiando la confianza y seguridad de la comunidad a la que presta sus servicios.

2. Introducción

En el contexto actual, el sector salud enfrenta grandes desafíos relacionados con la protección de su infraestructura tecnológica debido a la creciente digitalización y el aumento de ciberataques dirigidos a este ámbito. Las instituciones de salud manejan información altamente sensible, como datos médicos, administrativos y financieros, cuya protección es crucial para garantizar la confidencialidad, integridad y disponibilidad de los servicios ofrecidos a los pacientes. Sin embargo, la falta de medidas de seguridad adecuadas, especialmente en instituciones con recursos limitados, ha generado importantes riesgos que comprometen tanto la operatividad como la confianza de las comunidades atendidas.

La E.S.E. Cxayuce Jxut, ubicada en Toribío, Cauca, no es ajena a esta problemática. Como institución que presta servicios de salud a comunidades rurales e indígenas, enfrenta múltiples retos relacionados con la modernización de su infraestructura tecnológica y la implementación de sistemas de seguridad informática. Las vulnerabilidades en sus sistemas representan no solo un riesgo para la continuidad de los servicios, sino también para la privacidad y seguridad de la información médica de los pacientes.

Esta investigación se enfoca en evaluar la seguridad de la infraestructura tecnológica de la E.S.E. Cxayuce Jxut mediante la implementación de un test de penetración basado en la metodología OSSTMM (Open Source Security Testing Methodology Manual). Este enfoque permitirá identificar las principales debilidades en los sistemas, categorizar los riesgos y proponer soluciones prácticas que fortalezcan la resiliencia de la institución ante posibles ciberataques.

El estudio se enmarca en un enfoque cuantitativo, permitiendo un análisis técnico y sistemático de las vulnerabilidades, acompañado de herramientas automatizadas y técnicas manuales. A través de la identificación de activos críticos, la evaluación de riesgos y la generación

de un plan de acción, esta investigación no solo busca mejorar la seguridad de la E.S.E. Cxayuce Jxut, sino también establecer un modelo de buenas prácticas replicable en otras instituciones del sector salud.

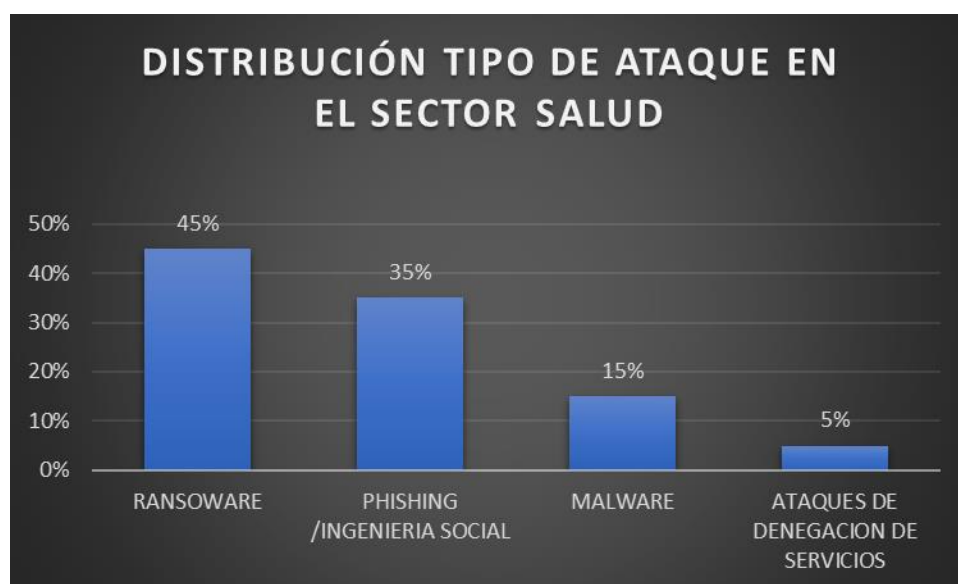
Por ejemplo, el dato más contundente es el porcentaje de afectación a nivel nacional: según reportes de **IBM**, aproximadamente el **60% de los ciberataques** dirigidos a Colombia en 2024 impactaron directamente al sector salud. Esto lo posiciona como el **sector más afectado del país**, superando a otros tradicionalmente sensibles como manufactura, transporte y gobierno.

La alta vulnerabilidad se confirma con la victimización de las instituciones:

- **Tasa de Víctimas:** Un alarmante **60% de las instituciones de salud** en Colombia ha sido víctima de ciberataques, según Latinpyme, lo que subraya la falta de infraestructura de defensa adecuada.
- **Tendencia de Crecimiento:** La amenaza se agrava con el tiempo, pues se registró un **aumento del 45%** en los ciberataques contra entidades prestadoras de servicios de salud (como Keralty o el Invima) entre 2022 y 2023.

Los ciberdelincuentes se centran en el sector salud debido al valor de la información médica sensible y la necesidad crítica de mantener la continuidad operativa. Por ello, los ataques que causan la mayor disrupción son los más comunes:

Ilustración 1 *Distribución de tipo de ataque en sector salud.*



Fuente: Elaboración propia

Nota. Esto demuestra que el cibercrimen explota la vulnerabilidad del personal para acceder a los sistemas. Es crucial invertir en capacitación continua y copias de seguridad para proteger el sector salud.

Con este proyecto se pretende contribuir al fortalecimiento de la infraestructura tecnológica de la institución, garantizando la protección de los datos de los pacientes, la continuidad operativa y la confianza de las comunidades atendidas. De esta manera, la investigación se alinea con los estándares internacionales y las normativas nacionales de seguridad informática, promoviendo un entorno seguro y confiable para la prestación de servicios de salud en el país.

3. Formulación del Problema

El sector hospitalario enfrenta desafíos crecientes en ciberseguridad debido a la digitalización y la dependencia de tecnologías para la gestión de información. En este contexto, el hospital Cxayuce Jxut, ubicado en Toribío, Cauca, presenta deficiencias en su infraestructura tecnológica, lo que compromete la seguridad de los datos de los pacientes y la eficiencia operativa. La escasez de recursos, la falta de capacitación en seguridad informática y la ausencia de un plan estructurado de ciberseguridad han generado vulnerabilidades críticas, exponiendo la información sensible a accesos no autorizados y ciberataques.

Aunque la institución ha implementado medidas básicas como controles de acceso y actualizaciones de software, estas han sido insuficientes para garantizar la integridad, confidencialidad y disponibilidad de los datos. La falta de una evaluación integral de la seguridad mediante metodologías especializadas impide identificar y mitigar riesgos de manera efectiva. Diversos estudios han demostrado la importancia de fortalecer la ciberseguridad en hospitales. Mora y Rodríguez (2022) analizan la vulnerabilidad de los hospitales ante ciberataques y sugieren estrategias de protección de datos en entornos hospitalarios. Por su parte, González (2021) estudia la implementación de metodologías de evaluación de seguridad en hospitales, destacando la efectividad de OSSTMM en la detección de vulnerabilidades.

En este sentido, la presente investigación busca evaluar la seguridad de la infraestructura tecnológica del hospital Cxayuce Jxut mediante la aplicación de OSSTMM, con el fin de identificar fallas y fortalecer la protección de la información. Se analizará el estado actual de la seguridad informática, se aplicarán pruebas de penetración y se diseñará un plan de acción para optimizar los mecanismos de protección. Resolver esta problemática permitirá mejorar la

privacidad de los pacientes, la eficiencia operativa del hospital y el cumplimiento de normativas como la Ley 1581 de 2012 sobre protección de datos personales en Colombia.

A partir de esta problemática, surge la pregunta de investigación: ¿Cómo contribuye la aplicación de un test de penetración basado en la metodología OSSTMM para mejorar la seguridad de la infraestructura tecnológica de la ESE Cxayuce Jxut?

4. Justificación

La seguridad informática en el sector salud es un aspecto crítico debido al manejo de información médica altamente sensible y la creciente digitalización de los servicios hospitalarios. En el caso de la E.S.E. Cxayuce Jxut, ubicada en el municipio de Toribío, Cauca, que presta atención a comunidades rurales e indígenas de Toribío y Jambaló, garantizar la protección de su infraestructura tecnológica es esencial para asegurar la continuidad operativa, la confianza de los pacientes y la integridad de los datos clínicos.

Esta investigación resulta conveniente pues busca identificar y evaluar los puntos más críticos dentro de la infraestructura tecnológica de la institución, aquellos que gestionan información médica, administrativa y financiera sensible. A través de un test de penetración selectivo, basado en la metodología OSSTMM (Open Source Security Testing Methodology Manual), se pretende detectar vulnerabilidades reales, clasificarlas por niveles de riesgo, y proponer estrategias de mitigación prácticas, ajustadas al contexto de la E.S.E. Cxayuce Jxut. Este proceso permitirá fortalecer la resiliencia tecnológica y prevenir interrupciones en la prestación de servicios esenciales.

Desde una perspectiva social, la investigación adquiere alta relevancia al contribuir directamente a la protección de los derechos de los pacientes, garantizando que su información esté resguardada y sea accesible únicamente por personal autorizado. La exposición o alteración de los datos clínicos no solo pone en riesgo la confianza institucional, sino que también puede generar errores en los tratamientos médicos, afectando gravemente la salud de los usuarios, especialmente en contextos rurales donde el acceso a servicios especializados es limitado.

A nivel práctico, este proyecto responde a una necesidad real de la institución, pues la falta de controles adecuados puede derivar en incidentes cibernéticos que comprometen la operatividad del hospital, su sostenibilidad y la calidad del servicio. Además, la ejecución del proyecto incluye actividades de formación y concientización para el personal de salud, promoviendo una cultura organizacional enfocada en la ciberseguridad.

En cuanto a su valor teórico, aunque el estudio tiene un enfoque aplicado, los resultados permitirán enriquecer el conocimiento sobre ciberseguridad en instituciones de salud rurales, aportando evidencia sobre las amenazas más frecuentes, sus causas y posibles soluciones. Esto podrá servir como base para futuros estudios o como referente para otras entidades en condiciones similares.

Metodológicamente, el uso de la OSSTMM adaptado a un entorno rural con limitaciones tecnológicas puede convertirse en un modelo útil y replicable. La experiencia desarrollada generará un plan de acción con propuesta de mejora que funcionarán como herramientas para otras instituciones del sector, aportando así una utilidad metodológica clara.

Finalmente, el proyecto es viable y factible, pues no requiere una intervención total de toda la infraestructura tecnológica, sino un análisis puntual en los sistemas más críticos. El estudio se llevará a cabo con herramientas automatizadas y técnicas manuales de bajo costo, aprovechando los recursos disponibles y el interés institucional en mejorar sus estándares de seguridad digital.

A nivel global, la urgencia de este tipo de investigaciones queda evidenciada por el aumento de los ataques informáticos en el sector salud. Según IBM, Colombia en 2024 recibió el 17% de los ciberataques en Latinoamérica, de los cuales el 60% afectaron al sector salud. Además, entre enero y noviembre de 2024, Colombia fue blanco de 36 mil millones de intentos de

ciberataques, siendo el sector salud uno de los más impactados. Esta tendencia confirma que los hospitales y centros médicos se han convertido en blancos prioritarios para los ciberdelincuentes, especialmente aquellos con escasos recursos, como también, el Foro Económico Mundial (2023), el promedio semanal de ataques dirigidos a instituciones de salud ha alcanzado los 1.684 incidentes, reflejando un incremento del 22% respecto al año anterior. Esta tendencia demuestra que los hospitales y centros médicos son objetivos cada vez más vulnerables, por lo que resulta urgente adoptar medidas preventivas para mitigar riesgos y garantizar la continuidad de los servicios como en el caso de la E.S.E. Cxayuce Jxut. Por tanto, esta investigación no solo es pertinente, sino fundamental para mitigar riesgos y garantizar un entorno seguro y confiable para la prestación de los servicios de salud en la región.

5. Objetivos

5.1. Objetivo General

- Desarrollar un test de penetración, implementando la metodología abierta de testeo de seguridad OSSTMM, con el fin de estimar el nivel de seguridad de la infraestructura tecnológica en las áreas más críticas de la E.S.E Cxayuce Jxut de Toribio Cauca.

5.2. Objetivo Específico

1. Identificar los activos críticos de la infraestructura tecnológica de la E.S.E Cxayuce Jxut de Toribio Cauca mediante un inventario exhaustivo de los sistemas, redes y dispositivos, con el fin de establecer los puntos clave de análisis en el test de penetración.
2. Realizar un análisis de vulnerabilidades en la infraestructura tecnológica, utilizando herramientas automatizadas y técnicas manuales, para detectar debilidades que puedan ser explotadas por atacantes.
3. Implementar la metodología OSSTMM (Open Source Security Testing Methodology Manual) para llevar a cabo pruebas de penetración estructuradas, cubriendo aspectos como seguridad en redes, sistemas, servicios y aplicaciones de la E.S.E Cxayuce Jxut.
4. Evaluar el nivel de exposición y posibles riesgos asociados a cada vulnerabilidad encontrada, categorizando su impacto y probabilidad de explotación para proporcionar un diagnóstico preciso del estado de seguridad.

5. Generar un informe detallado que presente los hallazgos del test de penetración, orientado a la mitigación de vulnerabilidades y al fortalecimiento de la seguridad de la infraestructura tecnológica de la E.S.E Cxayuce Jxut.
6. Establecer un plan de acción con propuestas de mejora para incrementar la resiliencia ante posibles ataques, incluyendo políticas de seguridad, controles técnicos y procedimientos de respuesta ante incidentes.

6. Metodología

Esta investigación se desarrollará bajo un enfoque cuantitativo, el cual permitirá recolectar y analizar datos numéricos de forma objetiva para estimar el nivel de seguridad informática en la ESE CXAYUCE JXUT. Este enfoque es ideal para medir variables específicas, identificar patrones y evaluar el cumplimiento de prácticas de seguridad mediante indicadores concretos.

6.1. Tipo de estudio

El estudio es de tipo descriptivo y diagnóstico, pues busca caracterizar el estado actual de la seguridad informática en la institución, identificar fortalezas y debilidades, y establecer un punto de partida para futuras mejoras.

Como complemento, se aplicará la técnica de caja blanca, orientada específicamente al análisis de la infraestructura tecnológica (Lozano & Correa, 2020). Esta técnica permite acceder y revisar de manera directa las configuraciones internas de los equipos, servidores, redes y demás componentes del entorno informático. Su propósito es identificar vulnerabilidades técnicas, configuraciones inseguras, falta de actualizaciones, o carencias en los mecanismos de protección física y lógica de los sistemas. Al tratarse de una revisión detallada, este enfoque facilita detectar riesgos que pueden afectar la disponibilidad, integridad y confidencialidad de la información institucional

Este estudio se enmarca en una investigación aplicada y exploratoria, dado que busca evaluar el estado actual de la seguridad informática en la ESE CXAYUCE JXUT y proponer soluciones prácticas basadas en la metodología OSSTMM (open source security testing

methodology manual). Además, se emplea un enfoque cuantitativo, permitiendo el análisis técnico de vulnerabilidades junto con la evaluación del impacto en la infraestructura tecnológica.

6.2. Fases del trabajo

6.2.1. Fase interacciones previas al compromiso

En esta fase se realizan reuniones con las áreas de interés de la empresa y con los colaboradores del área de TI, en las cuales se socializa la propuesta formal del trabajo de grado. Dicha propuesta incluye la idea del proyecto, la formulación de la pregunta de investigación, los objetivos, el alcance, el cronograma, los entregables y un cuestionario diseñado para identificar los aspectos y objetivos que deben considerarse en la ejecución de la prueba.

6.2.2. Fase recolección de información

- Dentro de esta fase se recopila la mayor cantidad de información posible que permita desarrollar a cabalidad la actividad. Dentro de ella se identifica la siguiente información:
- Información organizacional: La **E.S.E Cxayuce Jxut**, ubicada en Toribío, Cauca, es una institución prestadora de servicios de salud orientada a la atención integral de la comunidad bajo principios de calidad, equidad y pertinencia cultural. Su infraestructura tecnológica interna, conformada por equipos administrativos, impresoras en red y un servidor de archivos, es fundamental para la gestión institucional, por lo que resulta clave garantizar su seguridad informática para proteger la confidencialidad, integridad y disponibilidad de la información.
- Identificación de activos humanos internos y externos: La identificación de activos humanos constituye un paso fundamental en el análisis de seguridad, pues permite

reconocer a las personas que interactúan con la infraestructura tecnológica de la E.S.E Cxayuce Jxut. En este contexto, se clasificaron como **activos humanos internos** al personal administrativo, asistencial y de soporte técnico que hace uso directo de los equipos y servicios de la red interna.

- **Inventario e identificación de activos de hardware y software:** En la red privada del área de TI de la **E.S.E Cxayuce Jxut** se identificaron como activos de **hardware** los equipos administrativos, el switch principal, impresoras en red y el servidor de archivos; y como activos de **software** los sistemas operativos, aplicaciones de ofimática, software de gestión interna y antivirus. Este inventario se consolidó en un archivo en formato Excel que contiene la especificación y tipo de equipo, sistema operativo, dependencia y antivirus correspondiente, con el propósito de identificar y revisar los recursos más críticos dentro de la infraestructura tecnológica y facilitar el análisis de seguridad.

6.3. Fase de análisis de vulnerabilidades

El análisis de vulnerabilidades tiene como objetivo identificar las principales debilidades presentes en los sistemas, equipos y aplicaciones evaluados, las cuales podrían ser aprovechadas por un atacante. La forma de detección varía según los componentes a probar; por ello, para el desarrollo de esta fase se definieron una serie de actividades clave:

- **Diseño del plan de pruebas:** se determina el alcance de la evaluación, las áreas involucradas y la información a recolectar.
- **Conformación del equipo responsable:** se asigna el personal encargado de ejecutar la prueba.

- **Selección de herramientas:** se listan los recursos técnicos y comandos que serán utilizados en el proceso de escaneo.
- **Configuración de las máquinas:** Se llevaron a cabo las configuraciones necesarias en la máquina maestra, incluyendo la instalación del ambiente virtual, los sistemas operativos requeridos y las herramientas de escaneo que serían utilizadas durante el análisis
- **Definición de objetivos:** se identifican y documentan las direcciones IP que serán analizadas.
- **Ejecución de pruebas:** Posteriormente, se procedió a realizar los escaneos sobre la red privada de la institución, en los días previamente establecidos para tal fin, con el propósito de identificar posibles vulnerabilidades en los equipos y servicios conectados.

6.3.1. Instrumentos O Herramientas Utilizadas

6.3.1.1. Entrevista:

Se llevará a cabo una sesión con la alta gerencia y los líderes del área de TI, en la cual se presentaron los aspectos a considerar para la realización de la prueba. Durante la reunión, se define con la institución el alcance, los objetivos, los resultados esperados, las direcciones IP habilitadas y el personal responsable de supervisar la ejecución de la actividad.

6.3.1.2. Cuestionario:

Como parte del proceso metodológico, se aplicó un cuestionario dirigido al personal de la E.S.E Cxayuce Jxut, con el fin de obtener información directa sobre las prácticas y percepciones

relacionadas con la **seguridad informática** dentro de la institución. Este instrumento permitió identificar el nivel de conocimiento y cumplimiento de las políticas de seguridad.

6.3.1.3. Máquina Virtual – VirtualBox 7.0.20

Es un software que permite crear máquinas virtuales, es decir, instalar y ejecutar diferentes sistemas operativos dentro de un mismo computador físico. De esta forma, en lugar de disponer de varias máquinas físicas, es posible contar con múltiples entornos en un solo equipo. Su uso facilita la creación de ambientes controlados para realizar pruebas de aplicaciones, ejecutar análisis de vulnerabilidades con distribuciones como Kali Linux y garantizar que dichas actividades no afecten directamente el sistema operativo principal donde se encuentra instalado VirtualBox.

6.3.1.4. Kali Linux 2024 x64

Es un sistema operativo orientado a la realización de auditorías de seguridad informática, que permite evaluar y poner a prueba la resistencia de equipos y sistemas frente a posibles vulnerabilidades. Se reconoce como una de las principales distribuciones utilizadas en el ámbito del **hacking ético**, dado que incorpora un amplio conjunto de herramientas diseñadas para ejecutar escaneos, pruebas de penetración y revisiones de brechas de seguridad presentes en infraestructuras tecnológicas.

6.3.1.5. Nmap

Es una herramienta de software utilizada para el escaneo de redes, que permite identificar información detallada como puertos abiertos o cerrados, equipos conectados, sistemas operativos y sus versiones, así como los filtros de paquetes o cortafuegos en uso. Mediante el uso de diferentes comandos y opciones, Nmap facilita la recolección de datos específicos de acuerdo con el tipo de análisis de seguridad que se requiera.

6.3.1.6. Nessus 10.8

Es un programa especializado en la detección de vulnerabilidades, disponible en tres modalidades de licencia: Nessus Essentials, Nessus Professional y Tenable.io. Su funcionamiento se basa en el uso de plugins que permiten identificar fallas de seguridad en diversos sistemas operativos y aplicaciones, ofreciendo reportes detallados que sirven de apoyo en auditorías de seguridad y pruebas de penetración.

6.3.1.7. Cupp

Es una herramienta utilizada en auditorías de seguridad informática para la **creación de diccionarios personalizados de contraseñas**. Su funcionamiento se basa en recolectar información básica de los usuarios, como nombres, apellidos, fechas de nacimiento, nombres de familiares, mascotas, gustos o hobbies, y con estos datos genera listas de posibles contraseñas que suelen ser usadas por las personas.

6.3.1.8. FOCA

Es una herramienta utilizada para la recolección de metadatos en documentos, imágenes y archivos publicados en internet o en redes internas. Permite descubrir información sensible como nombres de usuarios, versiones de software, rutas de sistemas y detalles técnicos que pueden representar vulnerabilidades.

6.3.1.9. Dmitry

(Deepmagic Information Gathering Tool) es una aplicación de código abierto enfocada en la recopilación de información sobre objetivos específicos. Puede realizar búsquedas de subdominios, correos electrónicos, puertos abiertos y servicios activos, facilitando la fase de reconocimiento en pruebas de seguridad.

6.3.1.10. Masscan

Es uno de los escáneres de puertos más rápidos disponibles. Permite analizar grandes rangos de direcciones IP en poco tiempo, identificando servicios activos y configuraciones de red expuestas. Su velocidad lo convierte en una herramienta clave para auditorías de gran escala.

6.3.1.11. Maltego

Es una herramienta de análisis forense y de inteligencia que facilita la visualización de relaciones entre personas, dominios, direcciones IP, correos electrónicos y redes sociales. Es ampliamente usada en investigaciones de ciberseguridad y en técnicas de OSINT (Open Source Intelligence).

6.3.1.12. Netcat

Conocida como la “navaja suiza de las redes”, es una herramienta que permite establecer conexiones entre equipos, enviar y recibir datos, y abrir puertos para pruebas. Se utiliza en auditorías de seguridad para verificar servicios, crear túneles de comunicación y explorar Configuraciones De Red.

6.4. Alcances Y Limitaciones

6.4.1. Alcance

Se realizó un único análisis de vulnerabilidades al segmento de la red privada del área de TI de la empresa en sus áreas más críticas, con el propósito de identificar las brechas de seguridad activas que pudieran comprometer la **confidencialidad, integridad y disponibilidad** de la información. Este proceso permitirá elaborar un informe detallado con los hallazgos encontrados y, a partir de ellos, formular un plan de acción orientado a mitigar los riesgos detectados y fortalecer la seguridad de la infraestructura tecnológica.

Tabla 1 *Plan de actividades metodológicas para la aplicación de OSSTMM*

Objetivo	Actividad	Instrumento	Producto A Obtener
Identificar los activos críticos de la infraestructura tecnológica de la ESE Cxayuce Jxut de Toribío Cauca.	Realizar un inventario exhaustivo de los sistemas, redes y dispositivos.	Lista de activos tecnológicos y mapeo de infraestructura.	Informe de activos críticos y puntos clave para la prueba de penetración.
Realizar un análisis de vulnerabilidades en la infraestructura tecnológica.	Aplicar herramientas automatizadas y técnicas manuales para detectar debilidades.	Escaneo de vulnerabilidades, pruebas de configuración y análisis de registros.	Lista de vulnerabilidades detectadas y nivel de criticidad.
Implementar la metodología OSSTMM para pruebas de penetración.	Ejecutar pruebas estructuradas en redes, sistemas, servicios y aplicaciones.	Metodología OSSTMM, herramientas de pentesting.	Resultados de pruebas de penetración con evidencia técnica.

Evaluar el nivel de exposición y riesgos de cada vulnerabilidad.	Categorización de impacto y probabilidad de explotación.	Evaluación cuantitativa mediante RAV.	Diagnóstico de seguridad con priorización de vulnerabilidades.
Generar un informe detallado con recomendaciones de mitigación.	Documentar hallazgos y elaborar estrategias de mejora.	Informe técnico con recomendaciones.	Documento de análisis y estrategias de seguridad.
Establecer un plan de acción para mejorar la resiliencia.	Definir políticas de seguridad, controles técnicos y respuesta a incidentes.	Plan de seguridad y lineamientos de acción.	Plan de acción para fortalecer la infraestructura tecnológica.

Nota. La tabla muestra la relación entre los objetivos, actividades, instrumentos y productos esperados en el marco de la evaluación de la seguridad tecnológica de la E.S.E. CXAYUCE JXUT de Toribío, Cauca, siguiendo la metodología OSSTMM.

Fase publicación de resultados La finalidad de esta fase es poder determinar el valor de las máquinas que pueden verse afectadas. El valor de la máquina se determina de acuerdo con la información contenida allí y que tan importante es para la entidad. Por consiguiente, las siguientes actividades son las que se ejecutaran:

- Descripción de los datos obtenidos durante la prueba

- Descripción de las brechas de seguridad existentes dentro de los activos probados.
- Diseño del plan de acción

6.5. Fase de intervención

Para la valoración de la exposición y los riesgos asociados a las vulnerabilidades en la infraestructura tecnológica de la E.S.E. Cxayuce Jxut, se adoptó como base la metodología **OSSTMM** (Open Source Security Testing Methodology Manual), reconocida internacionalmente por su enfoque sistemático y cuantitativo en la evaluación de seguridad.

6.5.1. El procedimiento metodológico se desarrolló en las siguientes fases:

- **Definición del riesgo bajo OSSTMM**

El riesgo fue concebido como la existencia de limitaciones en la presencia de seguridad que pudieran afectar negativamente a las personas, procesos, información sensible, reputación institucional o cumplimiento normativo.

- **Evaluación según dimensiones críticas de OSSTMM**

Cada vulnerabilidad identificada fue analizada en relación con las cuatro dimensiones críticas:

1. **Seguridad (Safety):** impacto en la integridad física y continuidad de procesos institucionales.
2. **Privacidad (Privacy):** exposición, filtración o uso indebido de datos sensibles.
3. **Practicidad (Practicality):** efectos en la eficiencia de procesos organizacionales.
4. **Usabilidad (Usability):** equilibrio entre accesibilidad y medidas de seguridad.

- **Aplicación de los Risk Assessment Values (RAVs)**

Se realizará el cálculo RAV como un indicador porcentual de exposición y resiliencia, integrando:

1. **Porosidad:** visibilidad, accesibilidad y confianza en los sistemas.
2. **Controles activos:** mecanismos de seguridad presentes (Clase A y Clase B).
3. **Limitaciones:** debilidades técnicas u organizacionales que reducen la efectividad de los controles.

Para ello se utilizaron herramientas como **Nmap** (escaneo de visibilidad y puertos abiertos), **Nessus/OpenVAS** (detección de vulnerabilidades), y análisis manual de políticas de autenticación, segmentación de red y configuraciones de seguridad.

- **Clasificación de los hallazgos**

Los riesgos fueron organizados en categorías:

1. **Vulnerabilidades:** fallos técnicos explotables.
2. **Debilidades:** deficiencias de gestión o usabilidad.
3. **Exposiciones:** datos sensibles o técnicos visibles públicamente.
4. **Preocupaciones:** incumplimiento de estándares o buenas prácticas.
5. **Anomalías:** comportamientos inesperados detectados en sistemas y redes.

- **Medición del nivel de seguridad real (Security Δ y RAV final)**

1. Se calculó el **Security Δ (Delta)**, que corresponde a la diferencia entre la seguridad esperada y la real.

2. Finalmente, se obtendrá el valor **RAV actual**, expresado en una escala de **0 a 100**, que permitió establecer el nivel objetivo de seguridad alcanzado por la E.S.E. Cxayuce Jxut, evidenciando brechas de protección y áreas críticas de mejora.

6.6. Informe de Hallazgos y Evaluación de Vulnerabilidades

6.6.1. Metodología de Evaluación

La seguridad de la información en el sector salud es un aspecto altamente sensible, debido a la naturaleza crítica de los datos que gestiona, como las historias clínicas electrónicas, los registros de pacientes y la información administrativa de la institución. En este contexto, la E.S.E. Cxayuce Jxut fue sometida a un test de penetración controlado, implementando la metodología **OSSTMM** (Open Source Security Testing Methodology Manual), cuyo objetivo principal es identificar vulnerabilidades, verificar su grado de explotación y proponer medidas de mitigación, bajo un marco ético y normativo.

6.6.2. La metodología aplicada se estructuró en las siguientes fases:

6.6.2.1. Reconocimiento

En esta fase inicial se realizó la recopilación de información sobre la infraestructura tecnológica, incluyendo servidores, estaciones de trabajo, sistemas operativos, software instalado y dependencias críticas. El propósito fue identificar el alcance del entorno tecnológico y descubrir posibles puntos de entrada.

- **Herramientas utilizadas:** *Nmap* permitió detectar hosts activos, puertos abiertos, versiones de servicios y sistemas expuestos en la red.

- **Resultados esperados de la fase:** conformar un mapa de la superficie de ataque inicial, que sirviera de base para las siguientes etapas.

6.6.2.2. Análisis de Vulnerabilidades

Con la información obtenida en el reconocimiento, se aplicaron herramientas automatizadas y técnicas manuales para escanear servidores, aplicaciones y redes en busca de configuraciones inseguras o vulnerabilidades conocidas. Esta fase permitió identificar tanto fallos técnicos como malas prácticas de gestión.

- **Herramientas utilizadas:** *Nessus, OpenVAS, Dumpster, Netcat.*
- **Resultados esperados de la fase:** generar un inventario detallado de vulnerabilidades clasificadas según impacto y probabilidad de explotación.

6.6.2.3. Explotación Controlada

Las vulnerabilidades detectadas fueron sometidas a pruebas de explotación controlada, con el fin de confirmar su existencia y medir el impacto real que podrían tener en la infraestructura.

- **Herramientas utilizadas:** Hydra (pruebas de fuerza bruta sobre servicios de autenticación), Masscan (escaneo masivo de red), FOCA (extracción de metadatos), Netcat (establecimiento de conexiones directas).
- **Resultados esperados de la fase:** validar qué vulnerabilidades podían ser aprovechadas en un ataque real y determinar el nivel de criticidad de cada una.

6.7. Metodología de Presentación de Hallazgos

Para garantizar un análisis claro y comprensible de los resultados, los hallazgos fueron clasificados en cinco apartados:

1. **Descripción del hallazgo:** identificación clara de la vulnerabilidad y del componente afectado (servidor, red, aplicación o usuario).
2. **Impacto potencial:** consecuencias que la explotación podría tener sobre la operación hospitalaria, la información clínica o la reputación institucional.
3. **Probabilidad de explotación:** facilidad con la que un atacante podría aprovechar la vulnerabilidad.
4. **Nivel de riesgo:** categorización final (bajo, medio, alto, crítico) resultante de la combinación de impacto y probabilidad.
5. **Recomendación:** propuesta de acciones técnicas, organizacionales o normativas para mitigar el riesgo.

Este esquema metodológico permitió priorizar los hallazgos y vincular cada uno de ellos con medidas concretas de mejora, alineadas con **normativas nacionales** (Ley 1273 de 2009, Ley 1581 de 2012, Decreto 1078 de 2015, Resolución 1995 de 1999) e **internacionales** (ISO/IEC 27001, ISO/IEC 27799, HIPAA y NIST).

6.8. Metodología propuesta de mejora y plan de acción

El proceso de evaluación en la E.S.E Cxayuce Jxut se fundamentó en la **metodología OSSTMM**, pero no solo como una guía teórica, sino como un esquema operativo que permitió organizar las pruebas, estandarizar los criterios de análisis y garantizar la reproducibilidad de los resultados.

A partir de los hallazgos obtenidos en las etapas anteriores, se diseñó un **plan de acción estructurado** que busca mitigar vulnerabilidades, reducir riesgos y fortalecer la infraestructura tecnológica de la E.S.E Cxayuce Jxut. Este plan contempló las siguientes líneas de mejora:

- **Fortalecimiento de políticas de seguridad:** actualización de normativas internas y definición de protocolos claros de control de acceso, uso de contraseñas seguras y segmentación de la red.
- **Mejoras técnicas en infraestructura:** aplicación de parches y actualizaciones en sistemas operativos y aplicaciones críticas; implementación de controles adicionales en firewalls, antivirus y sistemas de monitoreo.
- **Capacitación del personal:** desarrollo de talleres y campañas de concientización para el personal administrativo, asistencial y técnico en torno a buenas prácticas de ciberseguridad.
- **Monitoreo y auditoría continua:** establecimiento de un programa de revisiones periódicas con herramientas de detección de intrusos, escaneo recurrente de vulnerabilidades y auditorías internas.
- **Gestión de incidentes:** creación de un protocolo de respuesta ante incidentes de seguridad que permita actuar de manera rápida y efectiva en caso de ataques.

De este modo, la metodología aplicada permitió no solo identificar y clasificar riesgos, sino también traducirlos en un **plan de acción concreto**, garantizando la mejora continua de la seguridad informática de la institución, en concordancia con los lineamientos de la metodología OSSTMM.

7. MARCO TEÓRICO

En la era de la transformación digital, la seguridad informática se ha convertido en una necesidad estratégica para garantizar la protección de la información y la continuidad de los servicios, especialmente en sectores sensibles como la salud. La digitalización ha mejorado significativamente la eficiencia operativa de los hospitales al centralizar historias clínicas, optimizar procesos administrativos y facilitar la comunicación interna. Sin embargo, esta evolución tecnológica también ha generado nuevas amenazas, como el robo de datos, accesos no autorizados, ataques de ransomware y sabotajes informáticos, que ponen en riesgo tanto a las instituciones como a los pacientes.

La seguridad informática se concibe como el conjunto de medidas, técnicas y políticas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información (Stallings, 2022). Estos tres pilares también conocidos como la tríada CI resultan esenciales en entornos hospitalarios, donde la información médica es altamente sensible y su exposición puede afectar no solo la privacidad de los usuarios, sino también la calidad del tratamiento clínico. Según Whitman y Mattord (2021), la efectividad de una infraestructura digital depende del equilibrio entre protección técnica y gestión de riesgos, incluyendo la actualización de sistemas, la capacitación del personal y la implementación de controles de acceso adecuados.

Diversos estudios han evidenciado que los hospitales, especialmente aquellos ubicados en zonas rurales o con recursos limitados, son blancos frecuentes de ataques informáticos debido a sus vulnerabilidades estructurales. Health IT Security (2023) señala que el 75% de los hospitales en América Latina han sido objeto de intentos de ciberataques en los últimos tres años, lo cual refleja una tendencia preocupante que exige la adopción de mecanismos de defensa proactivos. En este contexto, herramientas de evaluación como los test de penetración se consolidan como

estrategias clave para identificar fallos en la seguridad antes de que sean explotados por agentes maliciosos.

Entre los métodos más reconocidos para realizar estas evaluaciones se encuentra la metodología OSSTMM (Open Source Security Testing Methodology Manual), propuesta por Pete Herzog (2020). Esta guía ofrece un marco sistemático para realizar pruebas de penetración sobre redes, sistemas, servicios, aplicaciones y aspectos humanos de la seguridad. A diferencia de otros enfoques más generalistas, OSSTMM permite adaptar sus procedimientos a contextos específicos, lo que la convierte en una opción viable para instituciones como la E.S.E. CXAYUCE JXUT, donde los recursos tecnológicos son limitados y la infraestructura presenta condiciones de vulnerabilidad.

La metodología OSSTMM, al ser de código abierto, promueve una cultura de evaluación objetiva y reproducible, fundamentada en cinco canales de evaluación: humana, física, wireless, telecomunicaciones y redes de datos. Al aplicarse correctamente, permite establecer indicadores medibles sobre el nivel de exposición a amenazas, la resiliencia del sistema y la eficacia de los controles implementados. Esta aproximación puede complementarse con herramientas como Nmap, OpenVAS y Metasploit, las cuales facilitan el descubrimiento de vulnerabilidades técnicas y permiten simular escenarios de ataque controlado con fines diagnósticos (Kaspersky, 2021).

No obstante, más allá de lo estrictamente técnico, es indispensable reconocer que la seguridad informática también es un proceso social y educativo. Las tecnologías no operan de manera aislada, sino que requieren de usuarios conscientes, capacitados y comprometidos con las buenas prácticas de seguridad. Por ello, este tipo de proyectos implica una dimensión pedagógica, orientada a fortalecer las competencias del personal que interactúa con los sistemas, a través de procesos de sensibilización, formación continua y apropiación tecnológica. Se busca, entonces, no

solo implementar controles técnicos, sino también promover una cultura organizacional basada en la prevención, la responsabilidad digital y la mejora continua.

En el caso de la E.S.E. CXAYUCE JXUT, este componente formativo resulta aún más relevante, ya que se trata de una institución que opera en contextos indígenas y rurales, donde la infraestructura tecnológica ha sido históricamente limitada y el acceso a formación especializada en ciberseguridad es escaso. La implementación de una estrategia de seguridad requiere, por tanto, adaptarse a las realidades sociales y culturales del territorio, incorporando prácticas que respeten la identidad comunitaria y reconozcan los saberes locales.

La información médica, en estos contextos, no solo representa datos clínicos, sino también una extensión del conocimiento ancestral y de la confianza depositada en el sistema de salud. Su protección, por tanto, debe abordarse con una perspectiva intercultural que considere la privacidad como un valor compartido y la tecnología como una herramienta al servicio del bienestar colectivo. Este enfoque favorece la apropiación institucional de la ciberseguridad como un derecho y una responsabilidad colectiva, en la cual cada actor técnico, administrativo o comunitario cumple un rol fundamental.

En conclusión, el análisis de la seguridad informática en entornos hospitalarios rurales exige una mirada integral que articule herramientas técnicas, metodologías estructuradas, procesos de formación y comprensión del entorno cultural. Solo mediante esta integración es posible desarrollar infraestructuras digitales resilientes, proteger eficazmente los datos sensibles y fortalecer la capacidad operativa de las instituciones de salud en territorios con condiciones adversas. La experiencia que se deriva de este proceso no solo contribuye a mejorar la seguridad de una institución particular, sino que también sienta las bases para un modelo replicable en otros

entornos similares, donde la tecnología, la educación y la cultura se entrelazan en defensa del derecho a la salud y la información segura.

8. MARCO CONTEXTUAL

La **E.S.E. CXAYUCE JXUT**, ubicada en Toribío Cauca, presta servicios de salud a comunidades indígenas y rurales en Toribío y Jambaló. Su infraestructura hospitalaria depende de sistemas digitales para la gestión de historias clínicas y procesos administrativos, sin embargo, presenta vulnerabilidades en seguridad informática que ponen en riesgo la protección de datos y la continuidad de los servicios.

El hospital enfrenta desafíos tecnológicos como el uso de software desactualizado, falta de control en accesos a la red, ausencia de políticas de seguridad y cuidado de auditorías en sistemas. Estos factores lo hacen susceptible a ciberataques, una amenaza creciente en el sector salud a nivel global.

A nivel normativo, el proyecto busca alinear la gestión de la seguridad de la información con regulaciones como la Ley 1581 de 2012 (protección de datos personales en Colombia), el Decreto 1078 de 2015 (seguridad digital en el país) y estándares internacionales como ISO/IEC 27001 e HIPAA.

Este estudio contribuirá a mejorar la seguridad digital del hospital, protegiendo los datos de los pacientes y fortaleciendo la infraestructura tecnológica para garantizar la calidad y continuidad en la prestación de los servicios de salud.

9. MARCO LEGAL

Las pruebas que se realizan sobre la infraestructura o el entorno de TI se conocen como **pentesting** o **pruebas de penetración**. Su finalidad es que las organizaciones puedan identificar sus fallos de seguridad y comprender las posibles consecuencias de estos, el pentesting permite a las empresas reducir riesgos, priorizarlos y establecer los controles adecuados para fortalecer su sistema de seguridad.

9.1. Normativa Internacional

9.1.1. *Estándar ISO/IEC 27001*

La norma ISO/IEC 27001 establece los requisitos para crear, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro del marco de los riesgos propios de cada organización. Esta norma proporciona lineamientos para aplicar controles de seguridad ajustados a las necesidades específicas de la entidad, garantizando medidas suficientes y proporcionales para la protección de los activos de información. Su aplicación busca fortalecer la confianza de las partes interesadas y asegurar la continuidad y resiliencia de los procesos organizacionales.

9.1.2. *Convenio de Budapest sobre Ciberdelincuencia*

Colombia depositó el instrumento de adhesión ante el Consejo de Europa el 16 de marzo de 2020. Es el tratado que obliga a los Estados parte a tipificar delitos informáticos, a cooperar internacionalmente en investigaciones respecto a crímenes en sistemas informáticos, accesos ilícitos, daños, etc. Esto les da respaldo internacional a medidas como pentesting autorizado para prevenir delitos y vulnerabilidades.

9.1.3 Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio para la Protección de Datos Personales)

Colombia ha reconocido la importancia del Convenio 108, y es mencionado como instrumento vinculante de protección internacional de datos.

Este convenio es uno de los primeros tratados internacionales jurídicamente vinculantes en materia de privacidad y tratamiento de datos personales. Permite que Colombia justifique normativas de protección de datos robustas, lo que incluye evaluaciones de seguridad como pentesting para garantizar cumplimiento.

9.2 NORMATIVA NACIONAL

El desarrollo de pruebas de penetración en el sector salud colombiano debe sustentarse en un marco legal robusto que garantice la protección de los datos, la seguridad de la información y la confidencialidad de los pacientes. En este contexto, diversas normas nacionales respaldan la implementación de metodologías de ciberseguridad, como el pentesting, en instituciones de salud.

En primer lugar, la **Ley 1273 de 2009**, expedida por el Congreso de la República, modificó el Código Penal e incorporó el bien jurídico denominado *protección de la información y de los datos*. Esta ley tipifica los delitos informáticos, tales como el acceso no autorizado, la interceptación de datos, el daño informático y la obstaculización ilegítima de sistemas de información, estableciendo sanciones que buscan proteger la confidencialidad, integridad y disponibilidad de los datos.

Por su parte, la **Ley 1581 de 2012** establece disposiciones generales para la protección de datos personales, garantizando derechos fundamentales como la privacidad y el habeas data. Su reglamentación, a través del **Decreto 1377 de 2013**, refuerza las medidas para el tratamiento seguro de información sensible, entre las que se incluyen los datos clínicos y hospitalarios.

De manera complementaria, la **Ley Estatutaria 1751 de 2015** (Ley Estatutaria en Salud) reconoce la historia clínica como información sensible y confidencial, obligando a las instituciones a garantizar su seguridad y restringiendo el acceso únicamente a personal autorizado. En concordancia, la **Resolución 1995 de 1999**, expedida por el Ministerio de Salud, regula la administración de historias clínicas, estableciendo directrices sobre su custodia, conservación y protección contra accesos indebidos.

En cuanto al marco de política pública, el **Decreto 1078 de 2015** (Decreto Único Reglamentario del sector TIC) integra la política de Gobierno Digital en Colombia, incluyendo lineamientos sobre ciberseguridad, gestión de riesgos y protección de infraestructuras críticas. Este decreto se articula con el **Conpes 3854 de 2016**, que formula la Política Nacional de Seguridad Digital, orientada a proteger servicios esenciales como el sector salud, fomentando la resiliencia institucional y la reducción de riesgos cibernéticos. Asimismo, el **Conpes 3701 de 2011** contribuye a esta visión estratégica, al plantear políticas de seguridad y defensa de la información frente a amenazas digitales.

En conjunto, estas disposiciones conforman un marco normativo sólido que respalda la realización de pruebas de penetración en la **E.S.E. Cxayuce Jxut**, garantizando que dichas prácticas se desarrollen dentro de un marco jurídico, ético y profesional, protegiendo la información sensible de los pacientes y fortaleciendo la seguridad digital en el ámbito hospitalario.

9.2.1 Ley 1273 de 2009 Delitos Informáticos

La normatividad colombiana en materia de seguridad digital se encuentra reglamentada por la **Ley 1273 de 2009**, expedida por el Congreso de la República de Colombia. Esta ley modificó el Código Penal e incorporó un nuevo bien jurídico denominado *protección de la información y de los datos*. Su propósito es preservar de manera integral los sistemas que utilizan las tecnologías de la información y las comunicaciones, además de establecer sanciones para las conductas que atenten contra la confidencialidad, integridad y disponibilidad de los datos, fortaleciendo así la seguridad digital en el país.

El manejo de información en el sector salud está regulado por diversas normativas nacionales e internacionales:

Ley 1581 de 2012 (Colombia): Protección de datos personales en el ámbito hospitalario.

Decreto 1078 de 2015: Reglas de seguridad digital en Colombia.

ISO/IEC 27001: Gestión de la seguridad de la información en instituciones.

HIPAA (Ley de Portabilidad y Responsabilidad de Seguros Médicos): Normativa de seguridad en salud a nivel internacional.

El cumplimiento de estas normativas es fundamental para mejorar la seguridad digital en la E.S.E. CXAYUCE JXUT y reducir los riesgos asociados a ciberataques.

10. ANTECEDENTES

En los últimos años, el sector salud ha sido uno de los más afectados por ciberataques, debido a la creciente digitalización de los servicios hospitalarios y al manejo de información médica altamente sensible. Según el Foro Económico Mundial (2023), los ataques a instituciones de salud han aumentado un 22% en comparación con el año anterior, alcanzando un promedio semanal de 1.684 incidentes. Esta situación ha generado la necesidad urgente de fortalecer las estrategias de ciberseguridad en los entornos hospitalarios, especialmente en aquellos con recursos limitados.

Diversos estudios han abordado esta problemática. Mora y Rodríguez (2022) realizaron un análisis sobre la vulnerabilidad de los hospitales frente a ciberataques, destacando la necesidad de implementar metodologías especializadas para proteger los datos clínicos. Por su parte, González (2021) evaluó el uso de OSSTMM como una herramienta efectiva en la detección de vulnerabilidades dentro de entornos hospitalarios, señalando que su aplicación estructurada permite realizar diagnósticos precisos del estado de seguridad.

En América Latina, los ataques cibernéticos a hospitales han sido recurrentes. Health IT Security (2023) reporta que el 75% de las instituciones de salud en la región han sido blanco de ciberataques en los últimos tres años, lo cual demuestra una clara tendencia de riesgo en este sector. En Colombia, IBM (2024) informó que el país fue blanco de 36 mil millones de intentos de ciberataques entre enero y noviembre, siendo el sector salud el más impactado con un 60% de estos ataques.

A nivel metodológico, existen múltiples enfoques para evaluar la seguridad de los sistemas informáticos. Entre ellos destaca la metodología OSSTMM (Open Source Security Testing Methodology Manual), propuesta por Herzog (2020), la cual permite realizar pruebas de

penetración estructuradas en redes, sistemas y aplicaciones. Esta metodología ha demostrado su efectividad al proporcionar un marco sistemático para identificar, clasificar y mitigar vulnerabilidades. Comparada con otros estándares como NIST (2022) o ISO/IEC 27001 (2022), OSSTMM se adapta mejor a contextos específicos con limitaciones tecnológicas, como es el caso de hospitales rurales.

Sin embargo, pese a los avances en el área, existe un vacío en la aplicación de este tipo de metodologías en contextos rurales e indígenas de Colombia, como es el caso de la E.S.E. CXAYUCE JXUT, ubicada en Toribío, Cauca. Esta institución enfrenta importantes brechas tecnológicas y de seguridad que aún no han sido exploradas en profundidad mediante estudios académicos. Por lo tanto, esta investigación busca cubrir ese vacío, aportando evidencia empírica sobre el estado actual de la seguridad informática en este tipo de entornos y proponiendo acciones concretas de mejora.

Complementando lo anterior, Galán Lucerón (2023) en su tesis Ciberseguridad en el ámbito sanitario realiza un análisis multidisciplinario sobre el estado actual de la ciberseguridad en el sector salud. A través de una revisión bibliográfica y el estudio de casos reales, identifica los riesgos más comunes, los costos asociados a los incidentes y las buenas prácticas para mitigarlos. Su enfoque también contempla la conciliación entre las TIC y la deontología médica, así como la normativa vigente, ofreciendo recomendaciones para aumentar la resiliencia de las instituciones sanitarias frente a las amenazas cibernéticas. Este estudio resulta pertinente para contextos como el colombiano, donde aún existen vacíos significativos en la implementación de estrategias de protección en entornos rurales e indígenas.

En el contexto colombiano, la ciberseguridad en el sector salud ha adquirido una relevancia crítica debido al notable incremento de ciberataques que comprometen tanto la confidencialidad

de los datos como la continuidad de los servicios médicos. Según la Revista Hospitalaria de la Asociación Colombiana de Hospitales y Clínicas (ACHC), en 2022 las denuncias por delitos informáticos aumentaron un 30% respecto al año anterior, y en 2023 se registraron más de 20.000 casos de hurto mediante medios informáticos en el país. Instituciones de salud como Salud Total, Invima, EPS Sanitas y Audifarma han sido víctimas de ataques de ransomware que afectaron significativamente sus operaciones. Este panorama evidencia la necesidad urgente de implementar medidas de seguridad digital robustas, alineadas con marcos regulatorios internacionales como el GDPR y la HIPAA, para proteger la información sensible y garantizar la sostenibilidad de los servicios de salud. Estas consideraciones son especialmente pertinentes para entornos rurales e indígenas en Colombia, donde las brechas tecnológicas y de seguridad son más pronunciadas.

La investigación de Alan Raúl Gavino Llagas (2018) se centra en analizar la auditoría en seguridad informática y su relación con la gestión de riesgos en el Hospital Regional de Huacho, Perú. Se empleó un diseño no experimental, transversal y correlacional, con un enfoque cuantitativo. Los resultados revelaron una correlación muy alta (0,936) entre ambas variables, indicando que una auditoría efectiva en seguridad informática está estrechamente vinculada con una gestión de riesgos eficiente en el hospital. Este estudio destaca la importancia de implementar auditorías de seguridad informática para identificar y mitigar riesgos, garantizando la confidencialidad, integridad y disponibilidad de la información en entornos hospitalarios.

10.1. Convenio 108 del Consejo de Europa para la protección de datos personal

Colombia ha reconocido la importancia del Convenio 108, y es mencionado como instrumento vinculante de protección internacional de datos.

Este convenio es uno de los primeros tratados internacionales jurídicamente vinculantes en materia de privacidad y tratamiento de datos personales. Permite que Colombia justifique normativas de protección de datos robustas, lo que incluye evaluaciones de seguridad como pentesting para garantizar cumplimiento.

10.2. Normativa Nacional

El desarrollo de pruebas de penetración en el sector salud colombiano debe sustentarse en un marco legal robusto que garantice la protección de los datos, la seguridad de la información y la confidencialidad de los pacientes. En este contexto, diversas normas nacionales respaldan la implementación de metodologías de ciberseguridad, como el pentesting, en instituciones de salud.

Por su parte, la **Ley 1581 de 2012** establece disposiciones generales para la protección de datos personales, garantizando derechos fundamentales como la privacidad y el habeas data. Su reglamentación, a través del **Decreto 1377 de 2013**, refuerza las medidas para el tratamiento seguro de información sensible, entre las que se incluyen los datos clínicos y hospitalarios.

De manera complementaria, la **Ley Estatutaria 1751 de 2015** (Ley Estatutaria en Salud) reconoce la historia clínica como información sensible y confidencial, obligando a las instituciones a garantizar su seguridad y restringiendo el acceso únicamente a personal autorizado. En concordancia, la **Resolución 1995 de 1999**, expedida por el Ministerio de Salud, regula la administración de historias clínicas, estableciendo directrices sobre su custodia, conservación y protección contra accesos indebidos.

En cuanto al marco de política pública, el **Decreto 1078 de 2015** (Decreto Único Reglamentario del sector TIC) integra la política de Gobierno Digital en Colombia, incluyendo

lineamientos sobre ciberseguridad, gestión de riesgos y protección de infraestructuras críticas. Este decreto se articula con el **Conpes 3854 de 2016**, que formula la Política Nacional de Seguridad Digital, orientada a proteger servicios esenciales como el sector salud, fomentando la resiliencia institucional y la reducción de riesgos cibernéticos. Asimismo, el **Conpes 3701 de 2011** contribuye a esta visión estratégica, al plantear políticas de seguridad y defensa de la información frente a amenazas digitales.

En conjunto, estas disposiciones conforman un marco normativo sólido que respalda la realización de pruebas de penetración en la E.S.E. CXAYUCE JXUT, garantizando que dichas prácticas se desarrollen dentro de un marco jurídico, ético y profesional, protegiendo la información sensible de los pacientes y fortaleciendo la seguridad digital en el ámbito hospitalario.

10.2.1. Ley 1273 de 2009 Delitos Informáticos

La normatividad colombiana en materia de seguridad digital se encuentra reglamentada por la **Ley 1273 de 2009**, expedida por el Congreso de la República de Colombia. Esta ley modificó el Código Penal e incorporó un nuevo bien jurídico denominado *protección de la información y de los datos*. Su propósito es preservar de manera integral los sistemas que utilizan las tecnologías de la información y las comunicaciones, además de establecer sanciones para las conductas que atenten contra la confidencialidad, integridad y disponibilidad de los datos, fortaleciendo así la seguridad digital en el país.

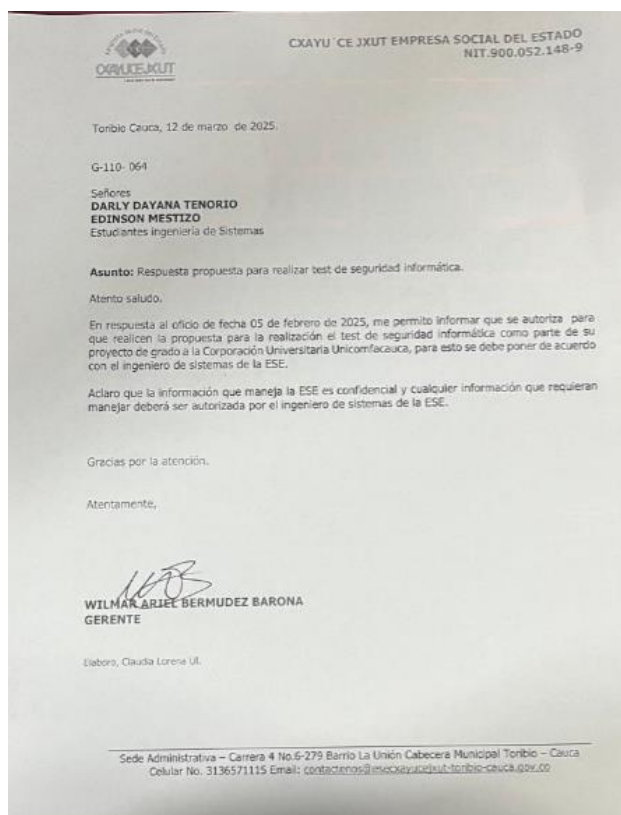
11. Capítulo 1.

11.1 Identificar los activos críticos de la infraestructura tecnológica de la E.S.E Cxayuce Jxut de Toribio Cauca mediante un inventario exhaustivo de los sistemas, redes y dispositivos, con el fin de establecer los puntos clave de análisis en el test de penetración.

En cumplimiento del primer objetivo específico, enfocado en la identificación de los activos críticos, se llevó a cabo un inventario exhaustivo de los sistemas, redes y dispositivos tecnológicos de la E.S.E. CXAYUCE JXUT. Esta etapa fue fundamental para establecer una línea base de los componentes más relevantes de la infraestructura, permitiendo delimitar los puntos clave que serían objeto de análisis durante el test de penetración.

Como primer paso en el desarrollo del proceso metodológico, se llevó a cabo un acercamiento formal con la entidad, cuyo objetivo fue presentar la propuesta del estudio de seguridad, detallando el alcance del mismo y compartiendo de manera clara los objetivos del test de penetración. Este encuentro permitió explicar cómo el proyecto busca contribuir al fortalecimiento de la seguridad tecnológica institucional. Dicha etapa, correspondiente a la fase de inducción de la metodología OSSTMM, resultó fundamental para generar confianza, asegurar la colaboración activa de la organización y obtener el acceso autorizado a la información necesaria para llevar a cabo el análisis. Finalmente, la propuesta fue aceptada de manera oficial por la dirección de la E.S.E. CXAYUCE JXUT, lo que dio luz verde al inicio de las actividades de identificación y análisis, contando desde ese momento con el respaldo institucional requerido.

Ilustración 2 Respuesta de la propuesta presentada.



Nota. Oficio emitido por la E.S.E. CXAYUCE JXUT, del municipio de Toribío, Cauca, el 12 de marzo de 2025, mediante el cual se autoriza a los estudiantes de Ingeniería de Sistemas la realización de un test de seguridad informática como parte de su proyecto académico.

Al recibir la aprobación, Posteriormente, se llevó a cabo la construcción del inventario bajo tres pilares fundamentales bajo un archivo Excel: **identificación, categorización y evaluación**. En la primera fase se registraron todos los equipos presentes (hardware, software, redes y dispositivos conectados), con el fin de comprender el entorno tecnológico de la organización. Luego, en la categorización, los activos fueron clasificados en grupos relevantes servidores, estaciones de trabajo, dispositivos de red y aplicaciones, lo que facilita su gestión y análisis. Finalmente, en la evaluación, cada equipo fue examinado según su nivel de criticidad,

vulnerabilidades potenciales, riesgos asociados y medidas de seguridad implementadas, permitiendo priorizar controles y acciones de mitigación.

Tabla 2 *Detalle de Equipos de Cómputo y Software de la E.S.E. CXAYUCE JXUT*

Descripción Pc	Tipo Pc	Dependencia	S.O.	Antivirus
procesador intel core i7 a 3,6 hz, ram 8 mb, disco duro 1tb, pantalla 22"	ESCRITORIO	SUBGERENCIA ADMINISTRATIVA	Sistema Operativo Windows 10	Kaspersky endpoint security
Slenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	PRESUPUESTO	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	CONTRATACIÓN	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	CARTERA	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- ultima gen 1tb ram 8gb amd a9-	TODO EN UNO	PERSONAL	Sistema Operativo Windows 10	Kaspersky endpoint security

9425 radeon r5 a 3,10 ghz				
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	CONTADOR	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	ALMACÉN	Sistema Operativo Windows 10	kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	GESTIÓN DOCUMENTAL	Sistema Operativo Windows 10	kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	SUBGERENTE CIENTÍFICO	Sistema Operativo Windows 10	kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	CONTROL INTERNO	Sistema Operativo Windows 10	kaspersky endpoint security
intel core i5 duo cpu t7200, 2,53 ghz, 4 gb ram, dd	ESCRITORIO	SISTEMAS	Sistema Operativo Windows 10	kaspersky endpoint security

320 gb, monitor 22"				
intel core i7 e7400 2,8 ghz, ram 2 gb, dd 320 gb, monitor lcd 22"	ESCRITORIO	SALUD OCUPACIONAL	Sistema Operativo Windows 10	kaspersky endpoint security
intel core i5 e7400 2,8 ghz, ram 2 gb, dd 320 gb, monitor lcd 22"	ESCRITORIO	4505	Sistema Operativo Windows 10	kaspersky endpoint security
intel core 2 duo 1,8 ghz, 1 gb ram, dd 160 gb, monitor 17"	ESCRITORIO	INGENIERO AMBIENTAL	Sistema Operativo Windows 10	kaspersky endpoint security
intel core 2 duo cpu t7200, 2,53 ghz, 2 gb ram, dd 320 gb, monitor 19"	ESCRITORIO	BIOMÉDICA	Sistema Operativo Windows 10	kaspersky endpoint security
intel core i5 cpu t7200, 2,53 ghz, 4 gb ram, dd 320 gb, monitor 22"	ESCRITORIO	ENLACE	Sistema Operativo Windows 10	kaspersky endpoint security
intel core i7 e7400 2,8 ghz, ram 2 gb, dd 320 gb, monitor lcd 22"	ESCRITORIO	PROGRAMAS	Sistema Operativo Windows 10	kaspersky endpoint security

dual core 2 duo 1,8 ghz, 1 gb ram, dd 160 gb, monitor 17"	ESCRITORIO	PIC	Sistema Operativo Windows 10	kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	FARMACIA	Sistema Operativo Windows 10	kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	FACTURACIÓN 1	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	FACTURACIÓN 2	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	FACTURACIÓN 3	Sistema Operativo Windows 10	Kaspersky endpoint security
dual core amd athlon 2,7 ghz, 1 gb ram, dd 160 gb, monitor 17"	ESCRITORIO	SIAU	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9-	TODO EN UNO	PRECONSULTA	Sistema Operativo Windows 10	Kaspersky endpoint security

9425 radeon r5 a 3,10 ghz				
intel core 2 duo cpu t7200, 2,53 ghz, 2 gb ram, dd 320 gb, monitor 19"	ESCRITORIO	PSICOLOGÍA	Sistema Operativo Windows 10	Kaspersky endpoint security
hp aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	ENFERMERÍA	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	PRENATAL	Sistema Operativo Windows 10	Kaspersky endpoint security
hp aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	CONSULTORIO 1	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	HOSPITALIZACIÓN	Sistema Operativo Windows 10	Kaspersky endpoint security
hp aio 22 a9 ultima gen 1tb ram 8gb amd a9-	TODO EN UNO	ODONTOLOGÍA	Sistema Operativo Windows 10	Kaspersky endpoint security

9425 radeon r5 a 3,10 ghz lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz Pentium dual core cpu e5400 2,7 ghz, ram 2 gb, dd 320 gb, monitor lcd 19" lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	VACUNACIÓN	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	ESCRITORIO	LABORATORIO	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz	TODO EN UNO	URGENCIAS CONSULTORIO	Sistema Operativo Windows 10	Kaspersky endpoint security
lenovo aio 22 a9 ultima gen 1tb ram 8gb amd a9- 9425 radeon r5 a 3,10 ghz pentium dual core cpu t4200, 2 ghz, 2 gb ram, portatil compaq presario cq40 14", dd 160 gb intel core i5, 2 ghz, 2 gb ram, portatil del 14", dd 500 gb intel core i5, 3,6 ghz, 8 gb ram, portatil del 15", dd 500 gb	TODO EN UNO	URGENCIAS ENFERMERÍA	Sistema Operativo Windows 10	Kaspersky endpoint security
intel core i5, 2 ghz, 2 gb ram, portatil del 14", dd 500 gb	PORTÁTIL	ASESOR JURÍDICO	Sistema Operativo Windows 10	Kaspersky endpoint security
intel core i5, 3,6 ghz, 8 gb ram, portatil del 15", dd 500 gb	PORTÁTIL	CALIDAD	Sistema Operativo Windows 10	Kaspersky endpoint security
	PORTÁTIL	ADMINISTRACIÓN	Sistema Operativo Windows 10	Kaspersky endpoint security

intel core i5, 3,6 ghz, 8 gb ram, portatil del 15", dd 500 gb	PORTÁTIL	ALMACÉN	Sistema Operativo Windows 10	Kaspersky endpoint security
servidor hp prolaint ml150	SERVIDOR	SISTEMAS	Sistema Operativo Windows Server 2003r2	Kaspersky endpoint security

Fuente: Elaboración propia.

Nota: Los datos de la tabla fueron obtenidos del archivo de Excel correspondiente al inventario de equipos realizado en las instalaciones de la E.S.E. CXAYUCE JXUT, en el municipio de Toribío, Cauca, durante el primer período del año 2025.

Tabla 3 *Inventario de equipos de cómputo de la E.S.E. CXAYUCE JXUT*

Equipos de computo	Cantidad
Desktop	12
Laptops	4
Servidores	1
Todo en uno	22
Routers	5

Fuente: Elaboración propia

Nota. La tabla presenta la cantidad y clasificación de los equipos de cómputo identificados en el inventario realizado en la E.S.E. CXAYUCE JXUT, a partir de la información consolidada en el archivo de Excel correspondiente.

Esta información nos proporciona una visión clara del entorno: cada equipo está asociado a su área correspondiente, lo que nos brinda un punto de partida sólido para identificar zonas críticas.

Para poder hacer un buen análisis de seguridad, lo primero que se debe tener claro es qué se quiere proteger. Por eso, este primer objetivo específico se enfoca en identificar los activos críticos que hacen parte de la infraestructura tecnológica de la E.S.E. CXAYUCE JXUT, ubicada en el municipio de Toribío, Cauca.

La identificación y clasificación de activos tecnológicos no solo constituyen el punto de partida del análisis de seguridad, sino que también se encuentran alineadas con lo establecido en la norma ISO/IEC 27001:2022, la cual permite a las organizaciones delimitar el alcance de su SGSI, priorizando recursos y concentrándose en aquellos activos, procesos o áreas de mayor relevancia estratégica (ISO, 2022). En este mismo sentido, Cane (2023) resalta que la gestión de activos de información ha sido fundamental en la planificación de la continuidad del negocio, la recuperación ante desastres y la preparación para la respuesta a incidentes, pues identificar sistemas, redes, bases de datos, aplicaciones, flujos de datos y otros componentes críticos que requieren protección constituye el primer paso para cualquier proceso de seguridad.

En el caso de la E.S.E. CXAYUCE JXUT, este enfoque resulta pertinente para definir la criticidad de los activos y orientar de manera precisa el test de penetración. Este paso no solo ayuda a planear las pruebas, sino que también da claridad sobre cuáles son los puntos más sensibles que se deben cuidar. Al trabajar con una entidad del sector salud, donde la información de los pacientes es delicada, es aún más importante tener esto bien organizado.

Para llevar a cabo este proceso se implementó la metodología OSSTMM (Open Source Security Testing Methodology Manual), un enfoque estructurado y reconocido internacionalmente para realizar pruebas de seguridad. Esta metodología divide las evaluaciones en diferentes áreas como seguridad humana, seguridad física, comunicaciones inalámbricas, seguridad de

telecomunicaciones y redes de datos, lo que permite un análisis completo y sistemático (PenTesting.Org, 2024).

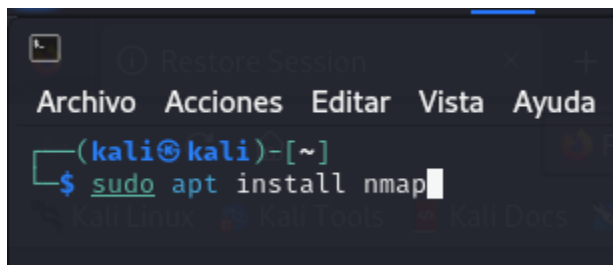
Dentro del marco de OSSTMM, esta etapa de identificación corresponde a la fase de reconocimiento y mapeo, donde se busca registrar todos los dispositivos y sistemas que se encuentran operativos en la red de la entidad. De esta forma, se construye una especie de “mapa digital” de toda la infraestructura tecnológica, el cual servirá de guía para las pruebas posteriores (Herzog, 2003, págs. 22–23).

11.2. Para hacer el inventario, se utilizaron las siguientes herramientas

Nmap: es un escáner de red que ayuda a detectar los equipos conectados y los servicios que están activos.

Como primer paso, se procedió a la **instalación de Nmap** mediante la terminal de Kali Linux, con el fin de realizar el escaneo de la red de la E.S.E. CXAYUCE JXUT.

Ilustración 3 *Instalación de Nmap*

A screenshot of a Kali Linux terminal window. The window has a dark background with a menu bar at the top containing 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. Below the menu bar, the prompt '(kali㉿kali)-[~]' is visible. The command '\$ sudo apt install nmap' is being entered at the prompt, with the cursor at the end of the line. The terminal also shows a 'Restore Session' button in the top left corner and some faint text at the bottom: 'kali Linux - Kali Tools - Kali Docs'.

Fuente: Elaboración propia

Nota. La ilustración fue obtenida directamente desde la terminal de Kali Linux durante el proceso de instalación de la herramienta Nmap.

El comando `sudo apt install nmap` se utiliza para descargar e instalar **Nmap** desde los repositorios oficiales de **Kali Linux**. El prefijo `sudo` otorga permisos de administrador para ejecutar la instalación, mientras que **apt** es el gestor de paquetes encargado de obtener y configurar el software. Este paso resulta indispensable para disponer de la herramienta dentro del entorno de auditoría y poder ejecutar los análisis de red posteriores.

Continuando con el uso de **Nmap**, se procedió a ejecutar el comando correspondiente para realizar un **escaneo activo de la red**, con el fin de identificar los dispositivos conectados dentro del rango de direcciones IP de la E.S.E. CXAYUCE JXUT.

Ilustración 4 Escaneo activo de la red con Nmap en Kali Linux

```

Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# nmap -sP -n 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 14:48 CET
Nmap scan report for 192.168.0.1
Host is up (0.0089s latency).
MAC Address: C4:E9:84:2B:89:96 (TP-Link Technologies)
Nmap scan report for 192.168.0.2
Host is up (0.00073s latency).
MAC Address: B8:69:F4:19:0F:5D (Routerboard.com)
Nmap scan report for 192.168.0.4
Host is up (0.0010s latency).
MAC Address: 9C:5A:44:8D:E9:BB (Compal Information (Kunshan))
Nmap scan report for 192.168.0.11
Host is up (0.0013s latency).
MAC Address: BC:EC:A0:3C:26:A8 (Compal Information (Kunshan))
Nmap scan report for 192.168.0.17
Host is up (0.00082s latency).
MAC Address: 9C:5A:44:8D:EA:C0 (Compal Information (Kunshan))
Nmap scan report for 192.168.0.22
Host is up (0.0015s latency).
MAC Address: 9C:5A:44:8D:EE:0D (Compal Information (Kunshan))
Nmap scan report for 192.168.0.39
Host is up (0.00079s latency).
MAC Address: 9C:5A:44:8D:EC:4C (Compal Information (Kunshan))
Nmap scan report for 192.168.0.40
Host is up (0.0015s latency).
MAC Address: 00:D8:61:9E:11:10 (Micro-Star Intl)
Nmap scan report for 192.168.0.42
Host is up (0.0025s latency).
MAC Address: 9C:5A:44:8D:EB:70 (Compal Information (Kunshan))
Nmap scan report for 192.168.0.44
Host is up (0.0013s latency).
MAC Address: 9C:5A:44:8D:EC:91 (Compal Information (Kunshan))
Nmap scan report for 192.168.0.63
Host is up (0.0056s latency).
MAC Address: E4:A8:DF:D7:8F:AD (Compal Information (Kunshan))
Nmap scan report for 192.168.0.71
Host is up (0.0020s latency).
MAC Address: D8:CB:8A:50:D7:B5 (Micro-Star Intl)
Nmap scan report for 192.168.0.72
Host is up (0.0014s latency).
MAC Address: 7C:4D:8F:07:79:78 (HP)
Nmap scan report for 192.168.0.78
Host is up (0.0034s latency).
MAC Address: B4:2E:99:80:09:6C (Giga-byte Technology)
Nmap scan report for 192.168.0.79
Host is up (0.00065s latency).
MAC Address: 98:29:A6:49:A8:8C (Compal Information (Kunshan))
Nmap scan report for 192.168.0.93

```

Fuente: Elaboración propia

Nota. La ilustración fue obtenida directamente desde la terminal de Kali Linux durante la ejecución del comando **nmap -sn 192.168.0.0/24**, el cual permite detectar 34 equipos activos en la subred analizada, mostrando sus direcciones IP y direcciones físicas (MAC).

El parámetro **-sn** indica a Nmap que realice un escaneo de descubrimiento de hosts (ping scan), es decir, identificar qué dispositivos se encuentran encendidos en la red sin necesidad de explorar los puertos. De esta manera, se obtiene una visión general de los equipos presentes en la infraestructura, lo que constituye un paso fundamental en la fase de reconocimiento.

Hojas de cálculo estructuradas: para organizar la información recolectada de forma clara.

11.3. Procedimientos Aplicados

Revisión interna: se hizo un primer acercamiento con el personal de sistemas para identificar los sistemas existentes y su uso.

Escaneo activo de la red: se usaron herramientas como Nmap para identificar dispositivos y servicios funcionando.

Organización del inventario: la información obtenida se organizó por tipo de activo, dirección IP, nombre del equipo, función y ubicación física.

Clasificación por criticidad: se determinó qué tan importante es cada activo para el funcionamiento de la E.S.E. CXAYUCE JXUT, dándole prioridad a los que manejan información de pacientes, servicios clínicos y sistemas de respaldo.

Verificación final: se validó la información con los responsables de cada área para confirmar que los datos eran correctos.

12. Capítulo 2

12.1 Realizar un análisis de vulnerabilidades en la infraestructura tecnológica, utilizando herramientas automatizadas y técnicas manuales, para detectar debilidades que puedan ser explotadas por atacantes.

Una vez identificados los activos tecnológicos más importantes de la E.S.E. CXAYUCE JXUT, el paso que sigue es revisar qué tan seguros están esos sistemas. Para eso se hace un análisis de vulnerabilidades, que consiste en buscar fallas o debilidades que podrían ser aprovechadas por una persona malintencionada para afectar la información o el buen funcionamiento de la entidad.

Este proceso combina el uso de herramientas automáticas con la aplicación de técnicas manuales. Es decir, no solo se emplean programas especializados que escanean los sistemas en busca de posibles vulnerabilidades, sino que también se realiza una revisión detallada de configuraciones, servicios y prácticas de seguridad, las cuales podrían representar riesgos operativos si no se gestionan adecuadamente.

Este enfoque integral permite obtener una visión más realista del estado de la infraestructura tecnológica, lo cual resulta especialmente relevante en entornos como el de la E.S.E. CXAYUCE JXUT, donde los recursos y el personal técnico especializado pueden ser limitados (Security Boulevard, 2024).

12.1.1. Metodología del análisis de vulnerabilidades

La metodología aplicada para el análisis de vulnerabilidades se desarrolló en cuatro fases principales: reconocimiento, descubrimiento, identificación de vulnerabilidades y análisis de resultados. En la fase de reconocimiento se emplearon herramientas OSINT (Dnsdumpster, Foca, Maltego) para recolectar información pasiva sobre la infraestructura. Posteriormente, en la fase de

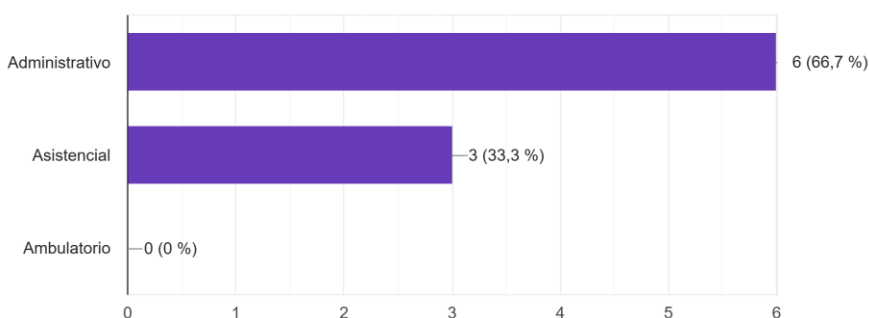
descubrimiento, se utilizaron Nmap, Masscan y Netcat para detectar hosts activos, puertos abiertos y servicios en ejecución. En la tercera fase se aplicó Nessus, complementado con validaciones manuales, para identificar y clasificar vulnerabilidades conocidas. Finalmente, se realizó una correlación de hallazgos utilizando Maltego y análisis manual, lo que permitió elaborar una visión integral del estado de seguridad de la infraestructura tecnológica de la E.S.E. CXAYUCE JXUT.

12.1.2. Herramientas utilizadas

Cuestionario: Este formulario fue diseñado para recopilar percepciones y prácticas del personal de E.S.E. CXAYUCE JXUT frente a la seguridad informática. Las respuestas obtenidas permiten identificar el nivel de conocimiento en el manejo de contraseñas, uso de equipos, acceso a información y medidas de protección implementadas, aportando insumos clave para el análisis de vulnerabilidades y la propuesta de mejoras en la infraestructura tecnológica.

Ilustración 5 áreas de trabajo

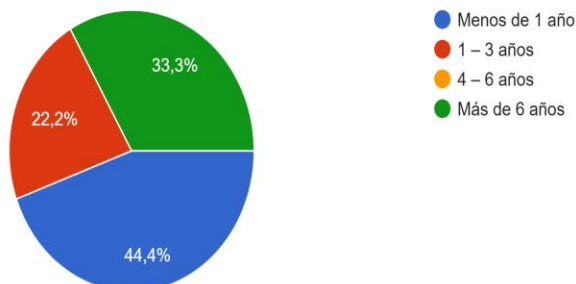
Área en la que trabaja:
9 respuestas



Nota. En el grafico representa el número de personas que laboran en el área Administrativa y Asistencial.

Ilustración 6 *Distribución del tiempo de experiencia del personal en la institución*

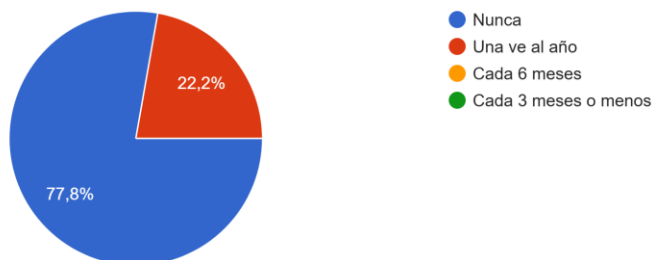
Tiempo de experiencia en la institución
9 respuestas



Nota. La gráfica muestra los resultados de la encuesta aplicada al personal de la E.S.E. Cxayuce Jxut, donde se observa que el 44,4% de los participantes tiene menos de un año de experiencia en la institución, el 22,2% cuenta con entre 1 y 3 años, y el 33,3% supera los 6 años de permanencia. No se reportaron respuestas en la categoría de 4 a 6 años.

Ilustración 7 *Frecuencia de cambio de contraseñas de acceso a los sistemas institucionales*

¿Con qué frecuencia cambia sus contraseñas de acceso a los sistemas institucionales?
9 respuestas

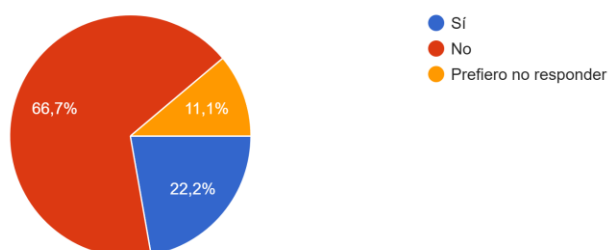


Nota. De acuerdo con los resultados de la encuesta, el 77,8% de los participantes indicó que nunca cambia sus contraseñas de acceso a los sistemas institucionales, mientras que el 22,2%

señaló que realiza esta acción una vez al año. No se registraron respuestas en las opciones de cambio cada seis meses o cada tres meses o menos, lo cual evidencia una práctica débil en la gestión de credenciales.

Ilustración 8 *Uso de la misma contraseña en múltiples sistemas o servicios*

¿Utiliza la misma contraseña para varios sistemas o servicios (Correo, Software institucional, Redes sociales)?
9 respuestas

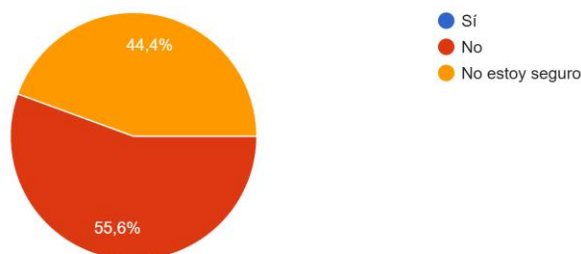


Nota. Los resultados de la encuesta muestran que el 22,2% de los encuestados reconoce utilizar la misma contraseña para varios sistemas o servicios (como correo, software institucional o redes sociales), mientras que el 66,7% afirma no hacerlo. Además, el 11,1% prefirió no responder. Este hallazgo refleja que, aunque la mayoría manifiesta aplicar buenas prácticas, aún existe un porcentaje significativo de usuarios que reutilizan contraseñas, lo que representa un riesgo de seguridad para la institución.

Ilustración 9 *Conocimiento del personal sobre la existencia de una política de seguridad informática documentada*

¿Conoce si la institución tiene una política de seguridad informática documentada?

9 respuestas



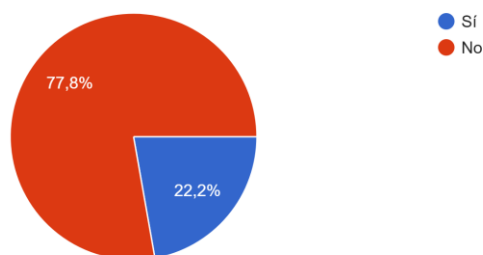
4

Nota. Según los resultados obtenidos, el 55,6% de los encuestados manifestó no conocer la existencia de una política de seguridad informática documentada en la institución, mientras que el 44,4% indicó no estar seguro. Ninguno de los participantes afirmó tener certeza sobre su existencia, lo que evidencia una brecha significativa en la comunicación y socialización de lineamientos de seguridad dentro de la organización.

Ilustración 10 *Inducción recibida sobre el uso seguro de los sistemas informáticos en la E.S.E.*

¿Ha leído o recibido alguna inducción sobre el uso seguro de los sistemas informáticos en la E.S.E.?

9 respuestas

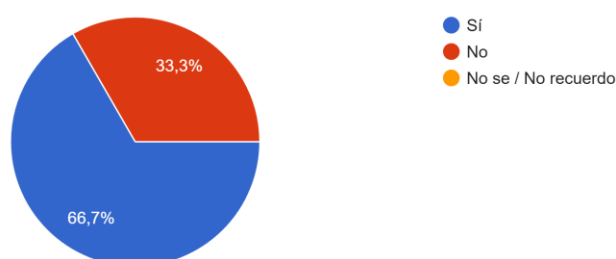


Nota. El 77,8% de los encuestados manifestó no haber recibido ni leído ninguna inducción relacionada con el uso seguro de los sistemas informáticos en la institución, mientras que

únicamente el 22,2% indicó que sí tuvo acceso a dicha información. Este resultado evidencia una carencia importante en los procesos de capacitación y sensibilización en seguridad informática, lo que incrementa la vulnerabilidad organizacional frente a posibles incidentes de seguridad.

Ilustración 11 *Recepción de correos sospechosos solicitando contraseñas o datos personales*

¿Alguna vez ha recibido un correo sospechoso que aparenta ser de un banco, entidad de salud u otro servicio, pidiéndole contraseñas o datos personales?
9 respuestas

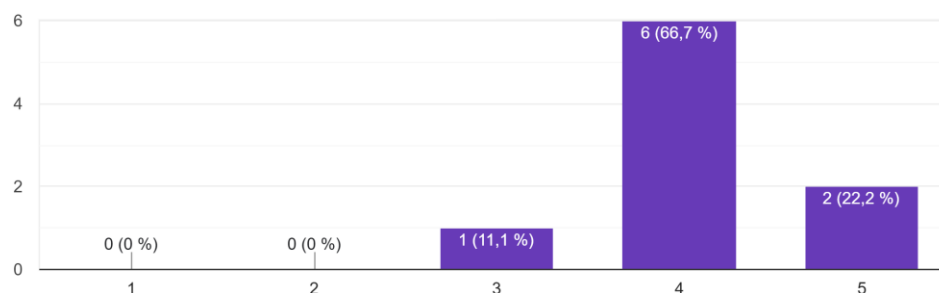


Nota. El 66,7% de los encuestados manifestó haber recibido alguna vez un correo sospechoso que aparentaba ser de un banco, entidad de salud u otro servicio solicitando contraseñas o información personal, mientras que el 33,3% indicó no haber tenido esta experiencia. No se registraron respuestas en la opción “No sé/No recuerdo”. Este resultado evidencia que la mayoría del personal ha estado expuesto a intentos de phishing, lo que subraya la necesidad de fortalecer la capacitación en el reconocimiento y manejo de este tipo de amenazas.

Ilustración 12 *Percepción del nivel de exposición de la institución frente a ataques informáticos*

En una escala de 1 a 5, ¿Qué tan expuesta considera que está la institución frente a los ataques informáticos? Ataque informático: Es cuando alg...dañar o bloquear información y servicios médicos.

9 respuestas

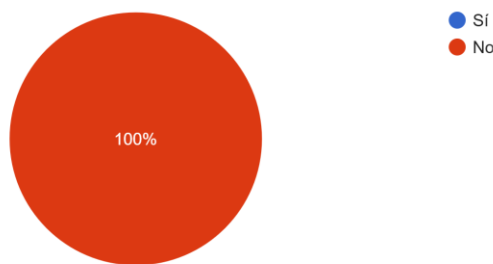


Nota. Según los resultados, el 66,7% de los encuestados considera que la institución está bastante expuesta a ataques informáticos (nivel 4 en la escala), mientras que el 22,2% la percibe en el nivel máximo de riesgo (5). Solo un 11,1% la ubicó en un nivel intermedio (3), y ninguno de los participantes seleccionó los niveles más bajos (1 o 2). Esto refleja una alta percepción de vulnerabilidad frente a incidentes que podrían dañar o bloquear la información y los servicios médicos.

Ilustración 13 *Participación en capacitaciones o talleres de seguridad informática en los últimos 12 meses*

¿Ha participado en capacitaciones o talleres de seguridad informática en la E.S.E. en los últimos 12 meses?

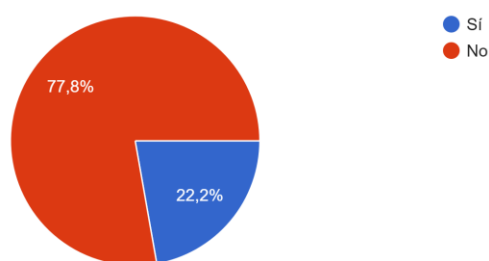
9 respuestas



Nota. El 100% de los encuestados manifestó no haber participado en capacitaciones ni talleres de seguridad informática en la E.S.E. durante el último año. Este resultado evidencia una falta de procesos de formación continua en temas de ciberseguridad, lo que representa una debilidad significativa para la institución al no fortalecer de manera periódica las competencias del personal frente a riesgos informáticos.

Ilustración 14 *Conocimiento del procedimiento para reportar incidentes de seguridad informática*

¿Sabe cuál es el procedimiento o a quién reportar si detecta un incidente de seguridad informática?
9 respuestas



Nota. El 77,8% de los encuestados indicó no conocer el procedimiento ni a quién reportar en caso de detectar un incidente de seguridad informática, mientras que solo el 22,2% afirmó tener claridad al respecto. Este hallazgo pone en evidencia una debilidad crítica en los protocolos de respuesta ante incidentes, lo cual podría retrasar la atención oportuna frente a un ataque informático y aumentar el nivel de riesgo para la institución.

Tabla 4 *Herramientas utilizadas en el test de penetración y su función principal.*

Herramienta	Función principal	Tipo
Virtual Box	Es un software de virtualización que permite crear y gestionar máquinas virtuales dentro de un mismo equipo físico.	Manual
Kali Linux	Es una distribución de Linux diseñada específicamente para seguridad informática, pruebas de penetración y análisis forense digital.	Automática/Manual
Hydra	Es una herramienta de auditoría de contraseñas diseñada para realizar ataques de fuerza bruta y de diccionario contra servicios de autenticación remota.	Automática/Manual
Cupp	Es una herramienta utilizada en auditorías de seguridad y pruebas de penetración para generar diccionarios personalizados de contraseñas.	Automática/Manual
Nessus	Escaneo de vulnerabilidades conocidas (CVE), clasificación por nivel de riesgo.	Automática
Nmap	Detección de hosts, servicios activos y puertos abiertos.	Automática/Manual
Dmitry	Recolección de información pasiva (DNS, WHOIS, subdominios).	Manual
	Conexión y manipulación de servicios en puertos abiertos.	Manual
Masscan	Escaneo masivo de puertos con alta velocidad.	Automática
dnsdumpster	Recolección de información de dominio y mapeo de red.	Manual
Foca	Descubrir información oculta en archivos, como nombres de autores, fechas de creación.	Automática
Maltego	Recolección y representación gráfica de datos	Automática

Fuente: Elaboración propia

Nota. La tabla presenta las principales herramientas empleadas en el proceso de análisis de seguridad, indicando su función principal y si su aplicación es automática, manual o híbrida.

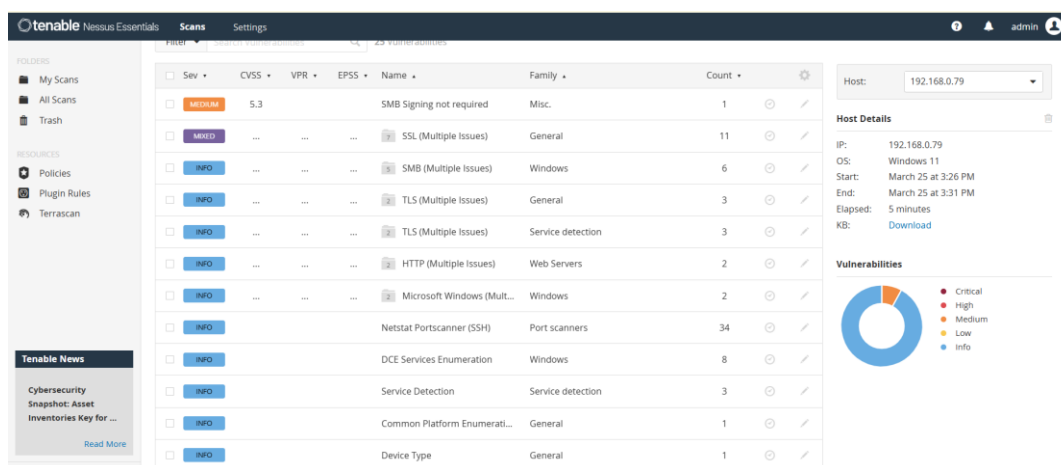
Para el desarrollo del análisis de vulnerabilidades y pruebas de seguridad, se seleccionaron diversas herramientas, tanto automáticas como manuales, con el fin de garantizar una cobertura amplia y precisa de la infraestructura tecnológica de la E.S.E. CXAYUCE JXUT. Estas

herramientas se eligieron siguiendo las recomendaciones de la metodología OSSTMM, la cual enfatiza la importancia de utilizar enfoques complementarios para obtener resultados más confiables.

En la Tabla 4 se presenta un resumen de las principales herramientas empleadas, su función dentro del proceso y el tipo de aplicación (manual, automática o mixta).

Nessus: permitió realizar un escaneo automatizado de vulnerabilidades conocidas (CVE), clasificándolas según su nivel de riesgo. Esta herramienta facilitó identificar rápidamente puntos débiles de los sistemas que podrían ser explotados por un atacante.

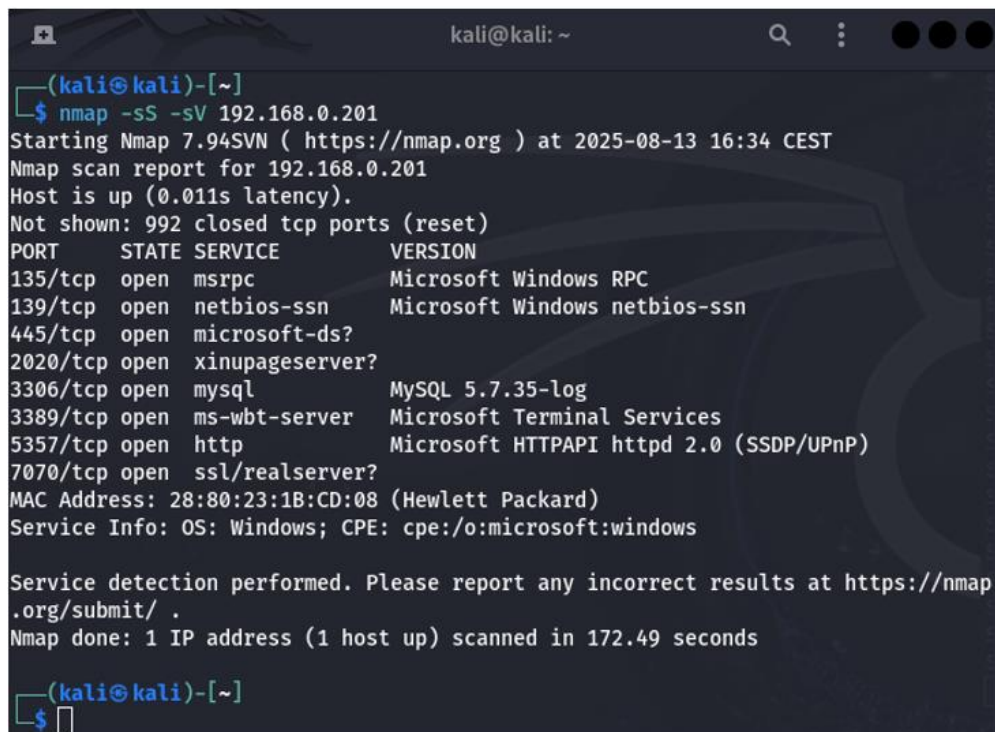
Ilustración 15 Resultados del escaneo de vulnerabilidades con Nessus Essentials.



Nota. La ilustración muestra las vulnerabilidades detectadas en el host analizado (192.168.0.79) clasificadas por nivel de severidad (crítico, alto, medio, bajo e informativo), junto con detalles del sistema operativo, servicios identificados y número de incidencias encontradas.

Nmap: Fue utilizado para la detección de hosts activos, puertos abiertos y servicios en ejecución. Su carácter mixto (manual y automático) hizo posible complementar los resultados con un análisis detallado, validando configuraciones específicas de red.

Ilustración 16 Resultados del escaneo de puertos y servicios con Nmap en el host 192.168.0.201.



```
(kali@kali)-[~]
$ nmap -sS -sV 192.168.0.201
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-13 16:34 CEST
Nmap scan report for 192.168.0.201
Host is up (0.011s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2020/tcp   open  xinu              xinu
3306/tcp   open  mysql            MySQL 5.7.35-log
3389/tcp   open  ms-wbt-server    Microsoft Terminal Services
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp   open  ssl/realserver?
MAC Address: 28:80:23:1B:CD:08 (Hewlett Packard)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.49 seconds

(kali@kali)-[~]
$
```

Nota. La ilustración presenta los puertos abiertos, el estado, los servicios asociados y, cuando fue posible, la versión identificada en el host 192.168.0.201. El análisis se realizó utilizando el comando `nmap -sS -sV`, que permite la detección de servicios y versiones activas en el sistema objetivo.

Dnseenum / Dnsdumpster: la recolección de información pasiva sobre dominios y subdominios asociados a la entidad, aportando datos relevantes sin necesidad de interactuar directamente con los sistemas (técnicas OSINT).

Ilustración 17 Registros A y MX obtenidos durante el análisis de subdominio.

A Records (subdomains from dataset)					
Host	IP	ASN	ASN Name	Open Services (from DB)	Rev
esecxayucejxut-toribio-cauca.gov.co	20.88.170.7	ASN 8875 20.64.0.0/10	MICROSOFT-CORP-MSN-AS-BLOCK United States	http: unknown server title: Object moved	401
MX Records					
10 aspmx2.googlemail.com	209.85.202.27	ASN 15169 209.85.202.0/24	GOOGLE United States		
5 alt1.aspmx.l.google.com	209.85.202.26	ASN 15169 209.85.202.0/24	GOOGLE United States		
10 aspmx3.googlemail.com	64.233.184.26	ASN 15169 64.233.184.0/24	GOOGLE United States		
5 alt2.aspmx.l.google.com	64.233.184.26	ASN 15169 64.233.184.0/24	GOOGLE United States		
10 aspmx4.googlemail.com	142.250.27.27	ASN 15169 142.250.27.0/24	GOOGLE United States		
10 aspmx5.googlemail.com	142.250.153.26	ASN 15169 142.250.153.0/24	GOOGLE United States		

Nota. La figura muestra los registros de tipo A (resolución de nombres de dominio a direcciones IP) y MX (servidores de correo) asociados al dominio esecxayucejxut-toribio-cauca.gov.co, identificando direcciones IP, rangos de red (ASN), proveedores de servicio y puertos relacionados.

Netcat: se aplicó como herramienta manual para la conexión y manipulación de servicios en puertos abiertos, permitiendo comprobar de manera práctica el nivel de exposición de determinados equipos o servicios.

Ilustración 18 Escaneo de puertos abiertos con Netcat en el host 192.168.0.247.

```
(kali㉿kali)-[~]
$ nc -zv 192.168.0.247 1-1000
192.168.0.247: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.247] 445 (microsoft-ds) open
(UNKNOWN) [192.168.0.247] 139 (netbios-ssn) open
(UNKNOWN) [192.168.0.247] 135 (epmap) open
```

Nota. La figura muestra el resultado de un escaneo realizado con la herramienta Netcat (nc -zv 192.168.0.247 1-1000), en el cual se identificaron los puertos 135 (epmap), 139 (netbios-ssn) y 445 (microsoft-ds) como abiertos en el host analizado.

Masscan: facilitó un escaneo masivo y de alta velocidad de puertos, optimizando el proceso de descubrimiento de servicios en la red institucional.

Ilustración 19 Escaneo masivo de puertos con Masscan en el host 192.168.0.22.

```
(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535 192.168.0.22 --rate=1000
[sudo] contraseña para kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-08-13 16:59:30
GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 5040/tcp on 192.168.0.22

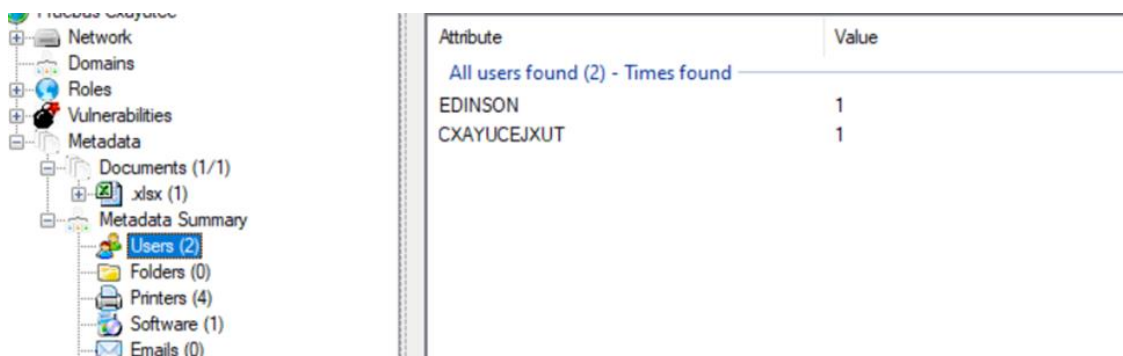
Discovered open port 135/tcp on 192.168.0.22

Discovered open port 139/tcp on 192.168.0.22
```

Nota. La figura muestra el resultado de un escaneo de 65.535 puertos realizado con la herramienta Masscan (`sudo masscan -p1-65535 192.168.0.22 --rate=1000`). Se identificaron los puertos 5040/tcp, 135/tcp y 139/tcp como abiertos en el host 192.168.0.22.

Foca: se utilizó para identificar metadatos en documentos disponibles públicamente, revelando información sensible como nombres de usuarios, rutas de red o software empleado, lo cual representa un riesgo adicional de fuga de información.

Ilustración 20 Extracción de usuarios a partir de metadatos con FOCA.



Attribute	Value
All users found (2) - Times found	
EDINSON	1
CXAYUCEJXUT	1

Ilustración 21 Visualización de relaciones y entidades con Maltego para la E.S.E. CXAYUCE JXUT,



La combinación de estas herramientas aseguró una evaluación integral: las herramientas automáticas agilizaron la detección masiva de vulnerabilidades, mientras que las manuales aportaron un nivel de verificación detallada que permitió validar los hallazgos y

adaptarlos al contexto específico de la E.S.E. CXAYUCE JXUT,. Este enfoque híbrido responde a la filosofía de OSSTMM, en la que la redundancia de pruebas garantiza resultados más confiables.

1.2.1.3. Resultados preliminares

Dentro los resultados obtenidos se identificaron 34 direcciones ip dentro de la red de los cuales viene con información de puertos servicios, versiones, sistema operativo. La E.S.E. CXAYUCE JXUT, ubicada en el municipio de Toribío (Cauca), atiende a comunidades rurales e indígenas, y como cualquier entidad de salud, maneja información muy sensible. Esta información, si no está bien protegida, puede ser robada, modificada o usada de forma indebida.

En contextos como el nuestro, donde a veces no se cuenta con todos los recursos tecnológicos, es común encontrar sistemas con contraseñas por defecto, equipos que no han recibido actualizaciones o redes que no están segmentadas. Todo esto puede representar una puerta abierta para los atacantes.

Por eso, hacer un análisis de vulnerabilidades no es algo que se deba dejar para después, sino que es una medida necesaria para proteger los datos de los pacientes y el funcionamiento de los servicios clínicos.

Durante el análisis de vulnerabilidades, se detectaron varios aspectos importantes:

Algunos equipos tenían servicios abiertos que ya no eran necesarios, lo cual representa un riesgo.

Se encontraron versiones de software que estaban desactualizadas, y que podrían ser aprovechadas si alguien logra acceder a la red.

En ciertas configuraciones se notó la falta de medidas de seguridad como doble autenticación o segmentación de red.

La mayoría de las vulnerabilidades encontradas podían ser solucionadas con configuraciones básicas, actualizaciones o cambio de contraseñas.

Al aplicar la metodología OSSTMM y las métricas mencionadas, se obtuvo un panorama más claro del nivel de exposición. Con esta información, es posible priorizar qué vulnerabilidades deben corregirse primero, según el riesgo que representan.

Este análisis también permitió evidenciar la necesidad de fortalecer la cultura de la seguridad en la entidad, pues muchas de las fallas no son técnicas, sino de procedimiento o falta de políticas internas claras.

13. Capítulo 3

13.1. Implementar la metodología OSSTMM (Open Source Security Testing Methodology Manual) para llevar a cabo pruebas de penetración estructuradas, cubriendo aspectos como seguridad en redes, sistemas, servicios y aplicaciones de la E.S.E Cxayuce Jxut.

La seguridad informática requiere de marcos de trabajo estructurados que permitan garantizar la rigurosidad en la evaluación de los sistemas tecnológicos. En este capítulo se presenta la implementación de la metodología OSSTMM (Open Source Security Testing Methodology Manual), en la E.S.E. Cxayuce Jxut de Toribío, Cauca, con el objetivo de identificar vulnerabilidades, medir la exposición y proponer controles de mitigación adecuados. Se describen las fases aplicadas, las herramientas empleadas, los criterios de medición y los resultados obtenidos (ISECOM, 2012).

13.2. Metodología OSSTMM

OSSTMM proporciona un conjunto de procesos normalizados para realizar auditorías de seguridad, cubriendo áreas críticas como:

- **Seguridad en redes:** Protocolos, configuraciones y exposición de servicios.
- **Seguridad en sistemas:** Sistemas operativos, parches y controles internos.
- **Seguridad en aplicaciones y servicios:** Detección de servicios activos, aplicaciones expuestas y niveles de acceso.
- **Factores humanos y físicos:** Controles organizacionales y de acceso físico.

13.3. Aplicación en la E.S.E. Cxayuce Jxut

Para el caso de estudio, se aplicaron las fases de la metodología OSSTMM siguiendo este orden:

- **Reconocimiento** de la infraestructura tecnológica mediante herramientas de escaneo.
- **Levantamiento de inventario** de activos críticos, clasificando equipos, sistemas y servicios.
- **Pruebas técnicas de seguridad** a nivel de red, sistemas y aplicaciones.
- **Documentación de hallazgos**, con evidencias de vulnerabilidades y configuraciones deficientes.

13.3. Justificación del uso de OSSTMM

OSSTMM ofrece un enfoque basado en métricas cuantificables (por ejemplo, RAV - Risk Assessment Value) y un marco de interacción que cubre redes, sistemas, aplicaciones y factores humanos/físicos. Frente a otras metodologías (p. ej. OWASP para aplicaciones o NIST para controles), OSSTMM aporta:

- Una visión holística de la seguridad (técnica + humana + física).
- Métricas objetivas que facilitan priorización y comparabilidad.
- Procedimientos normalizados que aumentan la reproducibilidad de la auditoría.

Por estas razones, OSSTMM se consideró la opción más adecuada para evaluar la exposición y riesgos de la infraestructura tecnológica de la E.S.E Cxayuce Jxut.

14. Capítulo 4

14.1. Evaluar el nivel de exposición y posibles riesgos asociados a cada vulnerabilidad encontrada, categorizando su impacto y probabilidad de explotación para proporcionar un diagnóstico preciso del estado de seguridad.

En este apartado se llevará a cabo la evaluación de la exposición y los riesgos asociados a las vulnerabilidades identificadas en la infraestructura tecnológica de la E.S.E. Cxayuce Jxut de Toribío, Cauca, aplicando los lineamientos de la metodología OSSTMM. La valoración se realizará considerando que el riesgo se definirá como la existencia de limitaciones en la presencia de seguridad que puedan afectar de manera negativa a las personas, los procesos, la información sensible, la reputación institucional o el cumplimiento normativo.

14.1.1. Dimensiones críticas de OSSTMM

La evaluación se orientará a establecer, en primer lugar, cómo cada vulnerabilidad podrá incidir en las dimensiones críticas de la seguridad definidas por OSSTMM: seguridad (safety), privacidad (privacy), practicidad (practicality) y usabilidad (usability). Estas dimensiones permitirán identificar el nivel de impacto que cada hallazgo podrá generar y servirán como marco para determinar la gravedad de los riesgos detectados.

- **Seguridad (safety):** toda vulnerabilidad que se identifique podrá ser analizada en términos de su capacidad de afectar la integridad física y emocional de las personas, así como la continuidad de los procesos institucionales.
- **Privacidad (privacy):** se evaluará de qué manera cada vulnerabilidad podrá facilitar el acceso indebido, la filtración o la exposición no autorizada de datos sensibles.
- **Practicidad (practicality):** las vulnerabilidades serán valoradas en función de su impacto en la eficiencia y viabilidad de los procesos organizacionales.

- **Usabilidad (usability):** se analizará cómo las vulnerabilidades podrán incidir en el equilibrio entre seguridad y accesibilidad, evitando que las restricciones excesivas generen nuevos riesgos.

14.2. Aplicación de los Risk Assessment Values (RAVs)

Posteriormente, se aplicarán los **Risk Assessment Values (RAVs)**, con el propósito de cuantificar la degradación de la seguridad a lo largo del tiempo. Los RAVs se calcularán teniendo en cuenta el grado de deterioro de cada módulo desde un estado de seguridad óptimo, el ciclo de tiempo en el cual se alcanzará la degradación máxima, la influencia de otros controles, los pesos asignados a las dimensiones de seguridad y la clasificación del riesgo según su tipo.

El RAV integrará tres componentes fundamentales: la **porosidad** (definida por la visibilidad, el acceso y la confianza), los **controles de seguridad implementados** y las **limitaciones presentes en la infraestructura**. De esta manera, se obtendrá un indicador porcentual que reflejará el grado real de exposición y resiliencia de los sistemas frente a posibles amenazas (Gordón, 2017).

En este proceso, los riesgos se categorizarán en vulnerabilidades, debilidades, fugas de información, preocupaciones o desconocidos, y se definirá si cada uno de ellos será identificado, verificado o considerado no aplicable. De esta manera, se logrará construir una visión objetiva y medible del nivel de exposición al que se encontrará la organización, permitiendo proyectar escenarios de impacto y proponer las medidas de mitigación más adecuadas para salvaguardar los activos críticos.

Tabla 5 Explicación de los apartados de las métricas RAV (OSSTMM v3)

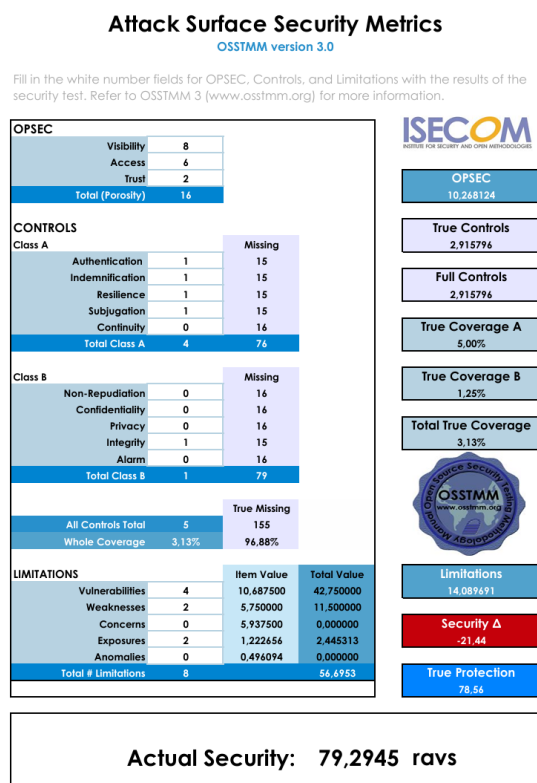
Apartado	Definición	Cómo se medirá en la E.S.E. Cxayuce Jxut
Visibilidad	Grado en que los sistemas, servicios o dispositivos podrán ser detectados desde el exterior.	Se aplicarán escaneos de red (ej. Nmap) para identificar puertos abiertos, servicios activos y versiones de software.
Acceso	Nivel de interacción que se podrá lograr con los servicios visibles.	Se realizarán pruebas de conexión y autenticación para comprobar accesos no protegidos o credenciales débiles.
Confianza (Trust)	Permisos y relaciones de confianza que la infraestructura otorgará por defecto.	Se analizarán políticas de acceso, segmentación de red y cuentas con privilegios por defecto.
Controles Clase A	Mecanismos de defensa activa: autenticación, indemnización, resiliencia, subyugación.	Se revisará la existencia de autenticación robusta, respaldos, políticas de recuperación y limitación de privilegios.
Controles Clase B	Protección de la información y procesos: no repudio, uso de cifrado (TLS/VPN), la confidencialidad, privacidad, integridad de datos y la existencia de integridad, alarmas.	Se verificará la trazabilidad (logs), el uso de cifrado (TLS/VPN), la privacidad, integridad de datos y la existencia de alertas de seguridad.

Vulnerabilidades	Fallos técnicos explotables en la infraestructura.	Se identificarán con escáneres de seguridad y pruebas de penetración (ej. Nessus, OpenVAS).
Debilidades	Deficiencias de gestión o usabilidad que incrementan el riesgo.	Se evaluará la configuración de contraseñas, políticas de seguridad y prácticas del personal.
Preocupaciones	Riesgos derivados de no cumplir buenas prácticas o estándares.	Se medirá revisando la alineación con normas como ISO/IEC 27001 y guías de ciberseguridad.
Exposiciones	Información sensible o técnica que queda públicamente visible.	Se buscarán datos expuestos en metadatos, dominios, repositorios y sitios web.
Anomalías	Comportamientos inesperados en sistemas o redes que pueden derivar tráfico y revisión de registros de en riesgos.	Se detectarán mediante análisis de seguridad.
Security Δ (Delta)	Diferencia entre la seguridad esperada y la real.	Se calculará al comparar los controles presentes frente a los que deberían existir.

True Protection	Nivel real de protección efectivo alcanzado.	Se expresará en porcentaje con base en la cobertura de controles activos y limitaciones presentes.
Actual (RAVs)	Security Valor final de seguridad obtenido, en puntos de 0 a 100.	Se obtendrá a partir del cálculo total de porosidad, controles y limitaciones según OSSTMM.
Fuente: Elaboración propia		

Nato. La tabla 5 detalla los apartados que conformarán las métricas de superficie de ataque bajo la metodología OSSTMM, describiendo su significado conceptual y la manera en que serán medidos dentro de la infraestructura tecnológica de la E.S.E. Cxayuce Jxut de Toribío, Cauca. Este glosario operativo permitirá establecer un marco de referencia claro y verificable para la obtención del Risk Assessment Value (RAV), garantizando que el proceso de evaluación de la exposición y riesgos de vulnerabilidades se realice con criterios objetivos, sistemáticos y replicables.

Ilustración 22 Calculadora RAV área SERVIDOR



OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Nota. La tabla presenta los resultados del cálculo del Risk Assessment Value (RAV) mediante la metodología OSSTMM 3.0, aplicado al servidor evaluado en la E.S.E. Cxayuce Jxut. Se observa un nivel de porosidad de 16, con una cobertura de controles efectiva del 3,13% y ocho limitaciones identificadas. El valor final de seguridad actual obtenido fue de **79,29 RAVs**, lo cual evidencia una protección parcial y la necesidad de implementar controles adicionales para reducir la exposición de la infraestructura.

15. Capítulo 5

15.1. Generar un informe detallado que presente los hallazgos del test de penetración, orientado a la mitigación de vulnerabilidades y al fortalecimiento de la seguridad de la infraestructura tecnológica de la E.S.E Cxayuce Jxut.

La seguridad de la información en el sector salud es un aspecto crítico, pues involucra el resguardo de datos altamente sensibles como las **historias clínicas**, la **identificación de pacientes** y la **información administrativa** de la institución. Una vulneración en estos sistemas no solo pone en riesgo la privacidad de los usuarios, sino que también puede afectar la **operación hospitalaria**, comprometiendo directamente la atención médica.

El test de penetración realizado bajo la metodología **OSSTMM** constituye una práctica ética y controlada que permite simular ataques reales sobre la infraestructura tecnológica de la E.S.E CXAYUCE JXUT. Su propósito principal es detectar vulnerabilidades que podrían ser explotadas por ciberdelincuentes, documentarlas y proponer acciones de mitigación que reduzcan el riesgo de incidentes.

Este capítulo presenta un informe detallado de los hallazgos obtenidos durante las pruebas, acompañado de un análisis del impacto y probabilidad de explotación, así como propuestas de mejora alineadas con normativas nacionales (Ley 1273 de 2009, Ley 1581 de 2012, Decreto 1078 de 2015, Resolución 1995 de 1999) e internacionales (ISO/IEC 27001, ISO/IEC 27799, HIPAA, NIST).

A continuación, te presento una estructura para el **capítulo de análisis de resultados** de un informe de **test de penetración**, enfocado en la mitigación de vulnerabilidades y el

fortalecimiento de la seguridad de la E.S.E Cxayuce Jxut. Esta estructura te servirá como guía para desarrollar el contenido de manera clara y profesional.

15.2. Metodología de Evaluación

La evaluación se llevó a cabo siguiendo una metodología robusta, que incluyó las siguientes fases:

- **Reconocimiento:** En la primera fase, denominada **Reconocimiento de activos**, se recolectó información sobre la infraestructura tecnológica, incluyendo detalle de los equipos, tipo de Pc dependencia, SO y antivirus. Para esta tarea se emplearon herramientas como **Nmap**, que permitió identificar hosts activos, puertos y servicios expuestos.
- **Análisis de Vulnerabilidades:** Se emplearon herramientas automatizadas y técnicas manuales para identificar vulnerabilidades en servidores, aplicaciones y redes, combinando la rapidez de los escáneres con la precisión del análisis manual. Entre las principales herramientas destacan **Nessus**, Dumsdter, Netcat y demás herramientas de escaning, reconocidas por detectar vulnerabilidades conocidas, configuraciones inseguras y servicios expuestos, además de generar reportes que facilitan la priorización de riesgos.
- **Explotación:** Se intentó explotar las vulnerabilidades encontradas para confirmar su existencia y evaluar el nivel de riesgo real que representan.

La fase de **Explotación** tuvo como propósito confirmar la existencia real de las vulnerabilidades detectadas, evaluando su grado de impacto en la seguridad de la infraestructura. Para ello se implementaron herramientas como FOCA, Masscan que

permitió simular ataques controlados sobre las debilidades detectadas; **Hydra**, utilizada para realizar pruebas de fuerza bruta en servicios de autenticación; y **Netcat**, herramienta empleada para establecer conexiones directas con sistemas vulnerables.

15.3. Metodología de presentación de hallazgos a la E.S.E CXAYUCE JXUT.

Con el fin de garantizar un análisis claro, estructurado y comprensible de los resultados obtenidos en el test de penetración, se adoptó un **modelo de clasificación de vulnerabilidades** que permite priorizar riesgos y orientar la toma de decisiones en la **E.S.E Cxayuce Jxut**. Esta metodología no solo organiza los hallazgos, sino que también asegura que cada vulnerabilidad se evalúe de manera integral, considerando tanto su impacto técnico como su repercusión en la seguridad de la información hospitalaria.

15.3.1. Presentación de análisis de vulnerabilidades con Nessus.

El plan de remediación tiene como objetivo identificar, clasificar y evaluar las vulnerabilidades detectadas en cada uno de los equipos que integran la red de la organización. A partir de esta categorización, se establece una priorización de acciones correctivas que permitan reducir los niveles de riesgo asociados, garantizando la protección de la información, la integridad de los activos tecnológicos y la resiliencia de la infraestructura de TI frente a posibles incidentes de seguridad.

Tabla 6 Clasificación de vulnerabilidades identificadas en el servidor según nivel de riesgo

Equipo		Servidor	
Impacto	Plugin	Descripción	Remediación
ALTO	Conjuntos de cifrado SSL de intensidad media compatibles (SWEET32)	El host remoto admite el uso de cifrados SSL de intensidad media. Nessus considera de intensidad media cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.	El hallazgo indica que el servidor permite cifrados débiles como 3DES o claves menores a 112 bits. Para solucionarlo, se deben deshabilitar estos cifrados en la configuración del servidor, permitir solo protocolos modernos (TLS 1.2 y 1.3) y usar suites seguras como AES-GCM con ECDHE. Después de aplicar los cambios, se reinicia el servicio y se valida nuevamente con Nessus o SSL Labs para confirmar que ya no se aceptan cifrados inseguros.
		El certificado X.509 del servidor no es confiable porque la cadena de confianza está rota. Esto puede ocurrir si: El certificado proviene de una CA no reconocida o falta un certificado intermedio. El certificado está caducado o aún no válido. La firma es incorrecta o utiliza un algoritmo no soportado.	Instalar un certificado digital válido emitido por una autoridad confiable, incluir los certificados intermedios, mantenerlo vigente y con algoritmos seguros, y validar su correcto funcionamiento con herramientas como SSL Labs o Nessus
BAJO	Solicitud de marca de tiempo ICMP para divulgación remota de fecha	El servidor responde a solicitudes ICMP de tipo “marca de tiempo”, lo que permite que alguien externo consulte la hora que tiene configurada la	Configurar el servidor o firewall para bloquear las solicitudes de marca de tiempo ICMP (tipo 13) y sus respuestas (tipo 14), evitando así que un atacante obtenga la hora del sistema.

		máquina. Un atacante podría usar esa información para intentar eludir sistemas de seguridad que dependen de la hora (por ejemplo, códigos o tokens que sólo son válidos durante un tiempo).
--	--	---

Fuente: Elaboración propia

Nota. La tabla presenta la clasificación de vulnerabilidades detectadas en el servidor de la E.S.E. Cxayuce Jxut de Toribío, Cauca, organizadas por nivel de riesgo (alto, medio y bajo). Se describen los hallazgos técnicos, el impacto potencial sobre la seguridad y las recomendaciones de remediación necesarias para mitigar los riesgos identificados.

Tabla 7 *Clasificación de vulnerabilidades identificadas en el Contratación según nivel de riesgo*

Equipo		Contratación	
Impacto	Plugin	Descripción	Remediación
MEDIO	No se requiere firma SMB	Cuando no hay firma, la información que viaja entre el cliente y el servidor no tiene una "prueba de autenticidad". Eso permite que un atacante pueda interceptar y modificar los datos en tránsito, haciéndose pasar por el servidor o por el cliente	En Windows, se hace desde las directivas de seguridad en la opción "Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)". En Samba (Linux), se activa en la configuración llamada "server signing".

BAJO	Solicitud de marca de tiempo ICMP para divulgación remota de fecha	El host remoto responde a una solicitud de marca de tiempo ICMP. Esto permite a un atacante conocer la fecha establecida en la máquina objetivo, lo que podría ayudar a un atacante remoto no autenticado a evadir los protocolos de autenticación basados en tiempo.	La solución de “filtrar” significa que en tu firewall o en la configuración de red debes bloquear esos mensajes ICMP específicos (13 y 14), de modo que tu servidor no responda con esa información de tiempo.
------	--	---	--

Fuente: Elaboración propia

Nota. La clasificación de vulnerabilidades se realizó con base en los resultados del escaneo automatizado de seguridad, organizando los hallazgos según su nivel de impacto (alto, medio y bajo). Las descripciones corresponden a las debilidades detectadas y las recomendaciones proponen acciones de mitigación alineadas con buenas prácticas de seguridad.

Tabla 8 Clasificación de vulnerabilidades identificadas en el Cartera según nivel de riesgo

Equipo	Cartera		
Impacto	Plugin	Descripción	Remediación
MEDIO	No se requiere firma SMB	El servidor SMB (el que se usa para compartir archivos e impresoras en red) no exige firma digital en sus comunicaciones. Esto significa que los mensajes que viajan entre el cliente y el servidor no están protegidos contra modificaciones.	En Windows, se hace en las políticas de seguridad con la opción “Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)”. En Samba (Linux), se activa con la opción “server signing”.

Fuente: Elaboración propia

Nota. La vulnerabilidad identificada corresponde a la ausencia de firma digital en el protocolo SMB. Este riesgo se clasifica con un impacto medio, dado que, aunque no permite la explotación directa del sistema, sí expone las comunicaciones a posibles ataques de interceptación

y modificación de datos. La aplicación de las medidas de remediación descritas (habilitar la firma SMB en Windows o Linux) es fundamental para garantizar la integridad de la información transmitida entre cliente y servidor, reduciendo así la probabilidad de ataques de tipo man-in-the-middle.

Tabla 9 *Clasificación de vulnerabilidades identificadas en el Contador según nivel de riesgo*

Equipo		Contador	
Impacto	Plugin	Descripción	Remediación
MEDIO	No se puede confiar en el certificado SSL	El certificado X.509 del servidor no es confiable porque la cadena de confianza está rota. Esto puede pasar si el certificado no viene de una autoridad reconocida, si está vencido/no vigente, o si tiene errores en la firma. En ese caso, los usuarios no pueden comprobar que el servidor es legítimo, lo que facilita ataques de tipo hombre en el medio (MITM).	Instalar un certificado SSL/TLS válido emitido por una autoridad confiable y configurarlo correctamente en el servidor.
	Certificado o autofirmado o SSL	El servicio está usando un certificado digital que no proviene de una autoridad de certificación reconocida. Por eso, los navegadores y clientes no pueden confiar en él, lo que permite que un atacante suplante al servidor y realice ataques de tipo hombre en el medio (MITM).	Adquirir o generar un certificado SSL/TLS válido y confiable emitido por una autoridad de certificación reconocida e instalarlo en el servidor.
	No se requiere firma SMB	Esto significa que el servidor SMB no tiene habilitada la firma digital de mensajes, por lo que la comunicación no está protegida. Sin esa firma, un atacante puede interceptar y modificar los datos que viajan entre el cliente y el servidor (ataque hombre en el medio).	Habilitar la firma de mensajes SMB en el servidor, ya sea en Windows (directiva “Firmar digitalmente las comunicaciones, siempre”) o en Samba (“Firma del servidor”), para asegurar la

MEDIO BAJO		integridad de las comunicaciones.
	Certificado SSL con nombre de host incorrecto	Esto quiere decir que el nombre común (CN) del certificado SSL no coincide con el nombre del servidor al que se está accediendo. En otras palabras, el certificado fue emitido para otra máquina o dominio, y por eso los clientes no pueden confiar en que están conectados al servidor correcto. Adquirir o generar un certificado SSL/TLS válido cuyo Common Name (CN) o Subject Alternative Name (SAN) coincida exactamente con el nombre de dominio o servidor utilizado.
	Solicitud de marca de tiempo ICMP para divulgación remota de fecha	El equipo remoto respondió a una petición ICMP Timestamp, revelando la hora configurada en la máquina. Un atacante remoto sin credenciales podría usar esa información para intentar eludir controles de autenticación basados en tiempo. En Windows Vista/7 y Windows Server 2008/2008 R2 las marcas de tiempo devueltas son intencionalmente inexactas, aunque normalmente se encuentran dentro de un rango de ~1000 segundos respecto a la hora real. Bloquee las solicitudes ICMP Timestamp (tipo 13) entrantes y las respuestas ICMP Timestamp (tipo 14) salientes.

Fuente: Elaboración propia

Nota. Las vulnerabilidades identificadas en la infraestructura tecnológica corresponden a debilidades en la configuración de servicios críticos como SSL/TLS, SMB e ICMP. Aunque la mayoría presentan un nivel de impacto medio, su explotación podría comprometer la confidencialidad, integridad y disponibilidad de la información, así como facilitar ataques de suplantación (man-in-the-middle) y de enumeración de red. Si bien cada hallazgo tiene medidas

de remediación específicas, en conjunto reflejan la necesidad de establecer una gestión integral de la seguridad, que incluya la implementación de certificados válidos emitidos por autoridades de confianza, la habilitación de mecanismos de firma digital en protocolos de red y la restricción de servicios no esenciales.

15.3.2. Descripción de hallazgo

Tabla 10 Clasificación de hallazgos del test de penetración en la E.S.E Cxayuce Jxut

Hallazgo	Descripción	Impacto	Probabilidad de Explotación	Nivel de Riesgo	Recomendación
Puertos abiertos en servidores internos	Servicios de red expuestos sin controles adecuados	Acceso indebido a información sensible y puerta de entrada a ataques	Alta	Critico	Cerrar puertos innecesarios y configurar firewall perimetral
Sistemas desactualizados	Servidores y aplicaciones con parches de seguridad pendientes.	Explotación de vulnerabilidades conocidas y escalamiento de privilegios	Media	Alto	Establecer plan de actualizaciones periódicas.

Falta de capacitación del personal	Desconocimiento en protocolos de seguridad digital y uso de contraseñas seguras	Incrementa riesgo de phishing, fuga de datos y accesos indebidos	Alta	Alta	Implementar programas de formación y campañas de concienciación en ciberseguridad
Ausencia de segmentación de red	En ciertas configuraciones se notó la falta de medidas de seguridad como doble autenticación o segmentación de red.	Movimiento lateral de atacantes en caso de intrusión	Alta	Alto	Separar redes críticas mediante VLANs y firewalls internos

Fuente: Elaboración propia.

Nota. La tabla presenta los principales hallazgos identificados en el test de penetración realizado en la E.S.E Cxayuce Jxut, organizados según impacto, probabilidad, nivel de riesgo y recomendaciones de mitigación.

15.3.3. Matriz de riesgo de la E.S.E CXAYUCE JXUT Toribío

La matriz de riesgos forma parte del proceso de análisis y evaluación de seguridad desarrollado en la ESE CXAYUCE JXUT de Toribío. Esta herramienta tiene como propósito identificar, valorar y clasificar los riesgos asociados a las vulnerabilidades técnicas y humanas detectadas durante el estudio, aplicando el marco metodológico OSSTMM (Open Source Security Testing Methodology Manual).

Para la construcción de la matriz, se tomó como referencia el modelo propuesto por **Pirani (2024)**, una plataforma especializada en la gestión de riesgos organizacionales. Este modelo permite visualizar de manera gráfica la relación entre la **probabilidad de ocurrencia** y el **impacto potencial** de cada riesgo, utilizando una escala de colores que facilita la priorización de acciones preventivas y correctivas dentro de la organización.

En este contexto, la matriz refleja los eventos que podrían afectar la confidencialidad, integridad y disponibilidad de la información institucional, como el uso de protocolos inseguros, certificados inválidos, contraseñas reutilizadas o intentos de phishing. Cada uno de estos riesgos fue evaluado según su frecuencia e impacto, permitiendo determinar los niveles de exposición más críticos y establecer medidas de mitigación adecuadas.

De esta manera, la matriz de riesgos constituye un componente esencial dentro del proceso de valoración y gestión de vulnerabilidades, pues vincula los resultados técnicos obtenidos en las pruebas de penetración con la realidad operativa de la entidad. Además, proporciona una base sólida para el diseño de estrategias que fortalezcan la cultura de ciberseguridad, la respuesta ante incidentes y la mejora continua de los sistemas de información en la ESE CXAYUCE JXUT de Toribío.

Ilustración 23 Matriz de riesgo

 ¿Quieres una matriz interactiva, automática y gratis? Crea tu cuenta en Pirani en este link <https://bit.ly/3f5CKYo>

Frecuente	0	0	0	0	1
Probable	0	1	1	1	0
Ocasional	0	0	1	0	0
Posible	2	2	2	1	0
Improbable	0	0	0	0	0
	Insignificante	Menor	Moderado	Mayor	Catastrófico

Nota. La presente matriz de riesgos se ha construido conforme a la metodología OSSTMM (Open Source Security Testing Methodology Manual), en la cual se evalúan los niveles de probabilidad y impacto de cada vulnerabilidad identificada durante el proceso de evaluación de riesgos.

15.3. Análisis comparativo del informe del pentesting en la E.S.E CXAYUCE JXUT

Tabla 11 Resultados de la encuesta de percepción y prácticas de seguridad digital del personal

Pregunta	Resultado
Área de trabajo	66,7% administrativo, 33,3% asistencial
Tiempo en la institución	44,4% entre 4–6 años, 33,3% menos de 1 año, 22,2% entre 1–3 años
Cambio de contraseñas	77,8% una vez al año, 22,2% nunca
Uso de la misma contraseña en varios servicios	66,7% sí, 22,2% no, 11,1% prefirió no responder
Conocimiento de políticas de seguridad	44,4% sí, 55,6% no
Inducción sobre uso seguro	22,2% sí, 77,8% no
Correos sospechosos (phishing)	33,3% sí, 66,7% no
Percepción de exposición a ataques	66,7% nivel 4, 22,2% nivel 5, 11,1% nivel 3
Capacitaciones recibidas	100% no

Conocimiento de reporte de incidentes	22,2% sí, 77,8% no
Fuente: Elaboración propia.	

Nota. Los resultados evidencian falencias en la cultura de ciberseguridad del personal, destacándose el uso de la misma contraseña en varios servicios (66,7%), el desconocimiento de políticas de seguridad (55,6%) y la ausencia total de capacitaciones (100%). Estas debilidades incrementan la vulnerabilidad institucional y reflejan la necesidad de programas de formación y concienciación en seguridad informática.

Al comparar los hallazgos técnicos con los resultados de la encuesta aplicada al personal, se evidencian tanto coincidencias como brechas relevantes. Mientras las pruebas técnicas detectaron contraseñas débiles y la ausencia de políticas de autenticación robusta, el 66,7% de los encuestados reconoció utilizar la misma contraseña en varios servicios, lo cual confirma la vulnerabilidad asociada a la gestión de credenciales. Asimismo, aunque se identificaron sistemas desactualizados, más del 55% del personal manifestó desconocer la existencia de una política formal de seguridad, lo que refleja una deficiencia en la comunicación y aplicación de normativas internas.

Otro aspecto crítico corresponde al factor humano: el 100% de los encuestados afirmó no haber recibido capacitación reciente en ciberseguridad, situación que coincide con la vulnerabilidad identificada en términos de falta de preparación y concienciación del personal. Finalmente, en cuanto a percepción de riesgo, el 88,9% considera que la institución se encuentra altamente expuesta a ataques, lo cual demuestra un nivel de conciencia significativo, aunque sin acciones correctivas claras que permitan reducir dicha exposición.

El análisis de los resultados obtenidos mediante las herramientas **Nmap**, Naabuu, Mascan, Netcat, permitió identificar diversos servicios expuestos en los equipos de la red interna. En general, los cinco hosts evaluados presentan un patrón común de vulnerabilidades, entre las que destacan la exposición de servicios relacionados con **SMB/NetBIOS (puertos 139 y 445)** y **RPC (135)**, considerados de alto riesgo debido a que históricamente han sido utilizados como vectores de ataque para la propagación de malware y ransomware.

En la mayoría de los dispositivos también se detectó la presencia del puerto **5357/tcp (httpapi)**, asociado a servicios web internos de Windows, y del puerto **7070/tcp**, identificado en algunos casos como un servidor *realserver* con soporte SSL. Estos servicios, aunque no siempre son críticos, amplían la superficie de ataque si no se encuentran debidamente controlados o segmentados.

Un hallazgo particularmente relevante se presentó en el host **192.168.0.201**, donde se detectó la exposición de **MySQL (3306)** y del servicio de **Escritorio Remoto (3389)**. La combinación de una base de datos accesible desde la red y un servicio de acceso remoto abierto incrementa significativamente el riesgo de fuga de información, acceso no autorizado y escalamiento de privilegios. En un escenario adverso, un atacante podría obtener credenciales válidas y comprometer tanto la base de datos como el sistema operativo.

Otro caso crítico corresponde al host **192.168.0.22**, el cual reporta un número elevado de servicios activos en puertos no estándar, incluyendo múltiples instancias web distribuidas en rangos como 40120, 49269, 51068, 59831 y 61137, entre otros. Adicionalmente, se observaron referencias a direcciones IP externas y posibles direcciones de correo electrónico, lo que sugiere la existencia de aplicaciones en desarrollo o pruebas expuestas sin control adecuado. Este

comportamiento representa un alto nivel de riesgo, ya que los servicios en puertos no convencionales suelen ser menos monitoreados y, por lo tanto, más susceptibles a explotación.

En los hosts **192.168.0.4**, **192.168.0.44** y **192.168.0.247**, si bien la cantidad de servicios expuestos es menor, se mantiene la recurrencia de puertos críticos como SMB, RPC y HTTP internos. Esto confirma que la red presenta una configuración homogénea en la cual los equipos heredan las mismas vulnerabilidades, lo que facilita la propagación de ataques si uno de ellos es comprometido.

El análisis de resultados obtenido a partir del test de penetración realizado en la E.S.E Cxayuce Jxut permitió evidenciar vulnerabilidades críticas y de alto impacto que comprometen tanto la infraestructura tecnológica como la seguridad de la información clínica y administrativa. Entre los hallazgos más relevantes se destacan los puertos abiertos en servidores internos, los sistemas desactualizados, la falta de capacitación del personal y la ausencia de segmentación de red, factores que incrementan la probabilidad de accesos no autorizados, fuga de datos y afectaciones a la continuidad de los servicios de salud.

16. Capítulo 6

16.1. Establecer un plan de acción con propuestas de mejora para incrementar la resiliencia ante posibles ataques, incluyendo políticas de seguridad, controles técnicos y procedimientos de respuesta ante incidentes.

La aplicación de planes de mejora en seguridad informática resulta fundamental para garantizar la **protección de la información crítica**, la continuidad operativa y la confianza de los usuarios y clientes en la organización. En un contexto en el que las amenazas cibernéticas evolucionan constantemente, no contar con medidas preventivas y correctivas expone a la institución a riesgos como pérdida de datos, accesos no autorizados, fraudes, sanciones legales y un daño significativo a su reputación.

Estos planes permiten **fortalecer la infraestructura tecnológica**, reducir vulnerabilidades detectadas y establecer procedimientos claros que faciliten la detección temprana y la respuesta eficaz ante incidentes. Además, fomentan una **cultura de seguridad digital** mediante la capacitación del personal, garantizan la implementación de controles técnicos como contraseñas robustas, autenticación multifactor y segmentación de redes, y aseguran que los sistemas se mantengan actualizados frente a nuevas amenazas.

En definitiva, aplicar estos planes de mejora no solo es una medida de protección, sino una **estrategia de sostenibilidad y resiliencia organizacional**, ya que permite minimizar riesgos, cumplir con normativas y asegurar que la organización esté preparada para enfrentar posibles ataques cibernéticos, protegiendo así sus activos más valiosos: la información, los usuarios y la confianza institucional.

16.2. Acciones correctivas para la seguridad informática.

Este plan de mejora se formula a partir del análisis de vulnerabilidades y hallazgos obtenidos en la auditoría de seguridad informática. Su objetivo es establecer acciones correctivas, responsables y tiempos de ejecución que permitan fortalecer la infraestructura tecnológica y mitigar los riesgos detectados.

Tabla 12 *Plan de acciones correctivas para la mitigación de vulnerabilidades en la infraestructura tecnológica*

Acción Correctiva	Descripción	Responsable	Tiempo de Ejecución
Restricción de servicios SMB, RPC y NetBIOS	Bloquear o filtrar en firewall los puertos 135, 139 y 445. En caso de requerirse SMB, restringir acceso a IPs internas autorizadas. Limitar acceso solo desde red	Administrador de Red / Seguridad TI	Corto plazo (1-2 semanas)
Protección de RDP (3389)	administrativa, habilitar MFA, aplicar políticas de bloqueo por intentos fallidos. Restringir acceso solo desde localhost o	Administrador de Servidores	Corto plazo (1 mes)
Fortalecimiento de MySQL (3306)	servidores autorizados, habilitar cifrado TLS y contraseñas fuertes. Identificar, deshabilitar o proteger servicios en	DBA / Seguridad TI	Corto plazo (1 mes)
Depuración de servicios no estándar	puertos 40120, 49269, 51068, 59831, 61137. Implementar WAF o proxy. Crear VLAN para separar servidores	Equipo de Infraestructura	Mediano plazo (2-3 meses)
Segmentación de Red	críticos, bases de datos y usuarios finales. Configurar firewall perimetral.	Administrador de Red	Mediano plazo (3-4 meses)
Aplicación de actualizaciones y parches	Mantener Windows y demás servicios con parches de seguridad	Equipo de Soporte / Infraestructura	Continuo (mensual)

Monitoreo con IDS/IPS	aplicados. Verificar versiones expuestas (ej. HTTPAPI). Implementar sistema de detección de intrusos para registrar intentos de explotación de vulnerabilidades.	Seguridad TI	Mediano plazo (4-6 meses)
Concientización de usuarios	Capacitar al personal en buenas prácticas (contraseñas seguras, phishing, reporte de incidentes).	Área de Talento Humano / Seguridad TI	Continuo (cada 6 meses)
Política de mínimos privilegios	Limitar privilegios de usuarios según funciones. Revisar periódicamente accesos y roles.	Seguridad TI	Continuo (revisiones trimestrales)

Fuente: Elaboración propias

Nota: El plan establece acciones correctivas con responsables y tiempos definidos, priorizando medidas técnicas y administrativas para reducir vulnerabilidades y fortalecer la seguridad de la infraestructura tecnológica.

La **implementación de controles técnicos**, como la segmentación de red mediante VLANs, la instalación de firewalls internos, la doble autenticación y la aplicación sistemática de parches de seguridad, se plantea como una estrategia clave para **disminuir la superficie de ataque y limitar el movimiento lateral de intrusos** en caso de una vulneración. Estas acciones no solo incrementan la protección de los activos críticos de la institución, sino que también fortalecen la capacidad de respuesta ante ciberataques.

16.3 Acciones Estratégicas para la seguridad informática

El presente plan reúne un conjunto de acciones estratégicas diseñadas para fortalecer la ciberseguridad organizacional. Estas iniciativas buscan reducir riesgos, mejorar la cultura de

seguridad digital y establecer controles técnicos y administrativos que garanticen la protección de la información crítica.

Tabla 13 Estrategias de fortalecimiento en ciberseguridad para la infraestructura tecnológica

Acción Estratégica	Descripción	Responsable	Tiempo de Ejecución
Capacitación continua en ciberseguridad	Desarrollar e implementar un plan de formación permanente en seguridad digital para todo el personal.	Área de Talento Humano / Seguridad TI	Continuo (cada 6 meses)
Políticas de contraseñas y MFA	Establecer contraseñas robustas y habilitar autenticación multifactor en sistemas críticos.	Administrador de Sistemas / Seguridad TI	Corto plazo (1-2 meses)
Gestión de actualizaciones y parches	Diseñar un calendario de instalación y monitoreo de actualizaciones de seguridad en sistemas y redes.	Equipo de Soporte / Infraestructura	Continuo (mensual)
Segmentación de redes internas	Separar redes mediante VLAN y controles de acceso para limitar el movimiento lateral en caso de intrusión.	Administrador de Red	Mediano plazo (3-4 meses)
Protocolo de reporte de incidentes	Definir y divulgar un procedimiento claro para notificación y gestión de incidentes de seguridad.	Seguridad TI / Comité de Crisis	Corto plazo (1 mes)

Fuente: Elaboración propias

Nota. Las estrategias planteadas combinan medidas técnicas y administrativas, asignando responsables y tiempos definidos, con el fin de fortalecer la resiliencia de la infraestructura tecnológica frente a incidentes de seguridad.

El factor humano se identificó como uno de los principales vectores de riesgo, pues la falta de capacitación y concienciación en seguridad digital aumenta la probabilidad de incidentes como phishing, fuga de información y uso indebido de credenciales. En consecuencia, la propuesta enfatiza la necesidad de establecer programas permanentes de formación y sensibilización, los cuales no solo reduzcan los riesgos derivados de malas prácticas, sino que también contribuyan a consolidar una cultura organizacional de seguridad digital.

Este plan de acción no es un gasto, sino una **inversión estratégica** en la protección de la información vital de la E.S.E Cxayuce Jxut. La resiliencia cibernética no se logra de la noche a la mañana; es un proceso continuo que requiere compromiso, recursos y un enfoque metódico para proteger a la organización en un entorno digital cada vez más hostil.

Finalmente, se concluye que la propuesta no debe concebirse como un ejercicio aislado, sino como un **proceso dinámico y continuo**, que requiere ser monitoreado y actualizado periódicamente mediante auditorías de seguridad, simulacros de respuesta ante incidentes y revisión constante de políticas. De esta manera, se garantiza la **mejora continua**, la **preparación frente a riesgos emergentes** y la consolidación de una estrategia integral que permita a la E.S.E. Cxayuce Jxut ser más resiliente frente a las crecientes amenazas del entorno digital.

17. Resultados alcanzados

17.1. Identificación de activos críticos

Para la clasificación de los activos críticos se llevó a cabo un proceso estructurado que comenzó con el reconocimiento de toda la infraestructura tecnológica de la E.S.E. Cxayuce Jxut. Posteriormente, se elaboró un inventario detallado en Excel que incluyó información relacionada con el área, las especificaciones técnicas, el sistema operativo y el antivirus de cada equipo. Con base en este recurso, se realizó un análisis de las dependencias que gestionan mayor volumen de datos sensibles, lo que permitió identificar y clasificar como áreas críticas aquellas que podrían generar un mayor impacto en caso de ser vulneradas. Entre estas se destacan: Servidor, Contaduría, Cartera, Contratación y Gestión Documental.

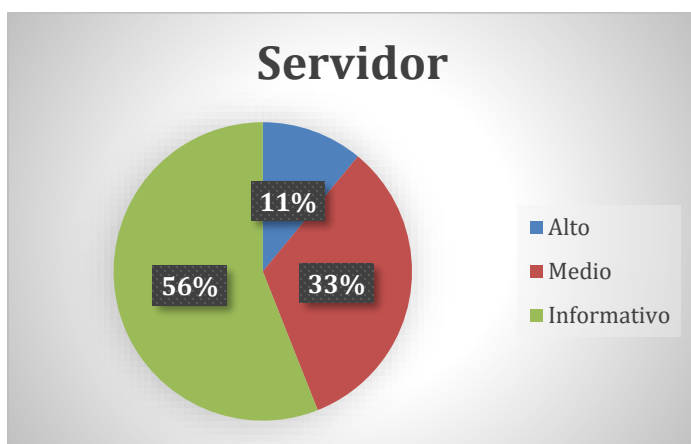
17.2. Análisis exhaustivo de vulnerabilidades

Se realizó un test de conocimiento para conocer la opinión del personal hospitalario con el fin de determinar la seguridad humana, para evaluar el nivel concientización y capacitación en temas de seguridad informática.

Analizando los resultados de la encuesta se reflejan una situación crítica en la gestión de la seguridad informática de la E.S.E Cxayuce Jxut, caracterizada por la falta de capacitación continua, la ausencia de socialización de políticas, prácticas débiles en el manejo de contraseñas y desconocimiento de procedimientos ante incidentes. A esto se suma una alta percepción de exposición a riesgos y la presencia de intentos de ataques externos (como phishing). Todo ello evidencia la necesidad urgente de implementar un plan de fortalecimiento en la cultura de seguridad institucional que incluya políticas claras, formación constante y protocolos de respuesta bien definidos.

Investigando las herramientas de evaluación de seguridad, se seleccionaron aquellas herramientas más adecuadas al proyecto en conformidad con la metodología OSSTMM. Para la ejecución de las pruebas se montó un laboratorio de evaluación: en la máquina atacante se instaló VirtualBox y, dentro de éste, Kali Linux. Con el sistema operativo arrancado se realizó un reconocimiento de red mediante Nmap en cada dependencia para identificar puertos y servicios expuestos; a continuación, se ejecutaron escaneos de vulnerabilidades con Nessus para detectar fallos conocidos. Los hallazgos obtenidos se registraron y clasificaron según su severidad, con el fin de priorizar las acciones correctivas y cumplir las fases de verificación definidas por metodología OSSTMM.

Ilustración 24 clasificación de vulnerabilidades Nessus en el servidor



Fuente: Elaboración propia.

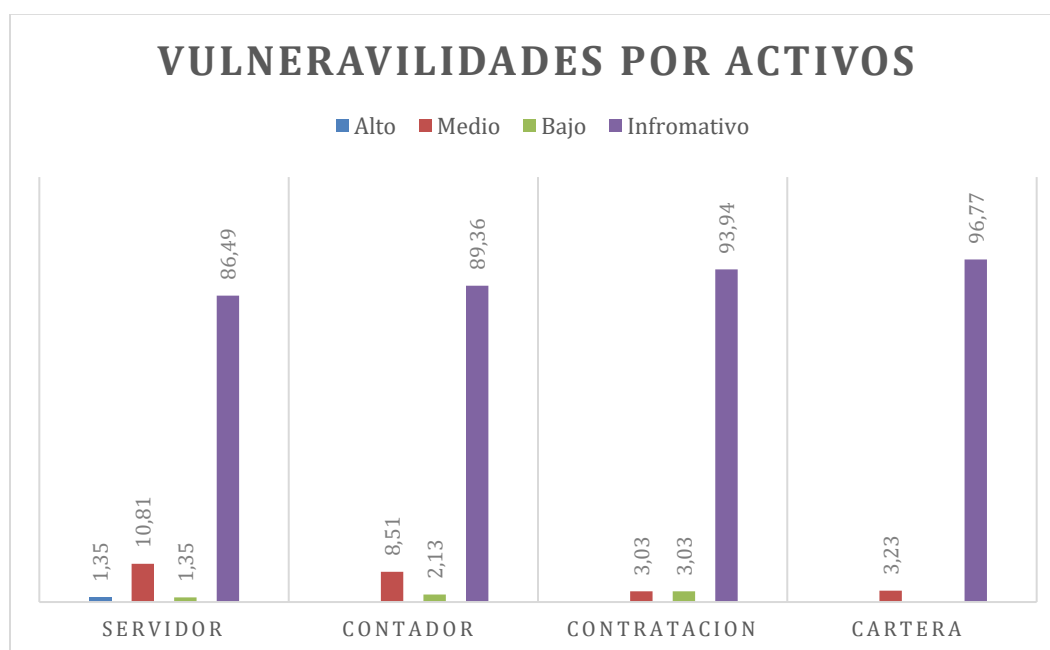
En el análisis realizado con la herramienta Nessus, se identificaron vulnerabilidades en el servidor clasificadas en tres niveles principales: alto, medio e informativo.

De acuerdo con la gráfica de distribución, el 56% corresponde a vulnerabilidades de tipo informativo, las cuales no representan un riesgo inmediato, pero proporcionan datos útiles para mejorar la configuración y fortalecer la seguridad. Por otra parte, el 33% de las detecciones son de

severidad media, relacionadas principalmente con problemas en certificados SSL, como certificados autofirmados o incompatibilidad de cifrados, que podrían ser aprovechados en escenarios de ataque intermedio (man-in-the-middle) si no se corrigen. Finalmente, se identificó un 11% de vulnerabilidades de severidad alta, las cuales representan un riesgo considerable para la confidencialidad y disponibilidad de la información, siendo necesario priorizar su corrección.

En términos generales, aunque la mayoría de los hallazgos son de carácter informativo y medio, la existencia de vulnerabilidades de severidad alta requiere atención inmediata, dado que pueden comprometer directamente los servicios críticos del servidor.

Ilustración 25 *Vulnerabilidades por activos*



Fuente: Elaboración propia a partir de los resultados del análisis de vulnerabilidades con herramientas automatizadas y técnicas manuales.

La gráfica anterior muestra la distribución de vulnerabilidades identificadas en los principales activos tecnológicos de la E.S.E Cxayuce Jxut: servidor, contador, contratación y

cartera. Se observa que, en todos los casos, el mayor porcentaje corresponde a vulnerabilidades de tipo informativo, con valores superiores al 80%, siendo el área de cartera la que presenta la proporción más alta (96,77%), seguida por contratación (93,94%), contador (89,36%) y servidor (86,49%).

En segundo lugar, se encuentran las vulnerabilidades de nivel medio, que alcanzan porcentajes moderados, principalmente en los activos de servidor (10,81%) y contador (8,51%), mientras que en contratación y cartera su incidencia es mucho menor, con valores entre el 3% y el 3,23%.

Las vulnerabilidades de nivel alto se presentan únicamente en el activo servidor (1,35%), lo que evidencia que este componente crítico de la infraestructura requiere atención prioritaria para mitigar riesgos asociados a la disponibilidad y seguridad de los servicios.

Finalmente, las vulnerabilidades de tipo bajo tienen una participación reducida en todos los activos, con valores cercanos al 1% al 3%.

En conclusión, el análisis revela que la mayor parte de los hallazgos corresponden a vulnerabilidades informativas, útiles para el fortalecimiento de la seguridad, mientras que las vulnerabilidades de severidad alta y media se concentran en el servidor y el contador, los cuales deben ser priorizados en la implementación de planes de mitigación.

El análisis realizado permitió identificar y clasificar un conjunto de herramientas fundamentales para el desarrollo de pruebas de penetración bajo la metodología OSSTMM. Entre los resultados más relevantes se destaca que la combinación de herramientas manuales, automáticas y mixtas facilita una cobertura integral de todo el ciclo de un test de seguridad.

Se evidenció que las herramientas manuales como VirtualBox, Dmitry, Netcat y dnsdumpster requieren un mayor nivel de conocimiento técnico, pero ofrecen al auditor un control detallado y flexible sobre el proceso. Por su parte, las herramientas automáticas como Nessus, Masscan, Foca y Maltego permiten una detección más rápida y eficiente de vulnerabilidades, aunque pueden generar falsos positivos que deben ser validados. Finalmente, las herramientas de uso mixto, entre ellas Kali Linux, Hydra, Nmap y Cupp, se consolidan como opciones versátiles, ya que permiten automatizar procesos sin perder la capacidad de personalización.

Asimismo, se logró demostrar que con este conjunto de herramientas se cubren todas las fases de una auditoría de seguridad informática:

- Reconocimiento y recolección de información (Dmitry, dnsdumpster, Maltego).
- Escaneo y detección de vulnerabilidades (Nmap, Masscan, Nessus).
- Explotación y auditoría de contraseñas (Hydra, Cupp).
- Entorno y soporte de pruebas (VirtualBox, Kali Linux).
- Análisis avanzado y gestión de datos (Foca, Maltego).

En conclusión, los resultados obtenidos confirman que la adecuada selección y utilización de herramientas de distinta naturaleza (manual, automática y mixta) permite llevar a cabo pruebas de penetración más completas, reduciendo riesgos y aumentando la precisión en la identificación de vulnerabilidades dentro de la infraestructura tecnológica de la institución evaluada.

17.3. Aplicación estructurada de la metodología OSSTMM

La aplicación de la metodología OSSTMM al servidor evaluado de la E.S.E. CXAYUCE JXUT, permitió determinar de manera cuantitativa el nivel real de seguridad de la infraestructura tecnológica. El análisis de superficie de ataque evidenció 8 servicios expuestos en 5 dispositivos,

lo cual generó un valor de porosidad total de 16, reflejando una visibilidad y accesibilidad elevada para un atacante.

En cuanto a los controles de seguridad, únicamente se identificaron cinco mecanismos efectivos, lo que corresponde a una cobertura real de 3,13% frente a los requerimientos establecidos por el modelo OSSTMM. Este bajo porcentaje de cobertura implica que la mayoría de los controles esperados no se encuentran implementados, especialmente aquellos relacionados con confidencialidad, privacidad, alarmas y continuidad operativa.

En la sección de limitaciones, se contabilizaron 8 hallazgos asociados a vulnerabilidades críticas, debilidades en políticas de autenticación y exposición de servicios innecesarios. El peso total de estas limitaciones fue de 56,69, lo que impactó de forma negativa en la seguridad calculada, generando un Security Δ de -21,44.

El procesamiento de los datos en la calculadora RAV arrojó un nivel de seguridad actual de 79,29 RAVs. Este resultado indica que, si bien existen controles mínimos, la alta porosidad y la cantidad de limitaciones reducen la protección efectiva del sistema a un nivel medio, lo que expone a la institución a riesgos de explotación en servicios críticos como SMB, RDP y MySQL.

En conclusión, los resultados muestran que la E.S.E. Cxayuce Jxut presenta una cobertura insuficiente de controles y un nivel considerable de exposición, lo cual hace necesario priorizar acciones correctivas como: restricción de accesos mediante firewall y VPN, implementación de MFA en servicios críticos, migración del sistema operativo a una versión soportada y fortalecimiento de políticas de monitoreo y respaldo.

17.4. Evaluación del nivel de exposición y riesgos

La aplicación de la metodología **OSSTMM** en la evaluación de la infraestructura tecnológica de la **E.S.E. Cxayuce Jxut** permitirá obtener resultados que no solo identifiquen vulnerabilidades técnicas, sino que también aporten información estratégica para fortalecer la resiliencia institucional frente a ciberataques. Los resultados esperados son:

17.4.1. Mapa integral de vulnerabilidades priorizadas

Se espera obtener un inventario detallado de las vulnerabilidades encontradas en servidores, aplicaciones, redes y servicios, clasificadas según su nivel de riesgo (alto, medio, bajo). Este mapa servirá como punto de partida para priorizar acciones de mitigación y asignar recursos de manera eficiente.

17.4.2. Indicadores cuantitativos de exposición mediante RAVs.

1. Identificación de debilidades organizacionales y humanas

Además de los fallos técnicos, se espera evidenciar debilidades derivadas de la gestión, la falta de capacitación del personal y el incumplimiento de buenas prácticas en seguridad digital. Estos hallazgos reforzarán la necesidad de programas de formación y concienciación en ciberseguridad.

2. Análisis del impacto en dimensiones críticas de OSSTMM

Cada hallazgo será evaluado en relación con las dimensiones de **seguridad, privacidad, practicidad y usabilidad**, lo que permitirá proyectar escenarios de impacto sobre la confidencialidad de la información clínica, la continuidad de los procesos de atención en salud y la confianza de los usuarios.

3. Clasificación estandarizada de riesgos

Los resultados permitirán categorizar las vulnerabilidades detectadas en: vulnerabilidades técnicas, debilidades de gestión, exposiciones de información, preocupaciones de cumplimiento normativo y anomalías en sistemas. Esto facilitará una visión estructurada de los riesgos, útil para la toma de decisiones estratégicas.

4. Recomendaciones técnicas y normativas fundamentadas

A partir de los resultados, se espera formular un conjunto de medidas de mitigación que incluyan la implementación de controles técnicos (firewalls, segmentación de red, autenticación multifactor), así como el cumplimiento de normativas nacionales e internacionales como la **Ley 1273 de 2009, Ley 1581 de 2012, ISO/IEC 27001 y la HIPAA.**

5. Fortalecimiento de la cultura de seguridad institucional

Finalmente, se espera que los hallazgos y recomendaciones contribuyan a sensibilizar a directivos, personal administrativo y asistencial sobre la importancia de la ciberseguridad en el sector salud, promoviendo un enfoque preventivo y de mejora continua.

1.4.5. Generación de un informe técnico con hallazgos y recomendaciones.

La aplicación de la metodología descrita permitirá alcanzar los siguientes resultados en la E.S.E. Cxayuce Jxut:

1. Mapa integral de vulnerabilidades

Se espera obtener un listado detallado de las vulnerabilidades técnicas y organizacionales, clasificadas por criticidad, que facilite a la institución priorizar la atención de los riesgos más urgentes.

2. Validación del nivel real de exposición

A través de la explotación controlada, se espera confirmar cuáles vulnerabilidades son efectivamente explotables, diferenciándolas de aquellas que representan riesgos teóricos. Esto proporcionará un diagnóstico más preciso y realista.

3. Indicadores cuantitativos de seguridad (RAVs)

Se obtendrán indicadores porcentuales que reflejen la diferencia entre la seguridad esperada y la seguridad real alcanzada por la institución, medidos en valores de **Risk Assessment Values (RAVs)** bajo OSSTMM.

4. Recomendaciones técnicas y organizacionales

Se espera formular propuestas claras, como la implementación de **controles técnicos** (cierre de puertos innecesarios, segmentación de red con VLANs, firewalls internos, autenticación multifactor), así como **medidas organizacionales** (programas de formación y concienciación en ciberseguridad).

5. Cumplimiento normativo

Los hallazgos estarán vinculados con normativas nacionales e internacionales, lo que permitirá a la E.S.E. garantizar el resguardo de datos sensibles en conformidad con la ley y con buenas prácticas internacionales.

6. Fortalecimiento institucional

Finalmente, los resultados esperados buscan que la institución avance hacia una cultura organizacional de seguridad digital, en donde tanto el personal administrativo como asistencial comprendan la importancia de proteger los activos tecnológicos y la información clínica.

17.5. Diseño de un plan de acción para la mejora de la seguridad

La aplicación de esta metodología permitió obtener resultados concretos y verificables:

1. Identificación de vulnerabilidades críticas

Se detectaron puertos abiertos en servidores internos, sistemas sin actualizaciones de seguridad, falta de segmentación de red y ausencia de controles robustos en la autenticación.

2. Confirmación de exposición real

A través de la explotación controlada se comprobó que varias de las vulnerabilidades podían ser aprovechadas por atacantes, lo que representa un riesgo tangible para la seguridad de la información clínica y administrativa.

3. Indicadores medibles de seguridad (RAVs)

Se aplicaron métricas de OSSTMM, obteniendo valores que reflejan que la seguridad real es inferior a la esperada, lo que evidencia limitaciones en la protección de los sistemas y controles insuficientes frente a la superficie de ataque.

4. Recomendaciones técnicas inmediatas

Cierre de puertos innecesarios, segmentación de red con VLANs, instalación de firewalls internos, aplicación de parches de seguridad y fortalecimiento de la autenticación.

5. Hallazgos de tipo organizacional

Se evidenció que la falta de capacitación del personal en ciberseguridad constituye un vector de riesgo, lo que incrementa la probabilidad de incidentes por phishing, manejo indebido de credenciales o fuga de información.

6. Cumplimiento normativo y alineación con buenas prácticas

Los hallazgos obtenidos refuerzan la necesidad de aplicar lo dispuesto en la **Ley 1273 de 2009**, la **Ley 1581 de 2012**, el **Decreto 1078 de 2015**, y de adoptar estándares internacionales como **ISO/IEC 27001**, **ISO/IEC 27799** e **HIPAA**.

18. TRABAJOS FUTUROS

A partir de la experiencia obtenida en el desarrollo de esta investigación, considero que aún queda un camino amplio por recorrer en materia de seguridad informática aplicada al sector salud. Este trabajo no debe entenderse como un punto final, sino como la base para seguir profundizando en nuevas líneas de acción que fortalezcan a la E.S.E. Cxayuce Jxut frente a las crecientes amenazas digitales.

En primer lugar, me parece fundamental ampliar el alcance de las pruebas realizadas, integrando otros componentes tecnológicos que no fueron abordados en esta etapa, como los dispositivos médicos conectados, las aplicaciones móviles y los servicios en la nube. Estos elementos cada vez tienen mayor protagonismo en la atención hospitalaria y deben ser evaluados con el mismo rigor.

Asimismo, considero importante complementar la metodología OSSTMM con otros marcos de referencia internacionales, como el NIST o la ISO/IEC 27701, que permitirían integrar la gestión de riesgos con el enfoque de protección de datos personales y de privacidad. Esto contribuiría a consolidar un sistema de seguridad más integral y alineado con las mejores prácticas globales.

Otro aspecto que visualizo como trabajo futuro es la implementación de ejercicios de Red Teaming, donde se simulen ataques avanzados en condiciones reales. Este tipo de pruebas pondría a prueba no solo la infraestructura técnica, sino también la capacidad de detección y respuesta de la institución frente a incidentes reales.

Por otra parte, considero clave trabajar en la automatización de los sistemas de monitoreo y en la incorporación de inteligencia artificial para la detección temprana de anomalías, lo cual brindaría una ventaja significativa en la anticipación a ciberataques.

El factor humano seguirá siendo un reto. Por eso, un trabajo futuro necesario es profundizar en la concienciación del personal, evaluando cómo las capacitaciones y la cultura organizacional influyen en la seguridad digital de la institución.

Finalmente, pienso que sería de gran valor establecer evaluaciones periódicas con métricas como los RAVs, que permitan medir de manera constante el avance en seguridad. Además, explorar el impacto económico de los ciberataques en el sector salud ayudaría a justificar inversiones y a fortalecer políticas de seguridad más sólidas.

En conclusión, los trabajos futuros que se derivan de esta tesis buscan dar continuidad a un proceso que debe ser dinámico y en constante actualización. Estoy convencida de que si la E.S.E. Cxayuce Jxut asume este reto con visión a largo plazo, podrá consolidarse como una institución más resiliente, preparada y confiable frente a los desafíos de la era digital.

19. RECOMENDACIONES

- Fortalecer los controles técnicos de seguridad
- Implementar la segmentación de red mediante VLANs y firewalls internos para limitar el movimiento lateral de atacantes.
- Cerrar los puertos innecesarios en los servidores y establecer reglas estrictas en el firewall perimetral.
- Adoptar mecanismos de autenticación multifactor (MFA) en accesos críticos y servicios expuestos a internet.
- Garantizar la actualización periódica de sistemas operativos y aplicaciones, aplicando parches de seguridad tan pronto como sean liberados por los fabricantes.
- Desarrollar una política institucional de seguridad digital
- Elaborar y formalizar un manual de políticas y procedimientos de ciberseguridad, alineado con la Ley 1273 de 2009, la Ley 1581 de 2012, el Decreto 1078 de 2015 y estándares como ISO/IEC 27001.
- Establecer roles y responsabilidades claras en la gestión de incidentes y la protección de datos.
- Incluir protocolos de respaldo, recuperación y continuidad del servicio ante fallos de seguridad o desastres tecnológicos.
- Fortalecer el factor humano como eje de seguridad
- Implementar programas de capacitación y sensibilización en ciberseguridad dirigidos a todo el personal administrativo y asistencial.
- Promover buenas prácticas en el uso de contraseñas, manejo de dispositivos externos, detección de intentos de phishing y protección de la información clínica.

- Realizar campañas periódicas de concienciación para reforzar la cultura de seguridad en la institución.
- Monitorear y evaluar continuamente la seguridad institucional
- Realizar auditorías internas y externas de seguridad al menos una vez al año, complementadas con simulacros de respuesta ante incidentes.
- Monitorear en tiempo real la red institucional mediante sistemas de detección y prevención de intrusos (IDS/IPS).
- Revisar y actualizar periódicamente el plan de acción en ciberseguridad, considerando las amenazas emergentes y las recomendaciones internacionales.
- Garantizar el cumplimiento normativo y la adopción de buenas prácticas
- Asegurar que el manejo de las historias clínicas y datos sensibles se realice conforme a la Resolución 1995 de 1999, la Ley Estatutaria 1751 de 2015 y estándares internacionales como la HIPAA.
- Avanzar hacia la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo ISO/IEC 27001, lo que reforzará la confianza de pacientes, autoridades y terceros en los procesos de la E.S.E.
- Proyectar la resiliencia institucional como proceso continuo
- Tratar la seguridad de la información no como una acción aislada, sino como un proceso dinámico y permanente.
- Invertir en infraestructura tecnológica robusta y en capacitación constante para asegurar la preparación frente a riesgos emergentes.

- Consolidar una **cultura organizacional de seguridad digital**, donde cada funcionario entienda su papel en la protección de la información y en la continuidad del servicio hospitalario.

20. CONCLUSIONES

La presente investigación permitió evaluar el nivel de seguridad de la infraestructura tecnológica de la **E.S.E. Cxayuce Jxut de Toribío, Cauca** mediante la aplicación de un **test de penetración basado en la metodología OSSTMM**, lo cual brindó un diagnóstico integral del estado actual de la institución frente a las crecientes amenazas cibernéticas. Los resultados evidenciaron la existencia de vulnerabilidades críticas como la apertura de puertos en servidores internos, la falta de actualización de sistemas, la ausencia de segmentación de red y la carencia de capacitación del personal en ciberseguridad. Estas debilidades incrementan de manera significativa la exposición de la entidad, comprometiendo la **confidencialidad, integridad y disponibilidad de la información clínica y administrativa**, así como la continuidad en la prestación de los servicios de salud.

El uso de métricas cuantitativas como los **Risk Assessment Values (RAVs)** permitió traducir los hallazgos en indicadores objetivos, mostrando que el nivel de seguridad alcanzado por la institución es medio y requiere un fortalecimiento inmediato. En este sentido, el proyecto no solo identificó riesgos, sino que también aportó un conjunto de **recomendaciones técnicas y organizacionales** que incluyen el cierre de puertos innecesarios, la aplicación sistemática de parches de seguridad, la segmentación de redes críticas mediante VLANs, la instalación de firewalls internos y la implementación de programas permanentes de formación en seguridad digital para el personal de la institución.

Asimismo, se comprobó que la resiliencia institucional frente a ciberataques depende de la integración de **controles técnicos, políticas organizacionales y normativas nacionales e internacionales**, entre ellas la **Ley 1273 de 2009**, la **Ley 1581 de 2012**, la **Ley Estatutaria 1751**

de 2015, el **Decreto 1078 de 2015**, y estándares internacionales como la **ISO/IEC 27001**, la **ISO/IEC 27799** y la **HIPAA**. De esta manera, el trabajo aporta un marco de acción que trasciende lo técnico para convertirse en una estrategia integral de cumplimiento normativo y protección de los activos más valiosos de la E.S.E. Cxayuce Jxut que es la información y los servicios de salud.

Finalmente, la investigación demuestra que la seguridad de la información en el sector salud no puede concebirse como un ejercicio puntual, sino como un proceso dinámico, continuo y en constante actualización. El test de penetración realizado constituye un punto de partida para la consolidación de una cultura organizacional de seguridad digital, que fomente la prevención, la respuesta oportuna ante incidentes y la mejora constante en la gestión de riesgos. De esta manera, la E.S.E. Cxayuce Jxut se proyecta hacia una mayor resiliencia y confianza institucional, garantizando la protección de los pacientes, el fortalecimiento de la operación hospitalaria y la alineación con las mejores prácticas internacionales en ciberseguridad.

21. BIBLIOGRAFÍA

Consejo Nacional de Política Económica y Social – CONPES. (2016, abril 4). Documento

CONPES 3854 de 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación.

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Presidencia de la República de Colombia. (2013, junio 27). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.834.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Congreso de la República de Colombia. (2015, febrero 16). Ley Estatutaria 1751 de 2015. Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones. Diario Oficial No. 49.427.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60470>

Ministerio de Salud. (1999, julio 8). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la historia clínica. Diario Oficial No. 43.667.

https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

Presidencia de la República de Colombia. (2015, mayo 26). Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Diario Oficial No. 49.523.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76656>

Consejo Nacional de Política Económica y Social – CONPES. (2011, julio 14). Documento CONPES 3701 de 2011. Política de seguridad y defensa de la información. Departamento Nacional de Planeación.

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Cane, T. (2023). *ISO 27001:2022 Annex A 5.9 – Inventory of Information and Other Associated Assets*. ISMS.online. https://www.isms.online/iso-27001/annex-a-2022/5-9-inventory-of-information-other-associated-assets-2022/?utm_source=chatgpt.com

Colombia, C. d. (2009, enero 5). *Ley 1273 de 2009. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – de la protección de la información y de los datos– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las* *comunica.*

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35164>

Colombia, C. d. (2012, octubre 17). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.*

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Colombia, P. d. (2013, junio 27). *Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.*

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Herzog, P. V. (2003, 23 de agosto). *OSSTMM 2.1 – The Open Source Security Testing Methodology Manual*. ISECOM. <https://untrustednetwork.net/files/osstmm.en.2.1.pdf>

LatinPyme. (3 de octubre de 2024). La amenaza de los ciberataques en el sector salud en Colombia.

<https://www.latinpyme.com/la-amenaza-de-los-ciberataques-en-el-sector-salud-en-colombia>

Mesa Álvarez, M. D., & Correa, M. A. (2020). *Análisis de las vulnerabilidades de la infraestructura tecnológica mediante testing de caja blanca, bajo la norma ISO 27005 en la compañía Caracol Radio, nodo principal Bogotá*. Institución: Universidad Cooperativa de Colombia. <https://repository.ucc.edu.co/server/api/core/bitstreams/b880c954-e86e-4df8-a715-454fafd38afe/content>

NQA. ((s. f.)). *GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf>

PenTesting.Org. (2024). *OSSTMM overview*. <https://www.pentesting.org/methodology-understanding-guide/>

Presidencia de la República de Colombia. (n.d.). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.834. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Security, I. (2024). *Reporte de Costo de una Brecha de Datos 2024 (Data Breach Report)*. <https://lanotaeconomica.com.co/movidas-empresarial/segun-ibm-colombia-en-2024-ha-recibido-el-17-de-los-ciberataques-en-latinoamerica-el-60-afectaron-al-sector-salud/#:~:text=Seg%C3%BAn%20IBM%2C%20Colombia%20en%202024,sector%20salud%20%2D%20La%20Nota%20Eco>

Pirani. (2024). Matriz de riesgos: herramienta interactiva para la gestión y evaluación de riesgos organizacionales. Recuperado el 6 de octubre de 2025, de <https://www.piranirisk.com/es/>

22. Anexos

Ilustración 26 *Entrada hacia las instalaciones de la E.S.E. Cxayuce Jxut*



Fuente: Elaboración propia

Ilustración 27 *Área de archivo y historias clínicas*



Fuente: Elaboración propia

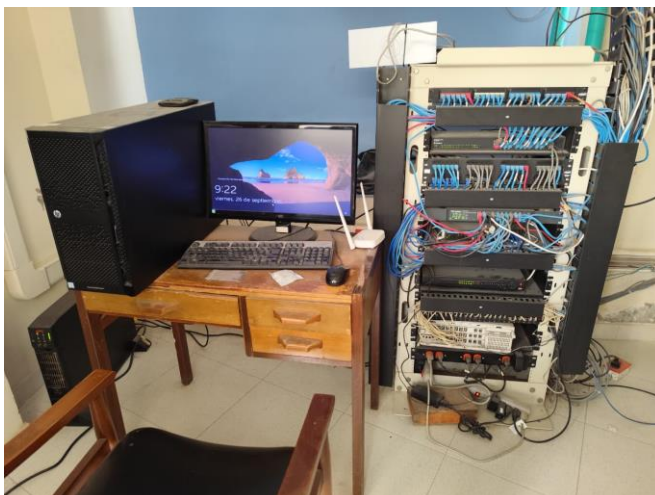
Ilustración 28 *Punto de distribución de red con cableado expuesto*



Fuente: Elaboración propia

Nota. La clasificación evidencia la exposición de servicios y puertos críticos en el área de servidores, lo que representa un alto riesgo de intrusión, explotación de vulnerabilidades conocidas y accesos no autorizados si no se aplican controles de seguridad adecuados.

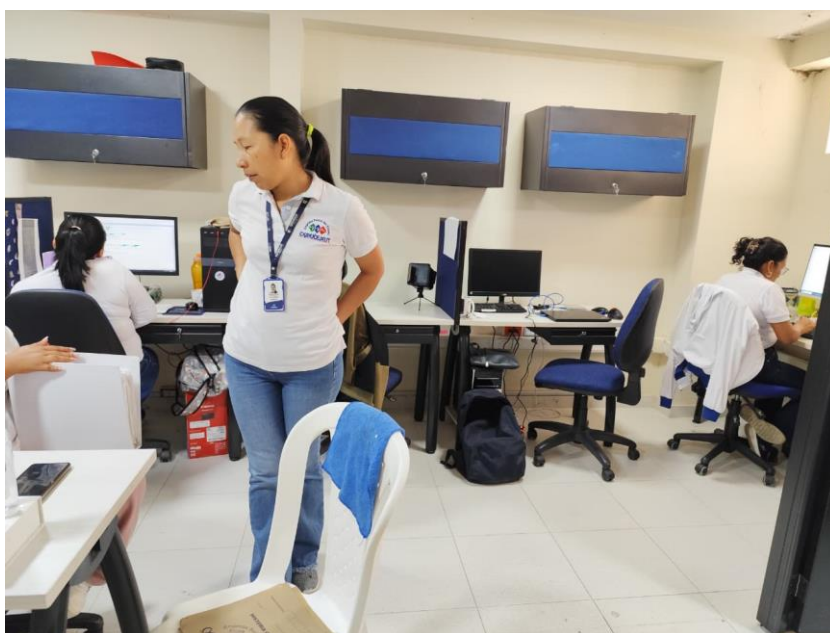
Ilustración 29 *Rack y servidor de comunicaciones con cableado estructurado desorganizado.*



Fuente: Elaboración propia

Nota. La imagen evidencia un rack de comunicaciones con cableado estructurado desorganizado y sin una adecuada gestión de orden ni protección física, lo que puede dificultar las labores de mantenimiento, incrementar los tiempos de respuesta ante incidentes y representar un riesgo para la continuidad operativa de la infraestructura tecnológica.

Ilustración 30 *área administrativa.*



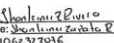
Fuente: Elaboración propia

Ilustración 29 cronograma de actividades

CRONOGRAMA DE ACTIVIDADES	
PROYECTO DE TESIS: "Implementación de Pruebas de Penetración y Evaluación de Seguridad mediante la Metodología OSSTMM en la Infraestructura Tecnológica de la E.S.E Cxayuce Jxut, Toriblo, Cauca, durante el semestre de 2025". El siguiente cronograma presenta la planeación de actividades realizadas en el marco del desarrollo del proyecto organizadas con sus respectiva fechas y descripción de actividades realizadas.	
No.	FECHA DESCRIPCIÓN
1	12/03/2025 Entrevista para acuerdo Entrevista con el ingeniero para acuerdo de días de trabajos y contextualización del proyecto.
2	14/03/2025 Identificación de activo mediante un inventario.
3	18/03/2025 Configuración del entorno de maquina virtuales.
4	18/03/2025 Escaneo de activos usando la herramienta Nmap.
5	24/03/2025 Escaneo de vulnerabilidades conocidas con Nessus.
6	26/03/2025 Recolección de información pasiva con la herramienta Dmitry.
7	1/04/2025 Conexión y manipulación de servicios en puertos abiertos con herramienta Netcat.
8	2/04/2025 Recolección de información de dominio y mapeo de red con herramienta Masscan.
9	7/04/2025 Descubrir información oculta en archivos, como nombres de autores con la herramienta Foca.
10	14/04/2025 Recolección y representación gráfica de datos por medio de la herramienta Maltego.
11	12/05/2025 Generar listas de contraseñas personalizada con la herramienta Cupp.
12	19/05/2025 Generar listas de usuarios personalizada con la herramienta Cupp.
13	7/07/2025 Implementación de encuestas mediante Google formulario.
14	14/07/2025 Identificación de vulnerabilidades por activos criticos.
15	18/08/2025 Análisis de exposición (Visibility / Access) mediante tabla de expacion y accesibilidad de vulnerabilidades.
16	1/09/2025 Evaluación de probabilidad de explotación mediante realización de la matriz de probabilidad.
17	2/09/2025 Clasificación de impacto (dimensiones OSSTMM) mediante Matriz de impacto categorizado.
18	3/09/2025 Integración en matriz de riesgo (RAV), combinado la probabilidad e impacto.
19	4/09/2025 Diagnóstico y reporte final (STAR Report), median un informe final.
20	15/09/2025 Procedimientos de respuesta ante incidentes mediante una guía.
21	29/09/2025 Entrega de informe final y plan de acción E.S.E Cxayuce Jxut.

Firmas de Conformidad:

Firma: 
 Nombre: WILMAR ARIEL BERMUDEZ BARONA
 C.C: 94541960
 Gerente E.S.E Cxayuce Jxut

Firma: 
 Nombre: Juan Carlos Zamora R
 C.C: 1062327036
 Ing. de sistemas E.S.E Cxayuce Jxut

Nota. La constancia y el cronograma evidencian la ejecución del proyecto de grado titulado “Implementación de Pruebas de Penetración y Evaluación de Seguridad mediante la Metodología OSSTMM en la Infraestructura Tecnológica de la E.S.E. Cxayu’ce Jxut”, desarrollado durante el año 2025. En ellos se detallan las actividades realizadas, las fechas de ejecución y la validación institucional por parte de la gerencia e ingeniería de sistemas de la entidad.

Ilustración 30 Constancia de cumplimiento de actividades del proyecto

CXAYU'CE JXUT EMPRESA SOCIAL DEL ESTADO
NIT.900.052.148-9

EL GERENTE CXAYU'CE JXUT EMPRESA SOCIAL DEL ESTADO DE LOS MUNICIPIOS DE TORIBIO Y JAMBALO - CAUCA

HACE CONSTAR:

Que los estudiantes EDINSON MESTIZO PAVI y DARLY DAYANA TENORIO, estudiantes de FACULTAD DE INGENIERIA de la CORPORACIÓN UNIVERSITARIA COMFACAUCA UNICOMFACAUCA, realizaron su proyecto de grado en CXAYUCE JXUT EMPRESA SOCIAL DEL ESTADO, se encuentran a paz y salvo en:

- Informe final del proyecto, con los resultados de las pruebas de penetración y la evaluación de seguridad realizada.
- Plan de acción, que contiene las recomendaciones y lineamientos para la mitigación de vulnerabilidades y mejora continua de la infraestructura tecnológica.

Dada en Toribio Cauca el ocho (08) día del mes de octubre del 2025.

WILMAR ARIEL BERMUDEZ BARONA
GERENTE

JHON LEINER ZAPATA RIVERA
ING. SISTEMAS-CONTRATISTA

Sede Administrativa - carrera 4 No.6-27 Barrio La Unión Cabecera Municipal Toribio - Cauca
Celular No. 3136571115 Email: contactenos@esecxayucejxut-toribio-cauca.gov.co

Nota. Documento expedido por la E.S.E. Cxayu'ce Jxut de Toribío Cauca, en el que se certifica que los estudiantes Edinson Mestizo Pavi y Darly Dayana Tenorio, de la Corporación Universitaria Comfacauca UNICOMFACAUCA, realizaron su proyecto de grado correspondiente al test de penetración y evaluación de seguridad informática bajo la metodología OSSTMM, y se encuentran a paz y salvo con la institución tras la entrega del informe final y plan de acción tecnológica.