UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Implementación de laboratorio virtual de ciberseguridad basado en estándares ISO/NIST para fortalecimiento digital en el ISU Sucre Quito, Ecuador

AUTOR

Guachán Morales, Victoria Alexandra

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en

MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Bayas Sampedro, Marcia Marisol

Santa Elena, Ecuador

Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Andrade Vera Alicia, Mgtr.

COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARCIA MARISOL BAYAS SAMPEDRO

Ing. Bayas Sampedro Marcia, PhD.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing. Orozco Iguasnia Jaime, Mgtr.

DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

LSI. Quirumbay Yagual Daniel, Mgtr.

DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. Rivera González María, Mgtr.

SECRETARIA GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por la cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por GUACHAN MORALES VICTORIA ALEXANDRA, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARCIA MARISOL BAYAS SAMPEDRO

Ing. Bayas Sampedro Marcia Marisol, PhD.

Santa Elena, 18 de mayo de 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Victoria Alexandra Guachán Morales**

DECLARO QUE:

El trabajo de Titulación, IMPLEMENTACIÓN DE LABORATORIO VIRTUAL DE CIBERSEGURIDAD BASADO EN ESTÁNDARES ISO/NIST PARA FORTALECIMIENTO DIGITAL EN EL ISU SUCRE QUITO, ECUADOR, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 18 de mayo de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
VICTORIA ALEXANDRA GUACHAN MORALES

Guachán Morales Victoria Alexandra

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Implementación de laboratorio virtual de ciberseguridad basado en estándares ISO/NIST para fortalecimiento digital en el ISU Sucre Quito, Ecuador, presentado por el estudiante, Victoria Alexandra Guachán Morales fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 10%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Certificado de análisis
Compilatio Magister+ | UPSE-ECU

Proyecto - Victoria Guachan (1)
ID : 0d0bade768ac07814e4453280ec12741c86ba08c

10%
Textos sospechosos

Nombre del fichero : Proyecto - Victoria Guachan (1).txt
Tamaño del archivo original : 5,18 MB
Número de palabras : 20.160
Número de caracteres : 138414

Depositante : MARCIA MARISOL BAYAS SAMPEDRO
Fecha de depósito : 19 de mayo de 2026
Tipo de carga : interface
fecha de fin de análisis : 19 de mayo de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARCIA MARISOL BAYAS SAMPEDRO

Ing. Bayas Sampedro Marcia Marisol, PhD.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Victoria Alexandra Guachán Morales**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 18 de mayo de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
VICTORIA ALEXANDRA GUACHAN MORALES

Guachán Morales Victoria Alexandra

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a los docentes que formaron parte de mi proceso académico, por sus valiosos conocimientos y su compromiso con la formación profesional.

A mi tutora Marcia Bayas, por su orientación, dedicación y acompañamiento constante, fundamentales para la culminación de este trabajo.

Al Instituto Superior Universitario Sucre, por brindarme la oportunidad de desarrollar este proyecto y por facilitar los recursos necesarios para su ejecución.

A todos ellos, mi profunda gratitud por su apoyo en este importante logro académico.

Victoria Alexandra Guachán Morales

DEDICATORIA

A Dios, por guiar mi camino, darme fortaleza en los momentos difíciles y permitirme alcanzar este logro.

A mis padres y hermanas, por su amor incondicional, sus enseñanzas y su apoyo constante. Gracias por inculcar en mí valores como el esfuerzo, la responsabilidad y la perseverancia, y por brindarme siempre palabras de aliento en los momentos más exigentes.

A mi esposo Cristopher y a mi hija Isabella, por ser mi mayor fuente de motivación y fortaleza. Gracias por su paciencia, comprensión y amor incondicional, por acompañarme en cada desafío y por dar sentido a cada uno de mis esfuerzos.

A todos ustedes, gracias por ser parte de este logro.

Victoria Alexandra Guachán Morales

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Este proyecto responde a la necesidad de disponer de un espacio seguro para evaluar la ciberseguridad del entorno digital del Instituto Superior Universitario Sucre, ubicado en Quito, Ecuador, sin intervenir sus sistemas reales. Para ello, se implementó un laboratorio virtual basado en los estándares ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5, destinado a identificar vulnerabilidades, ejecutar pruebas controladas, aplicar controles técnicos y evaluar la detección y respuesta ante incidentes. La investigación tuvo un enfoque mixto y un diseño cuasiexperimental pretest–postest, mediante análisis de vulnerabilidades, revisión de registros y monitoreo de eventos. El laboratorio integró VirtualBox, pfSense, Kali Linux, un servidor Ubuntu con WordPress y un sistema SIEM Wazuh. Como resultado, las vulnerabilidades se redujeron de 26 a 11, la detección mejoró del 25 % al 100 % y los tiempos de respuesta disminuyeron.

Palabras clave: ciberseguridad, laboratorio virtual, gestión de vulnerabilidades.

ABSTRACT

This project addresses the need for a secure environment to evaluate the cybersecurity of the digital infrastructure of Instituto Superior Universitario Sucre, located in Quito, Ecuador, without affecting its production systems. To achieve this, a virtual laboratory based on the ISO/IEC 27001:2022 and NIST SP 800-53 Rev. 5 standards was implemented to identify vulnerabilities, conduct controlled tests, apply technical controls, and assess incident detection and response capabilities.

The research followed a mixed-method approach with a quasi-experimental pretest–posttest design, supported by vulnerability analysis, log review, and event monitoring. The laboratory integrated VirtualBox, pfSense, Kali Linux, an Ubuntu server with WordPress, and the Wazuh SIEM platform. The results showed a reduction in vulnerabilities from 26 to 11, an improvement in detection rates from 25% to 100%, and shorter response times.

Keywords: cybersecurity, virtual laboratory, vulnerability management.

INTRODUCCIÓN

El uso creciente de tecnologías digitales ha modificado la forma en que las instituciones de educación superior gestionan sus procesos académicos, administrativos y comunicacionales. Las plataformas virtuales, sitios web institucionales y servicios digitales tienen un rol importante en el desarrollo de las actividades educativas. Sin embargo, esta dependencia tecnológica también amplía la exposición a riesgos como accesos no autorizados, explotación de vulnerabilidades en aplicaciones web, pérdida de información o interrupción de servicios. Por ello, la ciberseguridad es un componente esencial para proteger la confidencialidad, integridad y disponibilidad de la información institucional (UNESCO, 2020; European Union Agency for Cybersecurity [ENISA], 2023; ISO/IEC, 2022).

En América Latina, las instituciones educativas enfrentan desafíos para consolidar procesos de seguridad formales, mantener un monitoreo continuo y responder con prontitud a los incidentes. Según el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos, estas limitaciones son generadas debido a las restricciones presupuestarias, escasez de personal calificado y la ausencia de estrategias institucionales enfocadas en la seguridad digital (BID y OEA, 2020). La Agencia Europea de Ciberseguridad (ENISA) indica que las universidades son más vulnerables a los ciberataques, como el ransomware, el phishing y el acceso no autorizado (ENISA, 2023). En nuestro país, el gobierno ha publicado recomendaciones para reforzar la seguridad digital, pero las universidades aplican esas recomendaciones poco. Esa falta de aplicación reduce la disponibilidad de entornos controlados; en esos entornos los equipos simulan ataques, analizan vulnerabilidades y prueban controles de seguridad de forma sistemática (MINTEL, 2022).

El Instituto Superior Universitario Sucre (ISU Sucre) está en Quito, Ecuador. La institución tiene un desafío similar. El uso de procesos digitales en la academia, en la administración y en la comunicación ha aumentado. Con ese aumento la institución usa más plataformas web, más servicios institucionales y más entornos virtuales de aprendizaje. Pero la institución no tiene un entorno aislado donde pueda hacer pruebas de vulnerabilidades, hacer simulaciones de ataques y

monitorear eventos de seguridad sin tocar los sistemas operativos. Esta limitación impide aplicar de forma constante las recomendaciones de los estándares ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5. La limitación dificulta la gestión de vulnerabilidades, el monitoreo, el control de acceso y la respuesta a incidentes (ISO/IEC, 2022; NIST, 2020).

Ante la situación, el proyecto propone crear un laboratorio virtual de ciberseguridad. El laboratorio se basará en los estándares ISO/NIST y será un apoyo para fortalecer la seguridad digital del ISU Sucre. El laboratorio se concibe como un espacio separado de los sistemas reales, donde se pueden identificar vulnerabilidades, generar eventos de seguridad y comprobar controles en condiciones controladas. Para ello, se diseñó una arquitectura segmentada con una red LAN, una zona desmilitarizada y una red de ataque. El entorno integra VirtualBox, pfSense, Kali Linux, un servidor Ubuntu con WordPress y Wazuh como sistema SIEM para el monitoreo y análisis de eventos (Wazuh, s. f.). Esta organización permite aplicar controles técnicos y trabajar con principios de defensa en profundidad y confianza cero, al limitar accesos, separar segmentos y reducir posibles movimientos no autorizados dentro del laboratorio (Rose et al., 2020).

Este estudio emplea un diseño cuasiexperimental pretest-postest y una metodología de métodos mixtos. Se examinó el estado de seguridad inicial del ambiente institucional, se implementó el laboratorio como una intervención técnica y se contrastaron los resultados que surgieron después de la puesta en marcha de controles específicos (Shadish et al., 2002). Las métricas que se analizan son el número de vulnerabilidades identificadas, la tasa de detección de eventos, el tiempo medio para detectar (MTTD) y el tiempo medio para responder (MTTR), lo cual posibilita una evaluación cuantitativa del efecto del laboratorio en la posición de seguridad del ambiente evaluado.

El documento está estructurado en cuatro partes. La primera de ellas define el proyecto a partir de los antecedentes, la pregunta de investigación, el objetivo, la justificación y el alcance. La segunda desarrolla la base teórica y también la metodológica, y allí se integran conceptos que tienen que ver con la ciberseguridad. El capítulo cuatro, por su parte, expone la valoración de los resultados mediante el método pretest-postest, el análisis comparativo de indicadores, la interpretación de los hallazgos y los escenarios de prueba.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1 Antecedentes

En los últimos años, la transformación digital en el ámbito educativo ha impulsado el uso intensivo de las tecnologías de la información y comunicación para la gestión académica, administrativa y la comunicación institucional. En las instituciones de educación superior, el empleo de plataformas digitales, como los sistemas web institucionales y los entornos virtuales de aprendizaje, se ha vuelto esencial y crucial para mejorar la comunicación y la gestión educativa, así como los procedimientos académicos. Por otro lado, también ha aumentado las debilidades de acceso a las plataformas educativas, lo que las deja expuestas a ataques y amenazas cibernéticas que ponen en riesgo la disponibilidad, la integridad y la confiabilidad de los datos institucionales.

Según ENISA, mencionan que las instituciones de educación superior son uno de los entornos más expuestos a ciberataques. Además, el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos señalan que muchas instituciones educativas presentan dificultades para realizar evaluaciones continuas de seguridad y utilizar espacios técnicos especializados para pruebas de ciberseguridad. Estas limitaciones suelen relacionarse con restricciones presupuestarias, escasez de personal capacitado y ausencia de estrategias institucionales enfocadas en la seguridad digital (BID & OEA, 2020). Y debido a que manejan grandes volúmenes de datos y plataformas digitales son expuestos a varios tipos de ataques e incidentes dirigido a estos sistemas. Entre los más frecuentes están el ransomware, el phishing y los accesos no autorizados (ENISA, 2023).

En Ecuador existen lineamientos públicos orientados a fortalecer la seguridad digital; sin embargo, su adopción en instituciones de educación superior todavía presenta avances desiguales. Esta condición limita la disponibilidad de ambientes controlados para simular ataques, revisar vulnerabilidades y verificar controles de seguridad de forma sistemática (Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], 2022).

En el ISU Sucre, el uso permanente de servicios digitales para actividades académicas y administrativas obliga a que existan mecanismos de evaluación que no comprometan la operación diaria. Bajo este enfoque, un laboratorio virtual de ciberseguridad permite reproducir situaciones de riesgo, estudiar vulnerabilidades y probar medidas defensivas antes de trasladarlas a entornos reales.

1.2 Problema de investigación

En el ISU Sucre, el crecimiento de los procesos digitales en las áreas académicas, administrativas y comunicacionales ha incrementado el uso de plataformas web, servicios institucionales y entornos virtuales de aprendizaje. Aunque estas herramientas facilitan el acceso a la información y contribuyen a la continuidad de las actividades institucionales, también han incrementado los riesgos relacionados con accesos no autorizados, vulnerabilidades, pérdida de información y problemas en la disponibilidad de los servicios (NIST, 2020).

El problema central está en la limitada disponibilidad de recursos técnicos para evaluar preventivamente la seguridad de los servicios institucionales. Actualmente, el ISU Sucre no cuenta con un ambiente aislado que permita ejecutar pruebas de vulnerabilidad, realizar simulaciones de ataques y monitorear eventos sin afectar los sistemas en funcionamiento. Esta limitación dificulta la aplicación continua de controles asociados con ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5, particularmente en gestión de vulnerabilidades, monitoreo, control de accesos y también en respuesta ante incidentes (ISO/IEC, 2022; NIST, 2020).

Como consecuencia, la institución dispone de menos capacidad para anticipar amenazas, para detectar señales tempranas de incidentes y también para responder oportunamente. Todo esto incrementa la exposición de activos críticos y además dificulta la trazabilidad de los eventos registrados. Ante ello, se plantea implementar un laboratorio virtual de ciberseguridad que funcione como un entorno aislado donde sea posible analizar vulnerabilidades y también comprobar controles, todo sin intervenir directamente las plataformas institucionales.

1.3 Pregunta de investigación

¿De qué manera la implementación de un laboratorio virtual de ciberseguridad basado en los estándares ISO/IEC 27001 y NIST SP 800-53 contribuye al fortalecimiento de la seguridad digital del Instituto Superior Universitario Sucre?

1.4 Descripción del proyecto

El proyecto plantea la implementación de un laboratorio virtual de ciberseguridad para mejorar la seguridad del entorno digital del Instituto Superior Universitario Sucre. Como parte inicial, se desarrolló una arquitectura técnica que permita ordenar su puesta en marcha.

Los laboratorios virtuales de ciberseguridad, también conocidos como cyber ranges, se utilizan como entornos controlados para simular escenarios de ataque y defensa. En estos espacios es posible desarrollar prácticas técnicas, analizar vulnerabilidades y comprobar controles de seguridad sin intervenir directamente sobre infraestructuras reales (Chouliaras et al., 2021; Yamin et al., 2020).

Para este caso se utiliza VirtualBox como plataforma de virtualización. Sobre este entorno se integran Kali Linux orientado a pruebas controladas, pfSense enfocado en la segmentación y filtrado de tráfico, un servidor Ubuntu con WordPress que actúa como objetivo de evaluación, junto con Wazuh para el monitoreo y análisis de eventos de seguridad.

La arquitectura está organizada en tres zonas: LAN, DMZ y red de ataque. Con esta separación es posible representar escenarios cercanos a una red institucional básica, observar la comunicación entre segmentos, detectar servicios expuestos y también verificar controles sin comprometer servicios reales.

El diseño se basa en la ISO/IEC 27001 y la NIST SP 800-53 porque son útiles para organizar el monitoreo, la respuesta, el control de seguridad y la gestión de riesgos. De la misma manera, se toman en cuenta los principios de confianza cero y defensa en profundidad, porque contribuyen a

disminuir el movimiento lateral dentro del laboratorio, a segregar recursos y a restringir accesos (Rose et al., 2020).

Metodológicamente, el proyecto está planteado como una intervención aplicada con diseño cuasiexperimental. Se compara una línea base inicial con los resultados obtenidos después de implementar el laboratorio, lo que permite valorar cambios en vulnerabilidades, detección y respuesta. Además del componente técnico, la propuesta puede aportar a la capacitación práctica y a una cultura institucional más preventiva en ciberseguridad.

1.5 Objetivos del proyecto

1.5.1 Objetivo general

Implementar un laboratorio virtual de ciberseguridad basado en los estándares internacionales ISO/IEC 27001 y NIST SP 800-53, para fortalecer la protección del entorno digital institucional y optimizar la capacidad de respuesta ante amenazas cibernéticas en el ISU Sucre de Quito, Ecuador.

1.5.2 Objetivos específicos

1. Realizar un diagnóstico actual del nivel de seguridad informática y las principales vulnerabilidades presentes en las plataformas institucionales del ISU Sucre.

2. Diseñar la arquitectura técnica del laboratorio virtual de ciberseguridad, basado en los controles de seguridad de los estándares internacionales ISO/IEC 27001 y NIST SP 800-53.

3. Implementar el laboratorio virtual como entorno controlado para la simulación de ataques y aplicación de medidas de defensa en el portal web y las aulas virtuales.

1.6 Justificación del proyecto

La implementación de un laboratorio virtual de ciberseguridad en el ISU Sucre surge por la creciente dependencia institucional de plataformas digitales y por el incremento de amenazas que pueden llegar a afectar la continuidad académica junto con la protección de la información. En este escenario, la institución requiere un entorno de pruebas controlado donde se pueda realizar análisis de vulnerabilidades, simulaciones de ataque y también evaluación de controles sin intervenir directamente en los sistemas de producción, justo como recomiendan estudios relacionados con la seguridad en entornos educativos (Moreano Guerra et al., 2023).

En la situación actual, la institución no dispone de un espacio técnico permanente para hacer pruebas de penetración, análisis de vulnerabilidades o simulaciones de ataque sobre sistemas equivalentes a los productivos. Un laboratorio virtual sirve para cubrir esa brecha por medio de un entorno separado, documentado y repetible. Además, los cyber ranges se han empleado en contextos educativos y organizacionales como un apoyo para entrenamiento técnico, validación de controles y también para la mejora de la respuesta frente a incidentes.

El proyecto toma lineamientos de ISO/IEC 27001 y NIST SP 800-53 con el objetivo de evaluar controles de seguridad dentro de un entorno de pruebas. Que se pueda contar con un espacio donde estos controles se analicen antes de aplicarse en sistemas reales es algo que resulta útil para reducir riesgos durante su implementación, y además aporta información valiosa para mejorar los procesos de seguridad institucional.

Este proyecto plantea un aporte en dos dimensiones. Primero en la dimensión institucional, que brinda apoyo al personal técnico responsable de la infraestructura y del monitoreo. Y en la dimensión académica, se puede desarrollar prácticas de ciberseguridad para estudiantes y docentes, todas ellas vinculadas con escenarios reales de análisis, detección y también respuesta.

Desde un punto de vista técnico, contar con un laboratorio facilita la observación de controles de seguridad en un entorno educativo y lo más importante es que es bajo condiciones controladas. Obteniendo resultados que sirven como antecedente para futuras acciones institucionales

relacionadas con gestión de vulnerabilidades, monitoreo centralizado, así como respuesta a incidentes.

Lo que le da pertinencia a este proyecto es, fundamentalmente, la relación directa que guarda con las necesidades de seguridad digital del ISU Sucre. Por lo que respecta a la puesta en marcha del laboratorio, cabe decir que esta facilita el control preventivo de los riesgos; al mismo tiempo, hace posible trabajar con estándares internacionales de manera efectiva, y además ofrece un fundamento para actividades futuras, tales como la capacitación, la validación y la mejora constante.

1.7 Alcance del proyecto

El proyecto se desarrolló en el Instituto Superior Universitario Sucre, enfocado sobre todo en la infraestructura tecnológica con la que se manejan los servicios académicos y administrativos. El alcance comprende el diseño, la configuración, la implementación y también la validación inicial de un laboratorio virtual de ciberseguridad, pensado para simular amenazas y para evaluar controles en un ambiente controlado.

En lo técnico, se realizó un diagnóstico inicial de los servicios digitales institucionales, en concreto el portal web junto con el entorno virtual Moodle. La revisión buscaba identificar configuraciones inseguras, servicios expuestos y también los controles que ya existían. Luego, se implementó un entorno virtual con redes segmentadas y herramientas de análisis para poder recrear escenarios de ataque y defensa; este tipo de práctica se usa para evaluar controles de seguridad dentro de entornos organizacionales (Conti et al., 2018).

No se incluyen dentro del alcance ni la aplicación directa de medidas en los sistemas de producción, ni tampoco la adquisición de infraestructura física, ni mucho menos el desarrollo completo de políticas institucionales sobre seguridad. Por el lado de la validación, esta se restringe a las pruebas controladas que se llevan a cabo en el laboratorio. Con todo, los resultados que allí se obtengan bien podrían servir de base para acciones futuras de monitoreo, análisis o respuesta ante incidentes.

CAPÍTULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

La ciberseguridad tiene un papel importante en la protección de los servicios digitales utilizados por las instituciones de educación superior, sobre todo cuando administran plataformas académicas, procesos administrativos y datos sensibles de estudiantes y docentes.

En este capítulo se desarrollan los principales fundamentos teóricos relacionados con la implementación del laboratorio virtual de ciberseguridad en el ISU Sucre. También se revisan conceptos de seguridad de la información, modelos como defensa en profundidad y Zero Trust, además de estándares internacionales como ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5.

El capítulo también incluye la metodología aplicada en el proyecto. Se utilizó un enfoque mixto y un diseño cuasiexperimental pretest–postest para analizar los cambios entre el estado inicial y final del entorno evaluado mediante matrices de análisis, pruebas controladas y registros de eventos.

2.1 Ciberseguridad y fortalecimiento digital en instituciones educativas

Dentro de la ciberseguridad encontramos prácticas, procesos, tecnologías y controles destinados a proteger sistemas, redes, aplicaciones y datos frente a accesos indebidos, ataques, daños o interrupciones. En la educación superior, la importancia aumenta porque las plataformas académicas, sistemas administrativos y servicios web mantienen una concurrencia alta de usuarios y la información que se maneja es altamente sensible.

El fortalecimiento digital institucional puede entenderse como la capacidad de reconocer riesgos y proteger activos, además de detectar comportamientos anómalos, responder a incidentes y recuperar la continuidad de los servicios en tiempos récord. Esta lectura coincide con el NIST Cybersecurity Framework 2.0, que organiza la gestión de ciberseguridad en las siguientes funciones: gobernar, identificar, proteger, detectar, responder y recuperar (National Institute of Standards and Technology [NIST], 2024).

En el ISU Sucre, la dependencia de plataformas digitales para la gestión académica y administrativa requiere mecanismos de evaluación, monitoreo y respuesta que reduzcan riesgos sin afectar los sistemas productivos. Frente a esta necesidad, el laboratorio virtual de

ciberseguridad ofrece un entorno controlado para simular amenazas, analizar vulnerabilidades y validar controles.

2.2 Fundamentos de Seguridad de la Información

La seguridad de la información constituye la base de la ciberseguridad organizacional, porque orienta la protección de los activos digitales frente a accesos no autorizados, alteraciones indebidas o falta de disponibilidad. ISO/IEC 27001:2022 define las condiciones para la implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, tomando en cuenta el análisis y manejo de riesgos en el entorno particular de cada organización (ISO/IEC, 2022). La confidencialidad, la integridad y la disponibilidad son los tres principios en los que se basa esta perspectiva.

Estos principios guían el diseño del laboratorio virtual en este trabajo. Las pruebas controladas posibilitan la visualización de intentos de acceso no autorizado, eventos de seguridad, capacidades de respuesta y vulnerabilidades. De esa manera, los resultados obtenidos aportan a la protección de activos digitales y a la validación de controles técnicos aplicables al contexto del ISU Sucre.

2.3 Modelos Estratégicos de Seguridad

Los modelos estratégicos de seguridad permiten organizar la protección de los activos digitales mediante controles técnicos y administrativos. En un entorno institucional, estos modelos ayudan a reducir riesgos, limitar accesos no autorizados y mejorar la capacidad de detección y respuesta ante incidentes. En este caso, se trabajan dos enfoques principales de seguridad: defensa en profundidad y Zero Trust y su aplicación en el laboratorio virtual facilita la organización de controles por capas, la segmentación de la red, el monitoreo de eventos y la validación de accesos dentro de un entorno controlado.

2.3.1 Defense in Depth - Defensa en Profundidad

La defensa en profundidad consiste en aplicar varias capas de protección para evitar que un solo fallo comprometa todo el entorno tecnológico. Este enfoque no depende de un único control de

seguridad, sino de la combinación de medidas como segmentación de red, firewall, autenticación, monitoreo de eventos y respuesta ante incidentes.

En el laboratorio virtual del ISU Sucre, este modelo se aplica mediante la separación de zonas como LAN, DMZ y red de ataque, junto con el uso de pfSense para controlar el tráfico y Wazuh para monitorear eventos de seguridad. Si una capa es vulnerada, las demás ayudan a contener o detectar la actividad sospechosa.

Este enfoque se relaciona con las funciones del NIST CSF 2.0, especialmente identificar, proteger, detectar y responder, ya que permite gestionar riesgos de forma organizada y mejorar la postura de seguridad institucional (NIST, 2024).

2.3.2 Zero Trust Architecture — Arquitectura de confianza cero

La arquitectura Zero Trust se basa en el principio de no confiar automáticamente en ningún usuario, dispositivo o sistema, aunque se encuentre dentro de la red institucional. En lugar de asumir que todo lo interno es seguro, este modelo exige verificar continuamente los accesos y aplicar privilegios mínimos según la necesidad de cada usuario o servicio.

Según NIST SP 800-207, Zero Trust propone trasladar la seguridad desde un enfoque centrado únicamente en el perímetro de red hacia un modelo enfocado en usuarios, activos y recursos (Rose et al., 2020). En el laboratorio virtual, este enfoque se aplica de manera básica mediante el control de accesos, la segmentación de redes, la validación de tráfico permitido y el bloqueo de comunicaciones no autorizadas.

Aunque el proyecto no implementa una arquitectura Zero Trust completa, sí adopta principios fundamentales como la verificación de accesos, el mínimo privilegio y la restricción del movimiento lateral. Estos principios fortalecen el diseño del laboratorio y complementan el modelo de defensa en profundidad.

2.4. Estándares Internacionales de Ciberseguridad

Los estándares internacionales de ciberseguridad permiten ordenar la gestión de riesgos, seleccionar controles y evaluar la protección de activos digitales. Se toman en cuenta ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5 y NIST CSF 2.0 en este proyecto, ya que juntas hacen más fácil la conexión entre la gestión institucional de seguridad y las evidencias técnicas adquiridas en el laboratorio.

Por otra parte, el ISO/IEC 27001:2022 y el NIST no tienen exactamente la misma finalidad. La primera regla se centra en el Sistema de Gestión de Seguridad de la Información; por otro lado, NIST SP 800-53 Rev. 5 proporciona una lista pormenorizada de controles técnicos, organizacionales y de privacidad. Su uso combinado permite relacionar gestión de riesgos, controles aplicables y resultados de pruebas controladas.

2.4.1 ISO/IEC 27001:2022 aplicado a la ciberseguridad

El estándar ISO/IEC 27001:2022 define requisitos para establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (ISO/IEC, 2022). Desde esta norma, una organización puede gestionar riesgos considerando activos, amenazas, vulnerabilidades y controles adecuados para su tratamiento.

En el laboratorio propuesto, ISO/IEC 27001:2022 sirve como guía para ordenar la identificación de activos, el análisis de vulnerabilidades, el monitoreo de eventos y la validación de controles. Además, permite relacionar las pruebas con aspectos como gestión de vulnerabilidades técnicas, registro de eventos, control de accesos y segregación de redes.

2.4.2 NIST SP 800-53 Rev. 5 y NIST CSF 2.0

El estándar NIST SP 800-53 Rev. 5 brinda un extenso catálogo de controles de privacidad y seguridad para resguardar operaciones, activos organizacionales y sistemas de información contra diversas amenazas (NIST, 2020). En este proyecto, se emplea como punto de referencia para conectar las prácticas de seguridad adecuadas a contextos institucionales con los controles técnicos del laboratorio.

Los controles más importantes para el laboratorio están relacionados con la administración de riesgos, la supervisión de eventos, la protección de las comunicaciones, el monitoreo de incidentes y el control de accesos. Su aplicación se observa en la segmentación con pfSense, la detección mediante Wazuh, el análisis de vulnerabilidades y las acciones de contención aplicadas durante las pruebas.

El NIST CSF 2.0 complementa este análisis porque organiza la gestión de la ciberseguridad en funciones. Aunque el marco completo incluye gobernar, identificar, proteger, detectar, responder y recuperar, este proyecto trabaja sobre todo con las funciones identificar, proteger, detectar y responder, debido a su relación directa con los escenarios ejecutados en el laboratorio virtual.

2.5 Monitoreo de Eventos y Gestión de Incidentes mediante SIEM

El monitoreo de eventos es un componente fundamental dentro de la ciberseguridad, ya que permite observar el comportamiento de los sistemas, identificar actividades sospechosas y generar alertas ante posibles incidentes. Para ello, los sistemas SIEM centralizan y analizan registros provenientes de servidores, aplicaciones, dispositivos de red y otros componentes tecnológicos.

En el presente proyecto se utiliza Wazuh como herramienta SIEM de código abierto, debido a que permite recopilar eventos, analizarlos mediante reglas de detección y generar alertas de seguridad. De acuerdo con su documentación oficial, Wazuh analiza los logs mediante procesos de recolección, decodificación y coincidencia con reglas, con lo cual identifica eventos relevantes y los convierte en alertas de seguridad (Wazuh, s. f.).

Dentro del laboratorio virtual, hay que señalar que Wazuh desempeña un papel bastante central a la hora de evaluar la capacidad de detección y respuesta. Por medio de esta herramienta se registraron eventos vinculados a intentos fallidos de autenticación SSH, tráfico de reconocimiento que se generó con Nmap y también peticiones web que resultaron ser sospechosas. A partir de esos eventos, fue posible medir indicadores tales como la tasa de detección, el tiempo medio que tomaba detectar algo, y el tiempo medio que se requería para responder ante los incidentes simulados.

En cuanto a la incorporación del SIEM, esta relaciona el laboratorio con los controles de registro y monitoreo propios de la ISO/IEC 27001:2022, y también con las funciones Detect y Respond del NIST CSF 2.0. Además de generar evidencia técnica, cabe añadir que el monitoreo centralizado fortalece la capacidad institucional para identificar y atender eventos de seguridad con mayor celeridad.

2.6 Laboratorios virtuales de ciberseguridad

Los laboratorios virtuales de ciberseguridad, también conocidos como cyber ranges, funcionan como entornos controlados para simular redes, sistemas, servicios y escenarios de ataque sin afectar infraestructuras reales. Estos espacios ofrecen condiciones seguras para realizar pruebas, analizar vulnerabilidades, practicar técnicas de defensa y evaluar controles de seguridad.

Estos entornos ayudan a estructurar escenarios de entrenamiento, evaluación e investigación en ciberseguridad, mediante la integración de componentes de red, servicios, usuarios simulados, herramientas ofensivas y mecanismos de defensa. Por esta razón, los cyber ranges se utilizan como espacios para desarrollar capacidades técnicas y validar controles de seguridad en condiciones controladas (Chouliaras et al., 2021; Yamin et al., 2020).

En el ámbito educativo, estos laboratorios permiten fortalecer el aprendizaje práctico y el desarrollo de habilidades técnicas en actividades como escaneo de vulnerabilidades, pruebas de penetración, monitoreo de eventos, análisis de incidentes y respuesta ante amenazas. ENISA describe los cyber ranges como entornos virtuales controlados que simulan infraestructura de TI para ejecutar ejercicios técnicos de ciberseguridad (European Union Agency for Cybersecurity [ENISA], 2026).

Para los fines de esta investigación, se implementó un laboratorio con máquinas virtuales distribuidas en redes segmentadas. En concreto, dicho laboratorio incluye Kali Linux, pfSense, servidor Ubuntu junto con WordPress, y por su parte Wazuh. Con esta disposición se logra simular un entorno institucional de tipo básico, dentro del cual se llevan a cabo pruebas controladas de acceso no autorizado, escaneo, monitoreo de eventos y también detección de tráfico sospechoso.

Gracias a esta estructura, el equipo pudo obtener pruebas de índole metodológica y técnica que sirven para comparar el estado inicial y el estado final del entorno evaluado. De ese modo, se valida la implementación de controles de seguridad siguiendo los lineamientos de ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, y de paso las funciones operativas del NIST CSF 2.0.

2.7 Metodología del proyecto

La metodología del proyecto evalúa la implementación del laboratorio virtual de ciberseguridad como entorno técnico para el análisis, la simulación y la validación de controles. El enfoque aplicado responde a que la investigación no solo describe el problema, sino que plantea una intervención concreta para fortalecer la postura de seguridad digital del ISU Sucre.

La medición pretest–postest, que es un diseño cuasiexperimental, sirve de base para la metodología del desarrollo. Esta permite una comparación entre el estado inicial de los activos y servicios evaluados y los resultados logrados tras implementar el laboratorio. Esta decisión metodológica se toma para garantizar la efectividad de la propuesta a nivel técnico, sin que los sistemas productivos de la entidad se vean perjudicados.

2.7.1 Enfoque metodológico

El proyecto adopta un enfoque metodológico de carácter mixto, dentro del cual predomina el componente técnico-aplicado. En lo que respecta al componente cuantitativo, este se manifiesta, a manera de ilustración, en la medición de vulnerabilidades, los tiempos requeridos para la detección, los incidentes que fueron documentados, las acciones que se implementaron y, finalmente, los resultados comparativos obtenidos entre el pretest y el postest. Por su parte, el componente cualitativo se vincula con la selección de aquellos activos considerados fundamentales, el análisis del entorno institucional, la interpretación de los riesgos y la evaluación de las medidas de seguridad que han sido progresivamente implementadas.

La elección metodológica se justifica porque el problema no puede comprenderse solo desde una revisión documental. En la aplicación de la ciberseguridad en instituciones se requieren evidencias

técnicas verificables, obtenidas mediante pruebas controladas, monitoreo y validación de configuraciones. Por esta razón, el enfoque mixto integra contexto institucional y datos técnicos generados en el laboratorio.

2.7.2 Tipo de investigación

La investigación es de tipo aplicado, y esto es así porque responde a una necesidad específica del ISU Sucre, la cual consiste en evaluar de manera preventiva la seguridad digital. A diferencia de un trabajo de carácter meramente teórico, este proyecto lo que hace es implementar un laboratorio para llevar a cabo análisis de vulnerabilidades, simular escenarios de ataque, monitorear eventos y validar controles.

Por otro lado, dado que el estudio incluye activos, servicios y también riesgos iniciales, se puede decir que tiene un carácter descriptivo. Al mismo tiempo, resulta ser evaluativo, pues analiza los resultados previos y los posteriores a la intervención. Esta combinación de enfoques permite, por una parte, reconocer debilidades y, por otra, evaluar el progreso que se logró gracias al laboratorio.

2.7.3 Diseño Cuasiexperimental

El diseño que se adoptó para este trabajo es de tipo cuasiexperimental e incorpora pretest y postest. Lo que esto quiere decir es que se empieza con una medición inicial, después se aplica una intervención técnica y al final se comparan las variaciones que se alcanzaron. Por lo que hace a los indicadores objeto de examen, estos incluyen la capacidad de respuesta, los eventos que el SIEM registró, las vulnerabilidades que se identificaron y, asimismo, los tiempos que tomó la detección.

La elección de este diseño respondió a que el proyecto se concentra en establecer un entorno que ya viene definido de antemano, el cual cuenta con activos, servicios y escenarios que dan cuenta de las circunstancias propias del contexto tecnológico de ISU Sucre. Así las cosas, se mide la efectividad del laboratorio sin que haya necesidad de modificar los sistemas de producción, lo que permite mantener un ambiente controlado, aislado y que sea reproducible.

Por otro lado, no se emplea un diseño experimental puro, y la razón es que no hay asignación aleatoria de participantes, activos o escenarios, y tampoco se dispone de un grupo de control independiente. El estudio se lleva a cabo dentro de un contexto institucional específico, haciendo uso de los recursos que están disponibles y de unos activos que se seleccionaron atendiendo a su pertinencia frente al problema. Bajo estas condiciones, la comparación entre el antes y el después termina siendo metodológicamente más viable.

2.7.4 Población y muestra

La validación del proyecto se centró en los activos, servicios y escenarios de prueba implementados en el laboratorio virtual de ciberseguridad. Para ello, se empleó un muestreo no probabilístico intencional, seleccionando aquellos elementos con relación directa al problema de investigación y a los objetivos planteados. Entre los elementos seleccionados se encuentran el servidor web ubicado en la DMZ, el firewall pfSense para la segmentación y control del tráfico, el sistema SIEM Wazuh para el monitoreo de eventos de seguridad y los escenarios de evaluación definidos para el laboratorio. Estos escenarios permitieron realizar actividades de escaneo de vulnerabilidades, intentos de acceso no autorizado, generación de tráfico sospechoso y monitoreo de eventos.

De manera complementaria, se aplicó un cuestionario estructurado a 337 integrantes de la comunidad educativa del ISU Sucre (245 estudiantes y 92 docentes), con el propósito de obtener información sobre prácticas y percepción de seguridad digital. Los resultados obtenidos se utilizaron únicamente como apoyo para contextualizar la problemática institucional y no formaron parte de la validación técnica del laboratorio.

Como limitación, los resultados técnicos corresponden al contexto específico del ISU Sucre y no pretenden generalizarse de manera absoluta a otras instituciones de educación superior. La selección de activos, servicios y escenarios dependió de la información disponible, del alcance autorizado para las pruebas y de las condiciones del entorno virtual implementado.

2.7.5 Variables del estudio

La variable independiente es la ejecución del laboratorio virtual de ciberseguridad, entendido como un ambiente técnico, aislado y reproducible donde se ejecutan pruebas de vulnerabilidad, simulaciones de ataque, monitoreo de eventos y validación de controles basados en ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5.

El robustecimiento de la seguridad digital del ISU Sucre es lo que se considera como variable dependiente. Para su análisis se tienen en cuenta indicadores como la disminución de vulnerabilidades, el avance en la detección de sucesos, la trazabilidad de incidentes, la validación de controles y la habilidad para responder ante amenazas.

Se estudia el vínculo entre las dos variables mediante la comparación pretest-postest. Primero se determinan las condiciones de seguridad que ya existen; luego, en el laboratorio, se realizan controles y escenarios de prueba; finalmente, se examinan los indicadores para determinar si la intervención ha generado beneficios.

2.8 Técnicas de recolección de información

La recolección de información se realizó mediante técnicas cuantitativas y cualitativas, con el propósito de obtener datos técnicos del entorno evaluado y complementar el análisis con información relacionada con prácticas, percepciones y condiciones institucionales de ciberseguridad.

En el componente técnico, las pruebas de seguridad se sustentan en guías especializadas para evaluación de sistemas de información, las cuales recomiendan planificar, ejecutar, analizar hallazgos y definir acciones de mitigación dentro de procesos controlados de evaluación (Scarfone et al., 2008).

2.8.1 Técnicas cuantitativas

Las técnicas cuantitativas permitieron obtener datos medibles sobre el estado de seguridad del entorno evaluado, principalmente en relación con vulnerabilidades, eventos detectados y tiempos de respuesta.

Tabla 1.

Técnicas cuantitativas de recolección de información

Técnica	Propósito	Información obtenida
Análisis de vulnerabilidades	Identificar debilidades técnicas en servicios, configuraciones y aplicaciones del entorno evaluado.	Número de vulnerabilidades, nivel de criticidad y tipo de exposición.
Pruebas de penetración controladas	Ejecutar escenarios simulados de ataque dentro del laboratorio virtual.	Eventos generados, controles evaluados y comportamiento del sistema frente a amenazas.
Revisión de logs y eventos de seguridad	Analizar registros generados por los sistemas monitoreados mediante Wazuh.	Alertas, intentos de acceso no autorizado, tráfico sospechoso, MTTD y MTTR.
Encuesta estructurada	Obtener información complementaria sobre percepción y prácticas de seguridad digital de la comunidad académica.	Frecuencias y porcentajes sobre prácticas de seguridad, uso de contraseñas, autenticación en dos factores, capacitación y percepción de riesgos.

Nota. La tabla sintetiza las técnicas cuantitativas aplicadas para obtener datos medibles sobre vulnerabilidades, eventos de seguridad, tiempos de respuesta y percepción de riesgos en el entorno evaluado.

2.8.2 Técnicas cualitativas

Las técnicas cualitativas permitieron complementar los resultados técnicos mediante información relacionada con el contexto institucional, las prácticas internas de seguridad y la documentación existente sobre gestión de ciberseguridad.

Tabla 2.

Técnicas cualitativas de recolección de información

Técnica	Propósito	Información obtenida
Entrevista semiestructurada	Recoger información del área TIC sobre accesos, monitoreo, atención de eventos y limitaciones de seguridad.	Criterios del personal técnico sobre controles existentes, activos críticos, necesidades de monitoreo y respuesta ante incidentes.
Análisis documental	Revisar los documentos disponibles en la Unidad de TIC sobre seguridad, activos tecnológicos y soporte de servicios.	Se encontraron pocos documentos relacionados con ciberseguridad y varios temas pendientes de organización dentro del ISU Sucre.

Nota. Estas técnicas permitieron complementar la revisión técnica del laboratorio con información proporcionada por el área TIC y con la documentación disponible en el ISU Sucre.

Con la utilización de estas técnicas se logró obtener información para el análisis comparativo pretest–postest y para vincular los hallazgos con los controles de seguridad definidos en ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5 y las funciones operativas del NIST CSF 2.0.

2.9 Instrumentos de recolección de datos

Con los instrumentos de recolección de datos se logró registrar, organizar y analizar la información obtenida en las técnicas aplicadas. Permitiendo documentar evidencia técnica, describir escenarios de prueba y comparar los resultados del pretest y postest.

Tabla 3.

Instrumentos de recolección de datos utilizados en la investigación

Técnica	Instrumento	Descripción
Análisis de vulnerabilidades	Matriz de identificación de vulnerabilidades	Se usó para organizar activos revisados, debilidades encontradas, criticidad, impacto, probabilidad, nivel de riesgo y controles sugeridos. Revisar Anexo 1.

Pruebas de penetración	Ficha de evaluación de pruebas	Permitió registrar escenarios ejecutados, herramientas usadas, resultados obtenidos, controles revisados y observaciones de cada prueba. Revisar Anexo 2.
Revisión de logs y eventos de seguridad	Matriz pretest–postest	Sirvió para comparar los cambios entre la situación inicial y la posterior implementación del laboratorio. Revisar Anexo 3.
Entrevista semiestructurada	Guía de entrevista	Recogió información del personal técnico sobre controles existentes, necesidades, limitaciones y prácticas de ciberseguridad. Revisar Anexo 4.
Encuesta estructurada	Cuestionario estructurado	Su aplicación tuvo carácter complementario y se utilizó para contextualizar la situación institucional respecto a prácticas de seguridad digital. Revisar Anexo 5.
Análisis documental	Ficha de análisis documental	Ayudó a revisar documentos disponibles, documentos faltantes y temas que requerían organización dentro del ISU Sucre. Revisar Anexo 6.

Nota. La tabla reúne los instrumentos usados para registrar información técnica, opiniones del área TIC, respuestas de la comunidad académica y documentos institucionales revisados durante el proyecto.

Con los resultados obtenidos se logró establecer la línea base de seguridad, además de documentar la ejecución de pruebas controladas y comparar los indicadores del pretest y postest. A partir de esta información, las matrices y fichas aplicadas respaldaron la evaluación de la efectividad del laboratorio virtual de ciberseguridad.

CAPÍTULO 3. IMPLEMENTACIÓN DEL LABORATORIO VIRTUAL

En esta sección se describe la implementación del laboratorio virtual de ciberseguridad orientado al fortalecimiento digital del ISU Sucre. Presentando el diagnóstico inicial, el diseño de la arquitectura, la segmentación de red, la configuración de máquinas virtuales y la integración de herramientas de monitoreo y análisis de eventos.

El laboratorio se implementó en VirtualBox y en él se incluyeron varios componentes. En concreto, se usó pfSense para segmentar y regular el tráfico; por otro lado, Kali Linux sirvió para hacer las pruebas controladas; se dispuso también de un servidor Ubuntu con WordPress, el cual funcionó como objetivo de evaluación; y finalmente, se incorporó Wazuh como SIEM. Todas estas herramientas hicieron posible trabajar en un ambiente aislado, con controles que tenían que ver con la gestión de vulnerabilidades, el control de acceso, la vigilancia, la seguridad de las redes y también la respuesta ante situaciones imprevistas.

3.1. Diagnóstico inicial del entorno de seguridad

El diagnóstico inicial constituyó el punto de partida para la implementación del laboratorio virtual de ciberseguridad, ya que permitió identificar los activos tecnológicos relevantes, las condiciones generales del entorno digital institucional y las principales amenazas asociadas a los servicios expuestos. Esta fase permitió establecer una visión preliminar del estado de seguridad del ISU Sucre antes de la intervención técnica.

Con el análisis se identificó componentes que requieren protección, como lo son las plataformas web, servicios de red, mecanismos de autenticación y datos institucionales. Con esta información se diseñó una arquitectura de laboratorio controlada y segmentada, vinculada con controles seleccionados de ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5. La línea base y los resultados detallados del pretest se presentan en el Capítulo 4 y en los anexos.

3.1.1 Identificación de activos tecnológicos institucionales

Con la identificación de activos tecnológicos se logró reconocer los componentes que soportan los servicios digitales del ISU Sucre y que, por su función institucional, requieren protección frente a amenazas de ciberseguridad. Este levantamiento de información ayudó a definir qué sistemas, servicios e información debían considerarse en el diagnóstico y representarse después en el laboratorio virtual.

Dentro de los activos identificados están la infraestructura tecnológica, plataformas institucionales, servicios de red, mecanismos de acceso y datos académicos o administrativos. Esta clasificación permitió estimar el nivel de exposición del entorno y seleccionar los elementos que formarían parte del diseño del laboratorio.

Tabla 4.

Activos tecnológicos del ISU Sucre

Activo tecnológico	Descripción	Importancia para el proyecto
Servidor VPS institucional	Infraestructura virtual donde se alojan servicios digitales del ISU Sucre, como el portal web y plataformas académicas.	Se consideró por su exposición a Internet y por los riesgos asociados con accesos no autorizados o fallos en aplicaciones web.
Portal web institucional	Sitio utilizado para publicar información académica, administrativa y comunicacional.	Al ser un servicio público, permitió observar riesgos relacionados con formularios, configuraciones débiles y disponibilidad del sitio.
Plataforma Moodle	Entorno virtual usado por estudiantes y docentes para actividades académicas.	Su revisión fue importante por el manejo de cuentas de usuario, acceso a contenidos académicos y continuidad de clases virtuales.
Servidor físico institucional	Equipo local que puede alojar servicios internos o recursos de capacitación.	Se incluyó porque sus configuraciones internas y accesos también pueden influir en la seguridad del entorno institucional.
Datos institucionales	Información académica, administrativa y personal	Se trataron como un elemento transversal, ya que están presentes en

	manejada en las plataformas digitales.	varios servicios y pueden verse afectados por pérdida, cambio no autorizado o acceso indebido.
Servicios de red y autenticación	Servicios web, bases de datos, acceso remoto y mecanismos de inicio de sesión.	Ayudaron a definir pruebas sobre puertos expuestos, accesos no autorizados y controles de autenticación dentro del laboratorio.

Nota. La tabla presenta los activos tecnológicos considerados en el diagnóstico inicial del proyecto, priorizando aquellos relacionados con servicios digitales, datos institucionales y mecanismos de acceso que requieren protección dentro del entorno evaluado.

El diseño del laboratorio se orientó hacia aquellos servicios que resultan fundamentales dentro del contexto institucional, a saber: plataformas web, acceso remoto, supervisión de eventos y protección de datos. Y esto se hizo gracias a que previamente se identificaron los activos. Partiendo de esa base, fue posible establecer los controles de seguridad y también los escenarios de prueba que luego se utilizarían en las etapas posteriores.

3.1.2 Análisis del entorno digital del ISU Sucre

El entorno digital del ISU Sucre está compuesto por una serie de servicios tecnológicos cuyo propósito es apoyar la gestión académica, la administrativa y también la comunicacional dentro de la institución. Si se mencionan los principales componentes, allí se encuentran el portal web institucional, la plataforma Moodle, los servicios de red, algunos mecanismos de autenticación y, por supuesto, repositorios donde se guarda información tanto académica como administrativa.

El portal web, Moodle, los servicios de red y la información institucional fueron revisados porque sostienen actividades diarias del ISU Sucre. En ellos se publican contenidos, se gestionan accesos y se maneja información académica y administrativa. Por eso, una configuración débil, un puerto innecesario o un servicio sin actualizar puede aumentar la exposición del entorno. Para ordenar esta revisión se tomaron como referencia ISO/IEC 27001:2022, en la gestión de riesgos sobre activos de información, y NIST SP 800-53 Rev. 5, en controles de acceso, monitoreo y comunicaciones (ISO/IEC, 2022; NIST, 2020).

Con el análisis se logró identificar la necesidad de contar con un entorno controlado que represente riesgos del contexto institucional sin intervenir sistemas productivos. Por ello, el laboratorio se diseñó como un espacio segmentado y aislado para simular servicios institucionales, generar eventos de seguridad, evaluar vulnerabilidades y validar controles técnicos. Esta aproximación resulta pertinente en instituciones educativas que requieren evaluación continua de seguridad de la información (Moreano Guerra et al., 2023).

3.1.3 Identificación de amenazas y vulnerabilidades iniciales

Durante el diagnóstico inicial se revisaron amenazas y vulnerabilidades potenciales asociadas a servicios web, mecanismos de autenticación, configuraciones de red y capacidades de monitoreo del entorno digital del ISU Sucre. Con este análisis se definieron los escenarios de riesgo que debían representarse en el laboratorio virtual, sin intervenir directamente los sistemas productivos.

El escaneo de puertos, la explotación de vulnerabilidades en la web, el acceso sin autorización, el tráfico sospechoso y el ataque por fuerza bruta fueron las amenazas que se tuvieron en cuenta. En aplicaciones web, estos peligros están vinculados con configuraciones inseguras, errores de control de acceso, componentes en riesgo y problemas de autenticación. Estos temas son tratados por OWASP (OWASP Foundation, 2025).

Las debilidades iniciales se vincularon con configuraciones poco seguras, servicios expuestos, falta de segmentación, supervisión escasa y fallos de acceso. Estas condiciones pueden afectar la confidencialidad, integridad y disponibilidad de la información, principios centrales de ISO/IEC 27001:2022 (ISO/IEC, 2022). Con base en este diagnóstico se definieron cuatro escenarios de prueba: escaneo de vulnerabilidades, acceso no autorizado, tráfico sospechoso y monitoreo de eventos. Los resultados específicos se detallan en el Capítulo 4 y en los anexos.

3.1.4 Síntesis del diagnóstico inicial

El diagnóstico inicial permitió determinar que el ambiente digital del ISU Sucre necesita procedimientos de evaluación, seguimiento y control con el objetivo de reforzar la seguridad de

sus servicios tecnológicos. Se detectaron activos esenciales, riesgos potenciales y debilidades relacionadas con servicios expuestos, configuraciones inseguras, control de accesos y escasas capacidades para detectar eventos.

Estos descubrimientos fueron utilizados como fundamento para la creación de un laboratorio virtual que está segmentado, regulado y en concordancia con las normas internacionales de ciberseguridad. La arquitectura propuesta permitió representar escenarios de riesgo comunes en entornos institucionales, tales como escaneo de vulnerabilidades, intentos de acceso no autorizado, generación de tráfico sospechoso y monitoreo de eventos. La línea base cuantitativa y los resultados específicos del pretest se presentan en el Capítulo 4 y en los anexos correspondientes.

3.2 Diseño de la arquitectura del laboratorio virtual

La decisión de estructurar el laboratorio haciendo uso de redes LAN, una DMZ y también una red de ataque fue, en esencia, una respuesta directa a los hallazgos que dejó el diagnóstico inicial. Estos hallazgos fueron, concretamente: servicios que se encontraban expuestos, una ausencia total de segmentación, un monitoreo bastante limitado y, por otro lado, la necesidad de validar controles sin que se afectaran los sistemas productivos. Ahora bien, la conexión que se estableció entre el problema detectado y la solución propuesta hizo posible que la arquitectura no se limitara únicamente a una configuración operativa, sino que más bien terminara funcionando como una respuesta técnica frente a riesgos muy particulares del entorno institucional.

Con el fin de no hacer pruebas sobre los sistemas reales del ISU Sucre, se implementó el laboratorio como un espacio aparte dentro de VirtualBox. Allí se separaron las redes LAN, la DMZ y la red de ataque, para que los eventos que se generaran se pudieran revisar sin poner en riesgo las plataformas institucionales.

En esta arquitectura, pfSense permitió controlar el tráfico entre segmentos, mientras que Wazuh facilitó la revisión de registros y alertas producidas durante las pruebas. Esta organización permitió aplicar controles relacionados con gestión de vulnerabilidades, seguridad de redes, registro,

monitoreo y respuesta ante incidentes, tomando como referencia ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.2.1 Modelo de arquitectura propuesto

El modelo de arquitectura propuesto se estructuró por capas, con el propósito de organizar los componentes del laboratorio virtual según su función dentro del entorno de pruebas. Esta organización permitió separar la infraestructura de virtualización, los segmentos de red, los servicios simulados, las herramientas de monitoreo y la administración del laboratorio.

Tabla 5.

Estructura de modelo propuesto

Capa	Descripción
Capa de Infraestructura Física y Virtualización	Incluye el equipo host y la plataforma VirtualBox, donde se alojan las máquinas virtuales del laboratorio.
Capa de Red y Segmentación	Redes virtuales segmentadas y reglas de firewall para separar las zonas funcionales del laboratorio.
Capa de Servicios	Servidor Ubuntu con WordPress, configurado como activo objetivo para las pruebas controladas.
Capa de Seguridad y Monitoreo	Integración de pfSense y Wazuh para el control del tráfico, registro de eventos y generación de alertas de seguridad.
Capa de Gestión y Administración	Configuración, supervisión y mantenimiento del laboratorio virtual.

Nota. El modelo propuesto organiza el laboratorio virtual por capas funcionales. Así se facilita la separación de servicios, el control del tráfico entre redes y el monitoreo de eventos de seguridad.

La estructura se vincula con controles de ISO/IEC 27001:2022 como A.8.8, A.8.15, A.8.16, A.8.20 y A.8.22, y con controles NIST SP 800-53 Rev. 5 relacionados con protección de límites, control de acceso y monitoreo de eventos.

3.2.2 Topología lógica de red

La topología lógica del laboratorio virtual se organizó con redes segmentadas conectadas a través del firewall pfSense. Este componente funcionó como punto central para controlar el tráfico entre las zonas definidas. Con esta distribución se separaron la red LAN, la DMZ y la red de ataque, lo que facilitó la ejecución de pruebas de seguridad en un entorno controlado.

En la práctica, la separación entre LAN, DMZ y red de ataque ayudó a controlar qué tráfico podía pasar por pfSense y qué comunicaciones debían restringirse. Durante las pruebas, esta división también permitió revisar en Wazuh los eventos generados desde la red de ataque hacia el servidor ubicado en la DMZ. Por esta razón, la configuración se tomó como evidencia técnica para los controles SC-7 Boundary Protection de NIST SP 800-53 Rev. 5, A.8.20 Seguridad de redes y A.8.22 Segregación de redes de ISO/IEC 27001:2022 (ISO/IEC, 2022; NIST, 2020).

3.2.3 Segmentación y zonas de seguridad

La segmentación del laboratorio virtual se diseñó con el propósito de separar los componentes según su función y nivel de exposición. Para ello, se definieron tres segmentos principales: red LAN, red DMZ y red de ataque, interconectados y controlados mediante el firewall pfSense. Esta separación permitió limitar la comunicación entre zonas, controlar el tráfico permitido y reducir el riesgo de movimiento lateral dentro del entorno de pruebas.

Tabla 6.

Zonas de seguridad del laboratorio virtual

Zona de seguridad	Segmento / dirección	Función dentro del laboratorio
LAN	192.168.10.0/24	Aloja componentes de administración y monitoreo, como Wazuh, para la gestión y análisis de eventos de seguridad.
DMZ	192.168.20.0/24	Contiene el servidor Ubuntu con WordPress, utilizado como activo objetivo para las pruebas controladas.

Red de ataque	192.168.30.0/24	Aloja la máquina Kali Linux, desde donde se ejecutan pruebas controladas de escaneo, acceso no autorizado y generación de tráfico sospechoso.
Firewall	pfSense	Controla el tráfico entre LAN, DMZ y red de ataque mediante reglas de filtrado y segmentación.

Nota. La tabla presenta las zonas de seguridad implementadas en el laboratorio virtual.

Con esta segmentación, los servicios expuestos se situaron en la DMZ, las herramientas de vigilancia en la LAN y las pruebas ofensivas en una red distinta. Se logró evaluar los controles de seguridad en un ambiente que no pertenecía a los sistemas de producción gracias a la distribución.

3.2.4 Modelo de control de accesos

El modelo de control de accesos que se utilizó en el laboratorio virtual partió del principio de mínimo privilegio, de manera que únicamente se permitieron las comunicaciones que resultaban estrictamente necesarias entre los segmentos que se habían definido, los cuales fueron: LAN, DMZ y red de ataque. Para ello se emplearon reglas de firewall en pfSense, y el propósito de estas era dirigir el tráfico entre las distintas zonas y también restringir aquellos accesos que no estaban permitidos hacia los servicios del servidor que se encontraba situado en la DMZ.

Por lo que hace a los servicios, hay que decir que en el servidor Ubuntu se implementaron unos controles de autenticación más bien elementales, y esto se hizo sobre todo para la gestión del entorno WordPress y para el acceso remoto a través de SSH. Esos controles, los cuales se monitorizaron por medio de Wazuh, lo que hicieron fue facilitar la evaluación de los intentos fallidos de autenticación, así como los accesos no autorizados y también los eventos que venían vinculados con credenciales.

Este modelo se alinea con los controles A.5.15 Control de acceso, A.5.16 Gestión de identidad y A.5.17 Información de autenticación de ISO/IEC 27001:2022, así como con los controles AC-2 Gestión de cuentas y AC-6 Mínimo privilegio de NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.3 Componentes y diagrama del laboratorio

El laboratorio virtual de ciberseguridad se construyó a partir de máquinas virtuales y servicios que fueron organizados conforme a la arquitectura segmentada que se había definido con anterioridad. Cada uno de los componentes cumplió una función específica dentro del entorno de pruebas, y esto hizo posible simular ataques controlados, por un lado, proteger el tráfico entre zonas, por otro monitorear eventos y finalmente generar evidencia técnica para la evaluación que se realizaría posteriormente.

En lo que respecta a la estructura del laboratorio, esta se sostuvo sobre herramientas de virtualización, firewall, monitoreo y análisis de seguridad. Gracias a ello se pudo representar un entorno institucional controlado sin que se vieran afectados los sistemas productivos del ISU Sucre. Esta forma de organizar el laboratorio se alinea con los principios de defensa en profundidad, segmentación de red y monitoreo continuo, principios que, por lo demás, son recomendados por la ISO/IEC 27001:2022 y el NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.3.1 Componentes del laboratorio virtual

La selección de herramientas respondió a criterios de pertinencia técnica, costo, reproducibilidad y relación con el objetivo académico del proyecto. Se eligió pfSense por su capacidad para implementar segmentación, reglas de firewall y control de tráfico entre zonas. Kali Linux se incorporó por sus herramientas de evaluación ofensiva, ampliamente utilizadas en pruebas controladas; servidor Ubuntu con WordPress, por representar un servicio web institucional expuesto; y Wazuh, por ofrecer monitoreo centralizado, correlación de eventos y generación de alertas sin requerir licenciamiento propietario.

Estas herramientas son apropiadas para un laboratorio académico, porque permiten simular situaciones de riesgo, documentar evidencias técnicas y validar controles con recursos a los que se puede acceder con facilidad; en cambio, las opciones comerciales no lo son. Sin embargo, su uso

en producción requeriría cambios adicionales en cuanto a rendimiento, disponibilidad, gestión de identidades, respaldo y procedimientos formales de funcionamiento.
El laboratorio virtual se estableció utilizando máquinas virtuales segmentadas en diferentes partes de la red. Cada elemento desempeñó un papel particular en el ambiente de pruebas y ayudó a simular un escenario institucional controlado para realizar actividades de monitoreo, análisis y respuesta ante incidentes de seguridad.

Cada componente desempeñó un papel determinado en el proceso de pruebas durante la operación del laboratorio. pfSense fue la herramienta que controló la comunicación entre los segmentos; Kali Linux creó los escenarios de evaluación; Ubuntu Server con WordPress se desempeñó como servicio objetivo, y Wazuh reunió los eventos ocurridos durante las pruebas para su análisis futuro.

3.3.2 Roles de las máquinas virtuales.

Cada máquina virtual del laboratorio cumplió un rol específico dentro del entorno de pruebas. Esta distribución permitió separar las funciones de ataque controlado, servicio objetivo, monitoreo y control de tráfico, garantizando una arquitectura ordenada y coherente con los objetivos del proyecto.

Tabla 7.

Componentes y roles dentro de la arquitectura

Componente	Plataforma	Rol dentro del laboratorio	Función principal
Firewall perimetral	pfSense	Control de tráfico entre segmentos	Control de la comunicación entre LAN, DMZ y red de ataque mediante reglas de firewall.
Equipo atacante	Kali Linux	Máquina de pruebas controladas	Ejecución de escaneos, intentos de acceso no autorizado y generación de tráfico sospechoso.
Servidor objetivo	Ubuntu Server + WordPress	Servicio institucional simulado	Alojamiento del servicio web evaluado y generación de registros del sistema, Apache y SSH para su análisis.

Sistema de monitoreo	Wazuh SIEM	Monitoreo y correlación de eventos	Centralización de registros, detección de eventos de seguridad y generación de alertas durante las pruebas.

Nota. La tabla describe los componentes principales del laboratorio virtual, la plataforma utilizada, el rol asignado y la función que cumplen dentro del entorno de pruebas.

El establecimiento de roles posibilitó una distinción nítida entre los elementos defensivos, ofensivos y los de monitoreo del laboratorio. La entidad permitió que se llevaran a cabo escenarios controlados y además que se obtuviera evidencia técnica para evaluar los controles implementados previamente.

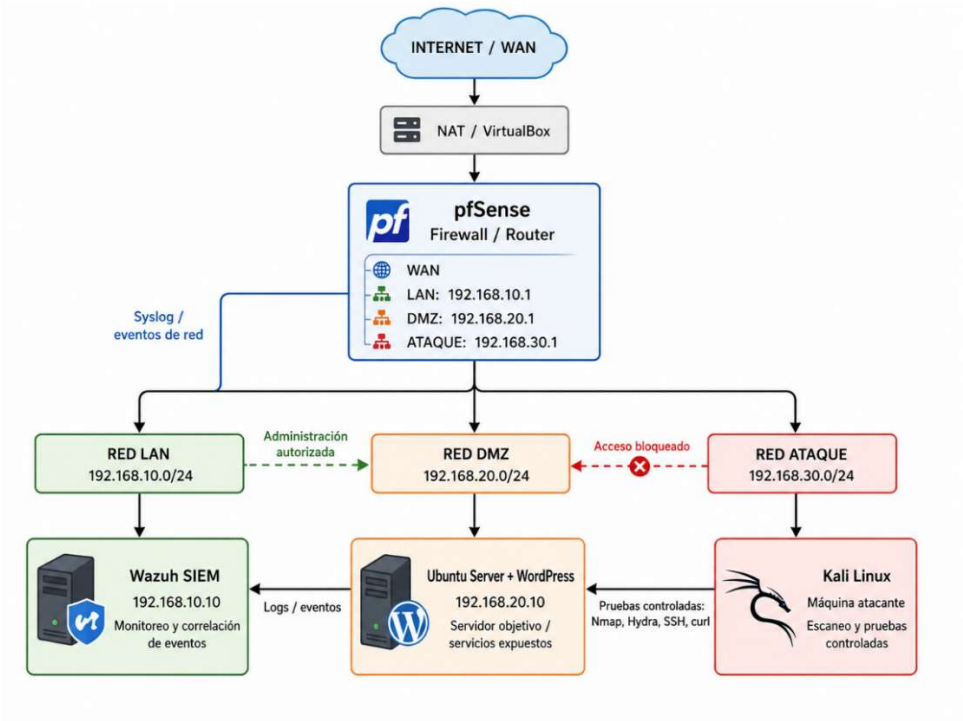
3.3.3 Diagrama de red y flujo de comunicación

El diagrama de red permite observar la organización del laboratorio virtual y la separación entre la LAN, la DMZ y la red de ataque. En esta estructura, pfSense se ubicó como el equipo encargado de regular la comunicación entre los segmentos, de acuerdo con las reglas configuradas para cada zona.

El flujo principal de comunicación parte desde Kali Linux, en la red de ataque, hacia el servidor Ubuntu con WordPress situado en la DMZ. Durante las pruebas, el servidor registra los eventos y los envía a Wazuh, ubicado en la LAN, para su análisis y correlación. Con este flujo se evaluaron controles de segmentación, monitoreo y respuesta ante incidentes, en relación con ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

Figura 1.

Arquitectura implementada del laboratorio virtual de ciberseguridad



Nota. La figura presenta la arquitectura implementada del laboratorio virtual, segmentada mediante pfSense en red LAN, DMZ y red de ataque. Esta distribución facilitó la ejecución de pruebas controladas y la validación de controles de segmentación, monitoreo, detección y respuesta ante incidentes. Fuente: Elaboración propia.

3.4 Implementación del entorno virtual

La implementación se desarrolló como una fase de validación técnica del diseño propuesto, no solo como la instalación de máquinas virtuales. Cada componente respondió a una necesidad identificada en el diagnóstico: pfSense ayudó a reducir la exposición y controlar el tráfico; Wazuh mejoró la visibilidad de eventos; Kali Linux generó escenarios de prueba; y servidor Ubuntu con WordPress representó un activo institucional sujeto a evaluación.

Durante esta fase se ajustaron las máquinas virtuales, los segmentos de red junto con los servicios requeridos para ejecutar pruebas controladas, monitorear eventos y también validar controles de seguridad sin afectar los sistemas productivos del ISU Sucre. De esta forma, el entorno virtual quedó preparado como la parte operativa del laboratorio de ciberseguridad.

El laboratorio se implementó en VirtualBox con una arquitectura segmentada compuesta por LAN, DMZ y red de ataque, interconectadas mediante pfSense. Esta configuración integró Kali Linux, Ubuntu Server con WordPress y Wazuh SIEM. Además, se vinculó con controles seleccionados de ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5 relacionados con seguridad de redes, monitoreo y respuesta ante incidentes (ISO/IEC, 2022; NIST, 2020).

3.4.1 Preparación del entorno de virtualización

La preparación del entorno de virtualización comenzó con la instalación y configuración de VirtualBox, utilizado como plataforma para alojar las máquinas virtuales del laboratorio. Con esta herramienta se creó un entorno aislado, reproducible y separado de los sistemas productivos institucionales, adecuado para ejecutar pruebas controladas de ciberseguridad.

En esta fase se asignaron los recursos de cada máquina virtual, entre ellos memoria, almacenamiento, interfaces de red y adaptadores virtuales. También se configuraron los segmentos LAN, DMZ y red de ataque, administrados posteriormente mediante pfSense. Sobre esta base se implementaron los servicios, controles y herramientas de monitoreo del laboratorio.

El uso de entornos virtualizados favorece la ejecución de pruebas de seguridad en ambientes controlados, ya que reduce el riesgo de afectación sobre sistemas reales y facilita la repetición de escenarios técnicos (Scarfone et al., 2011).

3.4.2 Configuración de máquinas virtuales y servicios

Una vez preparado el entorno de virtualización, se configuraron las máquinas virtuales que conformaron el laboratorio de ciberseguridad. Cada máquina fue asignada a un segmento de red específico y cumplió una función determinada dentro del entorno de pruebas, permitiendo simular ataques controlados, monitorear eventos y aplicar reglas de seguridad.

Tabla 8.

Máquinas virtuales y servicios configurados en el laboratorio

Máquina virtual	Plataforma / servicio	Segmento de red	Función dentro del laboratorio
Firewall	pfSense	LAN, DMZ y red de ataque	Controló el tráfico entre los segmentos y permitió aplicar reglas de firewall durante las pruebas.
Equipo atacante	Kali Linux	Red de ataque	Se utilizó para ejecutar escaneos, intentos de acceso no autorizado y tráfico sospechoso dentro del laboratorio.
Servidor objetivo	Ubuntu Server + WordPress	DMZ	Representó el servicio evaluado; generó registros de acceso, tráfico web y eventos usados en los escenarios.
Sistema de monitoreo	Wazuh SIEM	LAN	Recibió y mostró eventos del servidor para revisar alertas, detección y respuesta ante las pruebas realizadas.

Nota. La tabla muestra la distribución de las máquinas virtuales utilizadas en el laboratorio y el papel que cumplió cada una durante las pruebas de escaneo, monitoreo, acceso no autorizado y respuesta ante eventos.

La configuración de las máquinas virtuales permitió trabajar el laboratorio como una red separada por funciones. El servidor ubicado en la DMZ quedó como equipo de prueba; Kali Linux se usó para generar los eventos; pfSense controló el paso del tráfico entre segmentos; y Wazuh reunió los registros que después fueron revisados.

Con esta distribución se pudieron ejecutar los escenarios definidos para el proyecto y comparar lo que ocurría en cada prueba. Además, los resultados obtenidos sirvieron para revisar controles relacionados con redes, accesos y monitoreo, tomando como referencia ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.4.3 Integración de herramientas de monitoreo y análisis

La integración de herramientas de monitoreo y análisis permitió centralizar los eventos generados durante las pruebas ejecutadas en el laboratorio virtual. Para ello, se utilizó Wazuh como sistema

SIEM, ubicado en la red LAN, con el propósito de recolectar, analizar y correlacionar registros provenientes del servidor objetivo, servicios de autenticación, tráfico web y eventos de red.

Durante esta fase se configuró el monitoreo de eventos relacionados con intentos fallidos de autenticación SSH, actividad web sospechosa, escaneo de puertos y registros generados por los componentes del laboratorio. Esta integración permitió disponer de alertas y evidencia técnica para evaluar la capacidad de detección del entorno, en concordancia con los controles A.8.15 Registro y A.8.16 Actividades de monitoreo de ISO/IEC 27001:2022, así como con la función Detect del NIST Cybersecurity Framework (ISO/IEC, 2022; NIST, 2020; Wazuh, s. f.).

3.5 Implementación de controles de seguridad

Los controles implementados respondieron a los riesgos priorizados en el diagnóstico: exposición de servicios, accesos no autorizados, ausencia de monitoreo y limitada capacidad de respuesta. Con base en estos peligros, el laboratorio implementó controles técnicos que pueden ser verificados a través de pruebas, tales como filtrado, segmentación, autenticación, monitoreo, respuesta ante eventos y registro.

En la práctica, los controles no se trabajaron como un solo bloque. Primero se separaron las redes y se revisó el tráfico con pfSense; luego se ajustaron los accesos y algunos servicios del servidor; finalmente, los eventos generados durante las pruebas se observaron en Wazuh. Con esto se pudo revisar seguridad de redes, autenticación, registros, monitoreo y respuesta ante incidentes simulados. La relación con ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5 se tomó como una guía para ordenar esas pruebas dentro del alcance del laboratorio, no como una implementación completa de ambos marcos (ISO/IEC, 2022; NIST, 2020).

3.5.1 Controles de segmentación y filtrado de tráfico

La segmentación y el filtrado de tráfico se implementaron mediante pfSense, separando el laboratorio en tres zonas principales: LAN, DMZ y red de ataque. Esta configuración permitió

controlar la comunicación entre segmentos, limitar accesos no autorizados y reducir el riesgo de movimiento lateral dentro del entorno virtual.

Las reglas de firewall permitieron definir qué tráfico podía circular entre las zonas del laboratorio, especialmente desde la red de ataque hacia el servidor ubicado en la DMZ. Este control se relaciona con A.8.20 Seguridad de redes y A.8.22 Segregación de redes de ISO/IEC 27001:2022, así como con el control SC-7 Boundary Protection de NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.5.2 Controles de acceso y autenticación

Los controles de acceso y autenticación se aplicaron principalmente en el servidor Ubuntu y en los servicios evaluados dentro del laboratorio. Se consideró el uso de credenciales locales, restricciones de acceso remoto mediante SSH y protección básica del entorno WordPress, con el propósito de reducir intentos de acceso no autorizado.

Estos controles permitieron generar y monitorear eventos relacionados con autenticaciones fallidas, usuarios inexistentes e intentos de fuerza bruta, los cuales fueron analizados posteriormente mediante Wazuh. Esta implementación se alinea con A.5.15 Control de acceso, A.5.16 Gestión de identidad y A.5.17 Información de autenticación de ISO/IEC 27001:2022, además de los controles AC-2 Gestión de cuentas y AC-6 Mínimo privilegio de NIST SP 800-53 Rev. 5 (ISO/IEC, 2022; NIST, 2020).

3.5.3 Controles de monitoreo y detección de eventos

Los controles de monitoreo y detección se implementaron mediante Wazuh, ubicado en la red LAN, con el propósito de centralizar y analizar los eventos generados por el servidor Ubuntu, los servicios web, SSH y los registros asociados al tráfico del laboratorio.

Esta configuración permitió identificar eventos relacionados con intentos fallidos de autenticación, escaneo de puertos, tráfico web sospechoso y actividad anómala dentro del entorno virtual. Estos controles se alinean con A.8.15 Registro y A.8.16 Actividades de monitoreo de ISO/IEC

27001:2022, así como con la función Detect del NIST CSF (ISO/IEC, 2022; NIST, 2020; Wazuh, s. f.).

3.5.4 Controles de respuesta y mitigación de incidentes

Los controles de respuesta y mitigación se ejecutaron a partir de los eventos detectados durante las pruebas controladas. Cuando Wazuh identificó actividad sospechosa, se analizó la alerta y se configuraron reglas de bloqueo en pfSense como acción de contención.

Con estas acciones se comprobó la capacidad del laboratorio para responder ante incidentes simulados y limitar el acceso no autorizado desde la red de ataque hacia el servidor ubicado en la DMZ. Este control se asoció con A.5.24 Planificación y preparación para la gestión de incidentes y A.5.26 Respuesta a incidentes de seguridad de la información de ISO/IEC 27001:2022, así como con la función Respond del NIST CSF (ISO/IEC, 2022; NIST, 2020).

La puesta en marcha del laboratorio virtual generó un ambiente controlado, dividido y supervisado para realizar evaluaciones de ciberseguridad. La combinación de pfSense, Kali Linux y Ubuntu Server con WordPress y Wazuh permitió simular situaciones de ataque, registrar sucesos de seguridad e implementar controles técnicos vinculados a la autenticación, monitoreo, segmentación y respuesta ante incidentes.
Con esta configuración, el laboratorio quedó listo para la fase de evaluación, donde se analizan los resultados obtenidos mediante el enfoque pretest–postest. Los controles aplicados y la evidencia generada en el entorno virtual permiten valorar la efectividad del laboratorio dentro del proceso de mejora de la seguridad digital del ISU Sucre, aspecto que se desarrolla en el Capítulo 4.

3.5.5 Proyección institucional del laboratorio virtual

El laboratorio virtual que se creó estableció las bases técnicas necesarias para que el ISU Sucre pueda ir mejorando su ciberseguridad de manera gradual. Con este entorno, lo que se puede hacer es reproducir amenazas, validar controles y también generar evidencias sin que por ello se dañen los sistemas productivos. En cuanto al funcionamiento, allí entran el monitoreo de tráfico con

pfSense, la segmentación de red, el endurecimiento de los servicios y, por supuesto, la supervisión con Wazuh.

El alcance del laboratorio debe leerse según las condiciones en las que fue desarrollado. Se trabajó en un entorno virtual dentro de VirtualBox, útil para probar segmentación, monitoreo y respuesta, pero distinto a una red institucional en operación. Por esa razón, no se incluyeron situaciones como tráfico masivo, muchos usuarios conectados al mismo tiempo, integración con todos los sistemas del ISU Sucre o ataques avanzados. Los controles aplicados fueron principalmente técnicos y, para usarlos a nivel institucional, tendrían que acompañarse con políticas, procedimientos, capacitación y gestión de riesgos.

A futuro, el laboratorio puede mantenerse como un espacio de prueba y capacitación. Antes de aplicar cambios en sistemas reales, permitiría revisar configuraciones, repetir escenarios y documentar resultados. Para que tenga mayor utilidad institucional, debería complementarse con monitoreo centralizado, revisión periódica de vulnerabilidades, segmentación de red y una relación progresiva con un Sistema de Gestión de Seguridad de la Información.

CAPÍTULO 4. EVALUACIÓN Y RESULTADOS

En este capítulo se presentan los resultados obtenidos después de implementar el laboratorio virtual de ciberseguridad diseñado para el ISU Sucre. La evaluación parte de una comparación entre la situación inicial y el estado posterior a la aplicación de controles técnicos, teniendo como referencia las pruebas ejecutadas en el entorno controlado. Para esto, se consideran los hallazgos del pretest, las evidencias generadas durante los escenarios de prueba y los datos del postest asociados a vulnerabilidades, detección de eventos y tiempos de respuesta. Esta revisión deja ver, de forma práctica, qué cambios produjo la segmentación de red, el monitoreo con Wazuh, el control de tráfico mediante pfSense y el endurecimiento básico de servicios. Por otro lado, los resultados se interpretan en relación con los controles seleccionados de ISO/IEC 27001 y con las funciones del marco NIST, sin olvidar que la validación se realizó dentro de un laboratorio y no directamente sobre los sistemas productivos de la institución.

4.1 Modelo de evaluación del laboratorio

El modelo de evaluación se basa en un enfoque cuantitativo pretest–postest, orientado a medir la efectividad del laboratorio virtual mediante indicadores de seguridad y métricas alineadas a estándares internacionales.

4.1.1 Enfoque de evaluación (pretest – postest)

Se aplicó un enfoque de evaluación pretest–postest para medir el impacto de la implementación del laboratorio virtual de ciberseguridad. Este método permitió comparar el estado inicial del entorno con los resultados obtenidos tras la aplicación de controles de seguridad.
A continuación, se presentan los resultados consolidados de los principales indicadores evaluados:

Tabla 9.

Evaluación comparativa de indicadores de ciberseguridad

Indicador	Métrica (definición)	Pretest	Postest	Variación
Vulnerabilidades totales	Número total de vulnerabilidades detectadas	26	11	↓ 57,69%
Vulnerabilidades críticas	Vulnerabilidades de alto riesgo	15	5	↓ 66,67%
Tasa de detección	% de ataques simulados detectados	25%	100%	↑ 75 puntos porcentuales
Tiempo de detección (MTTD)	Tiempo promedio para identificar incidentes	9 min	5 seg.	↓ 99,07%
Tiempo de respuesta (MTTR)	Tiempo promedio para responder a incidentes	20 min	3 min 18s.	↓ 83,50%

Nota. Comparación entre el estado inicial (pretest) y posterior (postest) del entorno, evidenciando mejoras tras la implementación de controles de seguridad. El 25% corresponde a detección manual de logs y reporte del personal TIC (Anexo 4), no a monitoreo automatizado

El enfoque pretest–postest permitió comparar las condiciones iniciales del entorno con los resultados obtenidos después de aplicar controles técnicos, monitoreo y pruebas controladas. A partir de esta comparación, se identificaron mejoras en la reducción de vulnerabilidades, en la capacidad de detección y en los tiempos de respuesta. Estos elementos aportan evidencia medible para valorar la efectividad del laboratorio dentro del contexto institucional.

4.1.2 Indicadores de seguridad evaluados

Los indicadores seleccionados permiten evaluar la efectividad del laboratorio en tres dimensiones clave:

- Gestión de vulnerabilidades: mide la exposición del sistema a amenazas.
- Capacidad de detección: evalúa la eficiencia del monitoreo de eventos.
- Capacidad de respuesta: mide la rapidez de reacción ante incidentes.

Estos indicadores están directamente relacionados con la mejora de la postura de seguridad del entorno evaluado.

4.1.3 Métricas utilizadas (vulnerabilidades, detección, respuesta)

Las métricas utilizadas corresponden a estándares internacionales de medición en ciberseguridad, permitiendo cuantificar el desempeño del sistema antes y después de la implementación del laboratorio.

Las principales métricas aplicadas fueron:

- Conteo de vulnerabilidades: clasificación por criticidad
- Tasa de detección: porcentaje de eventos identificados
- MTTD (Mean Time to Detect): tiempo medio de detección
- MTTR (Mean Time to Respond): tiempo medio de respuesta

Para la clasificación de vulnerabilidades por criticidad, se consideró la lógica de valoración de severidad empleada en marcos como CVSS, que permite asignar niveles de riesgo según características técnicas de la vulnerabilidad, impacto y condiciones de explotación (FIRST, 2023).

4.1.4 Criterios de evaluación (ISO/NIST)

Los resultados se interpretan con base en controles de seguridad reconocidos.

Tabla 10.

Relación indicadores – estándares

Indicador	ISO/IEC 27001:2022	NIST CSF	Interpretación en el proyecto
Vulnerabilidades	A.8.8 Gestión de vulnerabilidades técnicas	Identify / Protect	El escaneo del servidor en la DMZ mostró puertos, servicios y configuraciones que necesitaban ajuste.
Detección de eventos	A.8.15 Registro / A.8.16 Actividades de monitoreo	Detect	Wazuh mostró alertas por intentos SSH fallidos, escaneos con Nmap y peticiones web de prueba.

Respuesta a incidentes	A.5.24 Planificación y preparación para la gestión de incidentes / A.5.26 Respuesta a incidentes de seguridad de la información	Respond	Después de revisar la alerta en Wazuh, se bloqueó el tráfico desde pfSense.
Control de accesos	A.5.15 Control de acceso / A.5.16 Gestión de identidad / A.5.17 Información de autenticación	Protect	Los intentos fallidos de autenticación ayudaron a revisar cómo respondía el servidor ante accesos no autorizados.
Segmentación de red	A.8.20 Seguridad de redes / A.8.22 Segregación de redes	Protect	La separación entre LAN, DMZ y red de ataque permitió controlar mejor el paso de tráfico entre zonas.

Nota. La tabla relaciona los indicadores evaluados en el laboratorio virtual con controles de ISO/IEC 27001:2022 y funciones del NIST Cybersecurity Framework, considerando su aplicación en los escenarios de prueba del proyecto.

Para interpretar los resultados, se emplean las funciones del NIST CSF como marco operativo. A su vez, NIST SP 800-53 se toma como referencia para relacionar los controles técnicos aplicables al laboratorio.

4.2 Línea base de seguridad (Resultados Pretest)

La línea base de seguridad corresponde al estado inicial del entorno tecnológico del ISU Sucre antes de la implementación del laboratorio virtual de ciberseguridad. Esta medición se realizó mediante la aplicación de instrumentos de recolección de datos (encuestas, listas de verificación y pruebas técnicas controladas), cuyos resultados se sintetizan a continuación.

Los indicadores detallados y sus evidencias gráficas se encuentran documentados en los anexos del presente proyecto.

4.2.1 Nivel inicial de vulnerabilidades

El análisis pretest permitió identificar un nivel significativo de vulnerabilidades en el entorno institucional, principalmente asociadas a configuraciones inseguras, falta de segmentación de red y ausencia de monitoreo continuo.

Tabla 11.

Nivel inicial de vulnerabilidades detectadas

Tipo de vulnerabilidad	Cantidad	Nivel de severidad predominante
Configuraciones inseguras	12	Alta
Puertos abiertos innecesarios	5	Media
Falta de segmentación de red	3	Alta
Software desactualizado	6	Media

Nota. Los datos fueron obtenidos mediante pruebas controladas en entorno simulado utilizando la herramienta Nmap v7.98.

En términos generales, el entorno presenta debilidades estructurales que aumentan la superficie de ataque, principalmente por la exposición de servicios y la falta de controles preventivos.

4.2.2 Estado de controles de seguridad

La evaluación de los controles tomó como referencia buenas prácticas relacionadas con ISO/IEC 27001 y con el marco NIST SP 800-53.

Tabla 12.

Estado inicial de controles de seguridad

Control evaluado	Estado	Observación
Control de accesos	Parcial	Aplicación limitada de políticas de acceso.
Gestión de contraseñas	Deficiente	Presencia de credenciales débiles.
Monitoreo de eventos	Inexistente	No se cuenta con un SIEM implementado.
Segmentación de red	Deficiente	Red plana, sin aislamiento entre segmentos.

Actualización de sistemas	Parcial	Procesos de actualización no estandarizados.

Nota. La evaluación utilizó listas de verificación elaboradas a partir de controles de seguridad recomendados en estándares internacionales.

A partir de la evaluación inicial, se observa que los controles de seguridad aún presentan un desarrollo limitado. Esta condición reduce la capacidad del ISU Sucre para prevenir incidentes y responder oportunamente ante eventos de seguridad.

4.2.3 Capacidad inicial de detección de eventos

Durante la fase pretest, la detección de eventos de seguridad mostró limitaciones asociadas a la falta de herramientas especializadas y de procedimientos definidos.

Tabla 13.

Capacidad de detección de eventos (Pretest)

Indicador	Resultado
Detección de accesos no autorizados	Baja
Generación de alertas	Nula
Registro de eventos (logs)	Parcial
Correlación de eventos	Nula

Nota. Los resultados provienen de la simulación de eventos de seguridad y de la observación del comportamiento del sistema.

La falta de un sistema de monitoreo centralizado limita la identificación temprana de incidentes. Esta condición puede prolongar la exposición del entorno ante eventos no detectados.

4.2.4 Análisis de riesgos inicial

Para conocer los puntos débiles del entorno antes de implementar el laboratorio, se hizo una revisión de los riesgos asociados a los activos y servicios que luego se representaron en el entorno virtual. Se usaron dos criterios para valorar cada riesgo: la probabilidad de que ocurra y el impacto que podría tener sobre la operación, la información o el acceso a los servicios del ISU Sucre. Con base en estos criterios se elaboró la matriz de riesgos que se muestra en la Tabla 14.

Tabla 14.

Matriz de riesgos inicial

Riesgo identificado	Probabilidad	Impacto	Nivel de riesgo
Acceso no autorizado	Alta	Alto	Crítico
Exposición de servicios	Alta	Medio	Alto
Pérdida de información	Media	Alto	Alto
Ataques de red interna	Media	Medio	Medio
Falta de monitoreo	Alta	Alto	Crítico

Nota. La tabla muestra la valoración del riesgo se realizó bajo criterios cualitativos (Alto, Medio, Bajo), tomando en cuenta el contexto institucional junto con los activos críticos.

Los resultados de la matriz muestran dos riesgos críticos: los accesos no autorizados y la falta de monitoreo. En ambos casos, la probabilidad y el impacto se valoraron como altos. Eso indica que, antes del laboratorio, la institución tenía problemas para detectar eventos sospechosos a tiempo y para gestionar los accesos de manera controlada. También aparecieron dos riesgos de nivel alto: exposición de servicios y posible pérdida de información. Estos hallazgos terminan de confirmar la necesidad de un espacio separado para poder probar controles, revisar configuraciones y generar evidencia sin afectar los sistemas reales.

4.3 Escenarios de pruebas de ciberseguridad

Este apartado describe los escenarios que se diseñaron para evaluar la efectividad del laboratorio virtual de ciberseguridad a través de la simulación de amenazas controladas. Con los escenarios se puede validar el comportamiento de los controles implementados, y también medir la capacidad de detección junto con la respuesta ante incidentes, todo en coherencia con el enfoque de evaluación pretest-postest.

Todas las pruebas se llevaron a cabo dentro de un entorno controlado, lo cual garantizó que no se viera afectada la infraestructura institucional real. De ese modo se pudo recolectar evidencia de carácter objetivo que luego sirviera para el análisis de los resultados.

4.3.1 Definición de escenarios de ataque

Los escenarios de ataque se definieron a partir de los hallazgos de la evaluación inicial y de las pruebas que podían ejecutarse dentro del laboratorio virtual. Se priorizaron servicios expuestos, accesos no autorizados, tráfico sospechoso y monitoreo de eventos. Cada escenario se organizó con un objetivo, un tipo de amenaza y un indicador de evaluación, como se muestra en la siguiente tabla.

Tabla 15.

Escenarios de ataque, detección y monitoreo de amenazas

Escenario	Descripción	Objetivo	Tipo de amenaza	Indicador evaluado
Escaneo de vulnerabilidades Revisar Anexo 7.	Simulación de reconocimiento activo sobre la red del laboratorio.	Identificar puertos abiertos, servicios expuestos y posibles vulnerabilidades.	Reconocimiento (fase inicial de ataque).	Nivel de exposición y cantidad de vulnerabilidades identificadas
Intento de acceso no autorizado Revisar Anexo 8.	Ejecución de intentos controlados de autenticación fallida.	Evaluar mecanismos de control de acceso y autenticación.	Ataque de fuerza bruta básico.	Capacidad de control frente a intentos de autenticación no autorizados.
Generación de tráfico sospechoso Revisar Anexo 9.	Simulación de actividad anómala dentro de la red.	Validar la capacidad de monitoreo y detección de eventos.	Actividad maliciosa simulada.	Tiempo de detección de eventos sospechosos.
Monitoreo y respuesta a eventos. Revisar Anexo 10.	Evaluación del sistema de monitoreo frente a eventos generados	Verificar generación de alertas y registros.	Evento de seguridad controlado.	Tiempo de respuesta y trazabilidad del evento detectado.

Nota. La tabla presenta los escenarios de ataque, detección y monitoreo definidos para evaluar el comportamiento del laboratorio virtual frente a amenazas controladas.

4.3.2 Configuración de pruebas en el laboratorio

Las pruebas se ejecutaron sobre la infraestructura virtual previamente implementada, la cual simula un entorno institucional básico compuesto por:

- Máquina atacante (entorno de pruebas ofensivas)
- Servidor monitorizado
- Sistema de monitoreo y correlación de eventos
- Red virtual segmentada

La configuración permitió:

- Aislamiento del entorno de pruebas
- Control total sobre los eventos generados
- Repetibilidad de los escenarios

Cada escenario fue ejecutado en dos fases:
Pretest: Sin optimización de controles (línea base)
Postest: Con controles implementados y configurados

Esta planificación permitió mantener trazabilidad entre los objetivos de prueba, los activos evaluados, los eventos generados y los controles validados, en concordancia con las buenas prácticas de evaluación técnica de seguridad de la información (Scarfone et al., 2008).

4.3.3 Herramientas utilizadas

Las herramientas se eligieron según las necesidades de cada escenario y las condiciones del laboratorio virtual. Se buscó que fueran compatibles con el entorno, que permitieran generar evidencia verificable y que se pudieran usar sin tocar los sistemas reales de la institución. En la siguiente tabla se muestran las herramientas usadas y qué función cumplió cada una en las pruebas.

Tabla 16.

Descripción de las herramientas utilizadas en el laboratorio

Herramienta	Uso aplicado en el laboratorio
Kali Linux	Desde esta máquina se generaron escaneos, intentos de acceso y tráfico de prueba hacia el servidor ubicado en la DMZ.
Nmap	Se aplicó sobre el servidor Ubuntu con WordPress para revisar puertos abiertos y servicios visibles.
Wazuh	Se revisó durante las pruebas para comprobar la llegada de eventos y alertas relacionadas con SSH, Nmap y peticiones web.
Metasploit básico	Se mantuvo como apoyo puntual para pruebas ofensivas básicas, solo dentro del entorno virtual.

Nota. Las herramientas se usaron solo en los escenarios definidos para el laboratorio virtual. Su aplicación permitió generar eventos, revisar servicios visibles y comprobar alertas sin intervenir sistemas reales del ISU Sucre.

4.3.4 Relación de pruebas con controles ISO/IEC 27001 y NIST

Con los escenarios de prueba se buscó validar controles de seguridad concretos y ver cómo se relacionan con buenas prácticas internacionales. Así se puede observar, desde lo técnico, de qué manera el laboratorio usa parcialmente los controles que vienen de ISO/IEC 27001 y del NIST.

Tabla 17.

Relación entre escenarios y estándares de seguridad

Escenario	Control ISO/IEC 27001:2022	Función NIST CSF	Descripción
Escaneo de vulnerabilidades	A.8.8 Gestión de vulnerabilidades técnicas	Identify	Identificación de puertos, servicios expuestos y debilidades técnicas del entorno.
Intento de acceso no autorizado	A.5.15 Control de acceso, A.5.16 Gestión de identidad, A.5.17 Información de autenticación	Protect	Evaluación de accesos indebidos mediante intentos fallidos de autenticación.

Generación de tráfico sospechoso	A.8.15 Registro, A.8.16 Actividades de monitoreo	Detect	Detección de eventos anómalos generados por SSH, Nmap y peticiones web sospechosas.
Monitoreo y respuesta a eventos	A.5.24 Planificación y preparación para la gestión de incidentes, A.5.26 Respuesta a incidentes de seguridad de la información	Respond	Validación de alertas en Wazuh y aplicación de respuesta mediante pfSense.
Segmentación y control de tráfico	A.8.20 Seguridad de redes, A.8.22 Segregación de redes	Protect	Separación de zonas LAN, DMZ y red de ataque para limitar accesos no autorizados.

Nota. La correspondencia se establece con base en la estructura vigente de ISO/IEC 27001:2022 y las funciones del NIST CSF, considerando la aplicabilidad del laboratorio como entorno académico de simulación y validación de controles.

Los resultados de cada escenario se relacionan con los indicadores establecidos en la fase metodológica. Los instrumentos utilizados para su registro se incluyen en los anexos correspondientes.

Para revisar cada escenario no se tomó un solo resultado, sino varios datos del comportamiento del laboratorio. Se observó si el entorno quedaba expuesto a vulnerabilidades, si Wazuh lograba mostrar los eventos generados, cuánto tiempo tomaba reaccionar ante una alerta y si los controles aplicados ayudaban a reducir el riesgo durante las pruebas.

En los anexos también se incluyen las evidencias visuales de los resultados, entre las cuales se cuentan capturas de pantalla, registros del sistema y dashboards. Todo ese material sirve de respaldo para el proceso de evaluación y, además, contribuye a que las pruebas queden debidamente documentadas y de tal forma que se puedan seguir paso a paso.

4.4 Ejecución de pruebas y validación de controles

En este apartado se presentan los resultados de la ejecución de los escenarios definidos en el ítem 4.3, con el propósito de evaluar el comportamiento del laboratorio virtual frente a amenazas simuladas y validar la efectividad de los controles de seguridad implementados.
La evidencia detallada de cada prueba (capturas, registros y resultados) se encuentra documentada en los anexos correspondientes.

4.4.1 Ejecución del escenario 1: Escaneo de vulnerabilidades

La prueba inició con la revisión del servidor Ubuntu con WordPress que estaba en la DMZ. Desde la red de pruebas se usó Nmap para ver qué servicios contestaban dentro del laboratorio y qué puertos estaban abiertos. Esto permitió saber el nivel de exposición del servidor, sobre todo en los servicios publicados y en la información que se podía encontrar durante el reconocimiento.
Para el servicio web, la revisión no se limitó a identificar puertos activos. También se observaron aspectos relacionados con la configuración del servidor, la exposición de la aplicación WordPress, los mecanismos de autenticación y el control de acceso. Estos criterios se relacionan con las pruebas de seguridad web consideradas por OWASP para la evaluación de aplicaciones expuestas (OWASP Foundation, 2025).

Se detectaron servicios activos y situaciones que necesitaban ser ajustadas en el laboratorio a partir del escaneo. Además, se detectó información que podría simplificar la contabilización de los usuarios en la aplicación web. La evaluación brindó información para el manejo de vulnerabilidades técnicas, en relación con la función Identify del NIST CSF y con el control A.8.8 de ISO/IEC 27001:2022, ya que posibilitó identificar activos expuestos, debilidades presentes en el ambiente analizado y servicios visibles.

4.4.2 Ejecución del escenario 2: Intento de acceso no autorizado

Lo que se realizó en este escenario fue simular un acceso no autorizado con un ataque de fuerza bruta usando Hydra apuntando al servidor objetivo del laboratorio. Mientras se hacía la prueba,

aparecieron varios intentos fallidos de autenticación que Wazuh tomó como actividad sospechosa por accesos indebidos.

También se vio que se dispararon mecanismos de protección por los intentos fallidos, y eso ayudó a restringir el acceso no autorizado al sistema.

Con esta prueba se confirmó que los controles de autenticación y de gestión de accesos sí funcionaban. Esos controles son A.5.15 Control de acceso, A.5.16 Gestión de identidad y A.5.17 Información de autenticación (ISO/IEC 27001:2022). Además, este escenario se relaciona con la función Protect del NIST CSF, que protege credenciales, usuarios y los mecanismos para acceder a los sistemas.

4.4.3 Ejecución del escenario 3: Generación de tráfico sospechoso

En esta prueba se generó actividad poco común desde la red de ataque hacia el servidor que estaba en la DMZ. Para ello se hicieron varios intentos fallidos de autenticación por SSH, una revisión de puertos y peticiones al servicio web. No se buscó afectar el servidor, sino dejar registros suficientes para ver si el sistema de monitoreo podía reconocer este tipo de comportamiento dentro del laboratorio.

Al revisar el panel de Wazuh, se observaron alertas relacionadas con los accesos rechazados y con la actividad generada desde la red de ataque. Estos registros permitieron contrastar lo realizado durante la prueba con la información recibida por el sistema de monitoreo. Con ello se evidenció que el laboratorio podía mostrar señales útiles para seguir comportamientos sospechosos dentro del entorno virtual.

Con este escenario se apoya la aplicación de controles de registro y monitoreo de eventos, por ejemplo A.8.15 Registro y A.8.16 Actividades de monitoreo de ISO/IEC 27001:2022. También se conecta con la función Detect del NIST CSF, la cual se enfoca en identificar a tiempo eventos anómalos y posibles incidentes de seguridad.

4.4.4 Ejecución del escenario 4: Monitoreo y respuesta a eventos

Con este escenario se evaluó la detección, el análisis y la respuesta del laboratorio ante eventos de seguridad que se generaron de manera controlada.

En esta parte no se trabajó con un ataque real al sistema institucional, sino con intentos SSH fallidos generados dentro del laboratorio. El evento quedó registrado en el servidor y, pocos segundos después, apareció en Wazuh. Desde esa alerta se tomó la IP de Kali Linux y se bloqueó el tráfico en pfSense. Luego se comparó la hora del intento con la hora de la alerta para calcular cuánto tardó el monitoreo en detectarlo.

Este panorama respalda la administración de incidentes y eventos de seguridad en el laboratorio. Se establece su relación con los controles A.5.24, que se refiere a la planificación y preparación para el manejo de incidentes, y A.5.26. Respuesta a incidentes relacionados con la seguridad de la información según la norma ISO/IEC 27001:2022. Además, se relaciona con las funciones Detect y Respond del NIST CSF ya que incluye la detección de eventos, el análisis de alertas y la contención.

4.4.5 Validación de controles de seguridad implementados

En los cuatro escenarios se revisó qué ocurría antes y después de aplicar los controles. El escaneo mostró servicios visibles y configuraciones que necesitaban ajuste. En las pruebas de acceso, los intentos fallidos quedaron registrados y pudieron verse en Wazuh. Luego, con el tráfico sospechoso, se verificó si el monitoreo mostraba señales útiles durante la ejecución.

Con la respuesta aplicada desde pfSense se cerró el ciclo de prueba, porque el tráfico de la máquina atacante pudo ser bloqueado. Así, la segmentación, el endurecimiento básico, el monitoreo y las reglas de firewall no quedaron solo como configuraciones, sino como controles observados dentro del laboratorio virtual.

Lo que muestran estos resultados es una mejora en la postura de seguridad del entorno, específicamente en lo que tiene que ver con la detección y con la respuesta ante amenazas. Y esto se da en coherencia con los indicadores que fueron definidos en el modelo de evaluación.

Si se mira el conjunto, el laboratorio virtual resulta estar a la altura de los principios de seguridad que establecen la ISO/IEC 27001 y el marco NIST, sobre todo en las funciones de identificar, proteger, detectar y responder. De esta manera se valida el aporte que este laboratorio hace al fortalecimiento de la ciberseguridad institucional.

4.5 Resultados del postest y mejora del sistema

La evaluación posterior o postest permitió valorar los cambios generados después de implementar el laboratorio virtual en el entorno evaluado. Para ello, se revisaron los indicadores definidos, la comparación con la línea base del pretest y las evidencias obtenidas en los escenarios ejecutados.

4.5.1 Reducción de vulnerabilidades detectadas

En el postest se observó una reducción en la cantidad y criticidad de las vulnerabilidades. Este cambio muestra una mejora en la seguridad del entorno luego de implementar el laboratorio virtual.

Tabla 18.

Reducción de vulnerabilidades detectadas

Tipo de vulnerabilidad	Pretest	Postest	Variación	Observación
Configuraciones inseguras	12	5	↓ 58,33%	Reducción por endurecimiento de SSH, Apache y WordPress
Puertos abiertos innecesarios	5	2	↓ 60,00%	Control mediante reglas de pfSense
Falta de segmentación de red	3	1	↓ 66,67%	Implementación de LAN, DMZ y red de ataque
Software desactualizado	6	3	↓ 50,00%	Actualización parcial de componentes
Total	**26**	**11**	**↓ 57,69%**	Mejora global del entorno

Nota. La mejora observada se debe a la implementación de controles técnicos como segmentación de red, reglas de firewall y fortalecimiento de accesos en el entorno virtual.

La reducción de vulnerabilidades no salió solo del conteo final, sino de revisar qué servicios estaban expuestos y qué ajustes se aplicaron en el laboratorio. Por eso, el resultado se vincula con A.8.8 de ISO/IEC 27001:2022, relacionado con la gestión de vulnerabilidades técnicas. También guarda relación con Identify del NIST CSF, porque el trabajo permitió reconocer riesgos y orientar medidas de mitigación.

4.5.2 Mejora en la capacidad de detección

Al incorporar el sistema de monitoreo, se logró que la detección de eventos de seguridad mejorara en el entorno evaluado.

Tabla 19.

Mejora en la capacidad de detección de eventos

Indicador evaluado	Pretest (Situación inicial)	Postest (Situación mejorada)	Mejora evidenciada
Detección de accesos no autorizados	Baja o inexistente	Detección automática mediante Wazuh	Incremento en visibilidad
Generación de alertas	No disponible	Alertas en tiempo real	Respuesta proactiva
Registro de eventos (logs)	Limitado	Registro centralizado	Mayor trazabilidad
Correlación de eventos	No implementada	Correlación mediante SIEM	Identificación de patrones
Detección de tráfico sospechoso	No identificable	Eventos detectados (SSH, Nmap, curl)	Mejora en análisis de amenazas

Nota. Al integrar Wazuh como SIEM se logró monitoreo continuo, detección de eventos y alertas en tiempo real dentro del laboratorio.

El resultado se vinculó con A.8.15 Registro y A.8.16 Actividades de monitoreo de ISO/IEC 27001:2022, porque Wazuh permitió recopilar y revisar los eventos generados en las pruebas.

También se relacionó con la función Detect del NIST CSF, al mostrar alertas sobre actividad sospechosa dentro del laboratorio virtual.

4.5.3 Mejora en tiempos de respuesta (MTTD / MTTR)

Una vez que se puso en marcha el laboratorio virtual, se observó que los tiempos de detección y también los de respuesta ante incidentes de seguridad resultaron más bajos si se comparaban con la línea base que se había establecido al inicio.

Tabla 20.

Mejora en tiempos de detección y respuesta

Métrica	Pretest (Situación inicial)	Postest (Situación mejorada)	Mejora evidenciada
MTTD (Tiempo de detección)	Alto (minutos)	Bajo (segundos/minutos)	Detección más rápida
MTTR (Tiempo de respuesta)	Alto	Reducido	Respuesta más eficiente
Identificación de incidentes	Manual o tardía	Automática (SIEM)	Mayor eficiencia operativa
Aplicación de respuesta	No definida	Implementación de reglas (pfSense)	Mitigación efectiva
Tiempo de reacción	Lento	Oportuno	Reducción del impacto

Nota. La reducción del tiempo de detección se vio en los escenarios que se ejecutaron, además de respuestas de contención como el bloqueo de tráfico.

La prueba se interpreta desde la gestión de incidentes trabajada dentro del laboratorio. La alerta observada en Wazuh y el bloqueo aplicado en pfSense muestran una respuesta básica frente al evento simulado. Por ello, el escenario se asocia con los controles A.5.24 Planificación y preparación para la gestión de incidentes y A.5.26 Respuesta a incidentes de seguridad de la información de ISO/IEC 27001:2022. Además, se conecta con las funciones Detect y Respond del

NIST CSF, porque incluye la detección del evento, la revisión de la alerta y la contención del tráfico desde la red de ataque.

4.5.4 Comparación de indicadores pretest vs postest

El análisis comparativo permite evidenciar de forma cuantitativa la mejora del sistema tras la implementación del laboratorio virtual.

Tabla 21.

Comparación de indicadores de seguridad

Indicador	Pretest	Postest	Resultado
Vulnerabilidades totales	Alto	Reducido	Disminución de vulnerabilidades identificadas
Vulnerabilidades críticas	Elevadas	Disminuidas	Reducción de exposición crítica
Tasa de detección	Baja	Alta	Aumento de eventos detectados
MTTD	Alto	Reducido	Menor tiempo de detección
MTTR	Alto	Reducido	Menor tiempo de respuesta
Capacidad de monitoreo	Limitada	Implementada (SIEM)	Monitoreo centralizado mediante SIEM
Gestión de incidentes	No estructurada	Definida	Respuesta organizada ante eventos

Nota. La comparación resume los cambios observados en la postura de seguridad del entorno, a partir de los indicadores técnicos definidos en el modelo de evaluación.

En el postest se observó un cambio más concreto en el laboratorio: las vulnerabilidades disminuyeron, los eventos generados durante las pruebas pudieron verse en Wazuh y la respuesta se apoyó en reglas aplicadas desde pfSense. Esto muestra que el entorno pasó de una revisión limitada a un proceso con mayor control sobre lo que ocurría durante los escenarios simulados. La relación con ISO/IEC 27001 y NIST se mantiene, pero se entiende dentro del alcance del proyecto, como una validación técnica parcial y no como una implementación completa de ambos marcos.

4.6 Análisis e interpretación de resultados

Después de presentar los datos del pretest, el postest y la comparación de indicadores, corresponde organizar el análisis general de los resultados obtenidos en el laboratorio virtual. Esta sección reúne los aspectos que ayudan a comprender el alcance de las pruebas realizadas, los cambios observados después de aplicar controles técnicos y los elementos que influyeron en esos resultados.

Esta parte cierra la lectura de los resultados del laboratorio. No se busca repetir las tablas, sino explicar qué dejó la comparación entre el pretest y el postest. A partir de los cambios observados, se comenta la reducción de vulnerabilidades, el uso de Wazuh para revisar alertas, la respuesta aplicada con pfSense y los límites de trabajar en un entorno virtual. También se ubican estos hallazgos frente a ISO/IEC 27001 y NIST, sin presentar el laboratorio como una aplicación completa de esos marcos.

4.6.1 Lectura de los resultados obtenidos

Al comparar los datos del pretest y del postest, el cambio más visible está en la reducción de vulnerabilidades y en cómo el laboratorio empezó a registrar los eventos de seguridad. Al inicio se observaron configuraciones inseguras, servicios expuestos y monitoreo limitado. Después de aplicar segmentación, reglas de firewall y endurecimiento básico, las vulnerabilidades totales bajaron de 26 a 11. Esto señala que las actividades realizadas en el laboratorio contribuyeron a reducir múltiples puntos de exposición del servidor sometido a evaluación.

La detección y la respuesta también han mejorado. Antes del laboratorio, se basaba más en observaciones limitadas del ambiente o en registros manuales la revisión de los eventos. Wazuh mostró alertas de tráfico sospechoso, escaneos y accesos fallidos en el postest; por su parte, pfSense se empleó para implementar acciones de bloqueo. Por eso, los datos no solo muestran una mejora en los números, sino también una forma más ordenada de observar, registrar y atender incidentes simulados dentro del entorno virtual.

4.6.2 Factores que explican las mejoras obtenidas

Las mejoras del postest se relacionan con varios ajustes aplicados antes de repetir las pruebas. La separación entre LAN, DMZ y red de ataque ayudó a que el tráfico del laboratorio no circulara de forma abierta entre todos los equipos. Con pfSense se revisó qué comunicación pasaba entre segmentos y, cuando apareció actividad no autorizada, se bloqueó el tráfico proveniente de la red de ataque.

Otro elemento importante fue Wazuh, porque permitió revisar en un solo panel los registros generados durante las pruebas. Allí aparecieron intentos fallidos de autenticación, escaneos de puertos y peticiones web sospechosas. Además, el endurecimiento básico de SSH, Apache y WordPress redujo parte de las configuraciones débiles encontradas al inicio. Por eso, la mejora no depende de una sola herramienta, sino del trabajo conjunto entre segmentación, monitoreo, ajustes de servicios y respuesta con pfSense.

4.6.3 Impacto en el contexto institucional

En el caso del ISU Sucre, el laboratorio aporta porque permite ensayar controles antes de moverlos a servicios reales. Se emplearon circunstancias que ya se habían considerado necesarias en el diagnóstico a lo largo de las evaluaciones: intentos de ingreso, servicios expuestos, falta de supervisión centralizada y respuesta ante incidentes. Fue factible examinar configuraciones, ver alertas en Wazuh y ejecutar bloqueos en pfSense sin arriesgar las plataformas administrativas o académicas al reproducir esos casos en un entorno aparte.

Este resultado, por otro lado, también constituye una base importante para la labor que realiza el sector técnico. El laboratorio puede resultar útil si se quiere realizar pruebas en repetidas ocasiones, cotejar variaciones que aparezcan después de modificaciones en la seguridad y también registrar evidencias para cuando sea necesario justificar nuevas medidas.

En lo que toca al ámbito académico, el entorno bien puede aprovecharse para hacer prácticas dirigidas sobre escaneo, supervisión y respuesta básica ante incidentes. Eso sí, la utilidad

institucional del laboratorio va a estar condicionada a que vaya acompañado de procedimientos, de responsables que estén establecidos y de revisiones que se hagan de forma regular. Y esto es así porque, por sí solo, el laboratorio no puede reemplazar una gestión formal de ciberseguridad.

4.6.4 Limitaciones del estudio

Los resultados de este proyecto deben entenderse dentro del alcance en el que fue desarrollado. El laboratorio permitió trabajar con una arquitectura virtual, segmentada y controlada, pero no reproduce por completo la operación diaria de los sistemas del ISU Sucre. En un entorno real podrían presentarse más usuarios conectados, mayor volumen de tráfico, servicios adicionales, cambios imprevistos en la red y comportamientos que no fueron parte de las pruebas realizadas.

Es importante señalar también que los escenarios fueron establecidos para corroborar controles específicos del laboratorio. Con Wazuh y pfSense se llevó a cabo el monitoreo con respuesta, así como la exploración de vulnerabilidades, accesos no permitidos y tráfico sospechoso. Esto posibilitó la obtención de información útil, aunque no contempla otros sucesos que podrían ocurrir en una organización, tales como ataques más sofisticados, campañas de phishing, malware, filtración de datos o interrupciones prolongadas.

Finalmente, el proyecto se concentró en la parte técnica de la ciberseguridad. Por esa razón, los resultados no equivalen a la implementación completa de un Sistema de Gestión de Seguridad de la Información. Para avanzar hacia una aplicación institucional más amplia, el laboratorio tendría que complementarse con políticas, responsables, procedimientos formales, capacitación, seguimiento periódico y mejora continua.

4.6.5 Relación con ISO/NIST

En este proyecto, ISO/IEC 27001:2022 y el marco NIST sirvieron como referencia para ordenar lo que se fue comprobando en el laboratorio. La norma y el marco no se aplicaron en toda su extensión, sino en los puntos que podían evidenciarse durante las pruebas. Por ejemplo, el escaneo realizado con Nmap ayudó a revisar debilidades técnicas relacionadas con A.8.8, mientras que la

separación de la LAN, la DMZ y la red de ataque mediante pfSense permitió trabajar aspectos vinculados con seguridad y segregación de redes, como A.8.20 y A.8.22. De la misma manera, los registros observados en Wazuh dieron soporte a los controles A.8.15 y A.8.16, porque permitieron revisar eventos generados durante los escenarios.

En las pruebas de autenticación fallida, la revisión no se centró únicamente en el intento de acceso, sino en lo que el servidor dejaba registrado para analizar después el evento. Con esos registros se revisaron aspectos como usuario utilizado, hora del intento, respuesta del servicio y alerta generada, por lo que este escenario se asocia con A.5.15, A.5.16 y A.5.17, relacionados con control de acceso, gestión de identidad e información de autenticación. Luego, cuando se bloqueó en pfSense el tráfico proveniente de la red de ataque, quedó una evidencia práctica de respuesta ante un incidente simulado, vinculada con A.5.24 y A.5.26. Desde el NIST CSF, el trabajo realizado se ubica en las funciones Identify, Protect, Detect y Respond, porque primero se reconoció la exposición del entorno, después se limitaron comunicaciones, se revisaron alertas y finalmente se aplicó una medida de contención.

Esta relación no debe entenderse como una aplicación completa de ISO/IEC 27001 y NIST, sino como una revisión técnica limitada a lo que se pudo comprobar en el laboratorio. El laboratorio validó controles técnicos en un ambiente controlado, pero no cubrió todos los elementos requeridos para un Sistema de Gestión de Seguridad de la Información ni el catálogo completo de NIST SP 800-53 Rev. 5. Por ello, los resultados representan una base inicial para futuras acciones institucionales, que deberían complementarse con políticas, responsables, procedimientos, auditorías, gestión formal de riesgos y mejora continua.

4.6.6 Aporte del proyecto

El principal aporte del proyecto está en mostrar que un laboratorio virtual puede apoyar la evaluación y validación de controles de ciberseguridad en una institución educativa. Su valor va más allá de la simulación de ataques, porque integra diagnóstico, controles, evidencias y resultados dentro de una metodología pretest–postest.

El laboratorio también acerca la teoría a la práctica, al aplicar estándares internacionales en un entorno técnico controlado. Este aporte es relevante para instituciones con recursos limitados, porque muestra que el fortalecimiento digital puede iniciarse con herramientas accesibles, reproducibles y vinculadas con buenas prácticas internacionales.

CONCLUSIONES

- La implementación del laboratorio virtual de ciberseguridad permitió alcanzar el objetivo general del proyecto. El entorno controlado facilitó la simulación de ataques, la identificación de vulnerabilidades, la aplicación de controles y la evaluación de la capacidad de detección y respuesta del ISU Sucre, sin intervenir los sistemas productivos institucionales.
- En el diagnóstico inicial se encontraron deficiencias, tales como configuraciones no seguras, servicios vulnerables, poca segmentación y una supervisión bastante restringida. Todos estos resultados demostraron la importancia que tenía el laboratorio, y además se usaron para establecer una línea base que sirviera para comparar las variaciones que se dieron después de la intervención.
- Por el lado de la arquitectura que se implementó, esta empleó segmentación LAN, DMZ y una red de ataque, e incorporó Wazuh, Ubuntu Server junto con WordPress y también Kali Linux. Con esta estructura lo que se logró fue validar controles técnicos de la ISO/IEC 27001:2022, del NIST SP 800-53 Rev. 5 y de las funciones del NIST CSF, todo ello dentro de un entorno institucional regulado.
- Los resultados obtenidos evidenciaron una reducción de vulnerabilidades de 26 a 11, una mejora en la capacidad de detección de eventos de seguridad del 25 % al 100 % y una disminución en los tiempos de detección y respuesta. Estos resultados demuestran la efectividad de los controles implementados mediante segmentación de red, endurecimiento de servicios, monitoreo centralizado con Wazuh y mecanismos de bloqueo gestionados por pfSense.
- Los resultados deben ser entendidos dentro del alcance que tuvo el proyecto. Hay que tener en cuenta que el laboratorio funcionó en un entorno virtual controlado, con escenarios definidos y sin condiciones propias de una infraestructura productiva completa, como podrían ser alta concurrencia de usuarios, tráfico masivo o amenazas avanzadas persistentes. Por esta razón, el laboratorio constituye una base técnica inicial para el ISU Sucre, pero eso sí, debe complementarse con políticas, procedimientos, gestión de riesgos y con un SGSI formal.

RECOMENDACIONES

- El ISU Sucre puede tomar los controles probados en el laboratorio como primer paso para ordenar su seguridad de la información. A partir de esa base, conviene definir quién estará a cargo de cada actividad, qué procedimientos se van a documentar y cómo se revisarán los avances. También sería necesario dejar aprobadas políticas internas y conservar evidencias de los cambios realizados, para que la mejora no dependa solo de configuraciones técnicas.

- Poner en práctica un ciclo recurrente de administración de vulnerabilidades que incluya la verificación posterior, el escaneo, la clasificación, la priorización y la remediación. Esta práctica contribuirá a que los servicios institucionales estén actualizados y a que la superficie de ataque sea más pequeña.

- Antes de llevar algún control al entorno real del ISU Sucre, conviene revisar cuáles funcionaron mejor en el laboratorio y cuáles pueden aplicarse sin afectar los servicios académicos. Se puede iniciar con ajustes puntuales en la segmentación de red, reglas básicas de firewall, accesos permitidos y respaldos. Cada cambio debería quedar documentado para facilitar su seguimiento y evitar modificaciones sin control.

- Para los servicios críticos del ISU Sucre, se podría mejorar el monitoreo con una herramienta centralizada, tomando como base las pruebas que se hicieron con Wazuh. Pero no es suficiente con instalar la herramienta; también hace falta definir quién revisa las alertas, cuándo se atienden y qué se hace dependiendo de la gravedad del evento.

- Lo recomendable es conservar el laboratorio virtual como un espacio de prueba antes de aplicar cambios en sistemas reales. También sirve para prácticas académicas y para que el personal técnico se capacite. Más adelante se pueden añadir escenarios como phishing, malware, caídas de servicio, recuperación y respuesta a incidentes más graves.

REFERENCIAS

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. https://doi.org/10.18235/0002513

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences, 11(4), 1809.* https://doi.org/10.3390/app11041809

Conti, M., Dargahi, T., & Dehghantanha, A. (agosto de 2018). Cyber threat intelligence: Challenges and opportunities. En *Cyber threat intelligence* (págs. 1-6). Springer. https://doi.org/10.1007/978-3-319-73951-9_1

European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. https://doi.org/10.2824/782573

European Union Agency for Cybersecurity. (2026). The ENISA cybersecurity exercise methodology. https://doi.org/10.2824/4949728

FIRST. (2023). *Common Vulnerability Scoring System version 4.0: Specification document. Forum of Incident Response and Security Teams*. https://www.first.org/cvss/specification-document

ISO/IEC. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* https://www.iso.org/standard/27001

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Agenda de Transformación Digital del Ecuador 2022–2025.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf

Moreano Guerra, C., Huera Páez, G., Pesántez Huanga, C., & Franco Rocha, Y. (18 de julio de 2023). Seguridad en la plataforma moodle, utilizada por los Institutos Superiores Tecnológicos públicos del Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*. https://doi.org/10.37811/cl_rcm.v7i4.6884

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations.* https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://doi.org/10.6028/NIST.CSWP.29

OWASP Foundation. (2020). *Web Security Testing Guide v4.2*. https://owasp.org/www-project-web-security-testing-guide/v42/

OWASP Foundation. (2025). *OWASP Top 10:2025*. https://owasp.org/Top10/2025/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (Agosto de 2020). *Zero Trust Architecture.* https://doi.org/10.6028/NIST.SP.800-207

Scarfone, K., Souppaya, M., & Hoffman, P. (2011). Guide to security for full virtualization technologies (NIST Special Publication 800-125). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-125

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment (NIST Special Publication 800-115). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-115

Shadish, W., Cook, T., & Campbell, D. (2002). *Experimental and Quasi-experimental Designs for Generalized Causal Inference.* https://books.google.com.ec/books/about/Experimental_and_Quasi_experimental_Desi.html?id=o7jaAAAAMAAJ&redir_esc=y

UNESCO. (2020). *La educación en un mundo post-COVID*. UNESCO: https://unesdoc.unesco.org/ark:/48223/pf0000373717_spa

Wazuh. (s. f.). *Data analysis*. Wazuh Documentation: https://documentation.wazuh.com/current/user-manual/ruleset/index.html

Yamin, M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. https://doi.org/10.1016/j.cose.2019.101636

ANEXOS

Anexo 1. Matriz de identificación de vulnerabilidades.

La matriz se usó para ordenar la información que se obtuvo en la revisión inicial de los activos tecnológicos del ISU Sucre. Ahí se registraron las debilidades que se encontraron en servicios, plataformas institucionales y componentes del diagnóstico, además de datos como criticidad, impacto, probabilidad, nivel de riesgo y controles sugeridos.

Los datos registrados en la matriz ayudaron a conocer cómo estaba el entorno antes de montar el laboratorio virtual. A partir de esa revisión se pudo ubicar qué servicios estaban más expuestos, qué debilidades aparecían con mayor frecuencia y qué controles podían revisarse después. Esta información se conectó con ISO/IEC 27001:2022 y NIST SP 800-53 Rev. 5, sobre todo en temas de vulnerabilidades, monitoreo y protección de los servicios institucionales.

Matriz de identificación y clasificación de vulnerabilidades

ID	Activo afectado	Tipo de activo	Vulnerabilidad identificada	Tipo de vulnerabilidad	Descripción / evidencia	Criticidad	Impacto (Confidencialidad Integridad Disponibilidad)	Probabilidad	Riesgo	Control recomendado	Estado	Fecha	Responsable
VUL-001	Servidor Web (VPS)	Software / infraestructura	Servicios expuestos y versión vulnerable a ataques conocidos	Exposición de servicios	Servidor web expuesto a Internet con servicios activos que requieren actualización, endurecimiento y monitoreo permanente.	Alta	Alto-Alto-Medio	Alta	Crítico	Actualizar servicios, aplicar hardening del servidor, revisar puertos expuestos y monitorear eventos. ISO A.8.8 / NIST RA-5.	En proceso	10/04/2026	Coordinador de TI
VUL-002	Aulas virtuales (Moodle)	Software	Uso de contraseñas débiles o por defecto	Control de acceso débil	Riesgo de acceso no autorizado por credenciales débiles, reutilizadas o sin políticas robustas de autenticación.	Media	Medio-Alto-Medio	Media	Alto	Aplicar política de contraseñas, limitar intentos fallidos, revisar usuarios activos y fortalecer autenticación. ISO A.5.15, A.5.17 / NIST AC-2.	Mitigado parcialmente	No registrada	Unidad de TICs
VUL-003	Página web institucional	Software / aplicación web	CMS, plugins o configuraciones web con posibles debilidades	Vulnerabilidad web	Exposición de componentes web que pueden facilitar enumeración de usuarios, explotación de formularios o ataques automatizados.	Alta	Medio-Alto-Medio	Alta	Alto	Actualizar CMS, temas y plugins; proteger archivos críticos; limitar intentos de acceso y revisar permisos. ISO A.8.8 / NIST SI-2.	En proceso	20/3/2026	Unidad de TICs
VUL-004	Sucre Review	Software / sistema institucional	Vulneración reportada sin registro formal	Control de acceso débil	Sistema reportado como vulnerado; no existe registro institucional formal de fecha, vector de ataque, impacto o acciones de contención.	Crítica	Alto-Alto-Medio	Alta	Crítico	Registrar incidente, levantar bitácora, revisar accesos, restablecer credenciales, validar integridad y aplicar monitoreo. ISO A.5.24, A.5.26 / NIST IR-4.	Pendiente de documentación	20/3/2026	Unidad de TICs
VUL-005	SAGA	Software / sistema institucional	Vulneración reportada sin registro formal	Control de acceso débil	Sistema reportado como vulnerado; no se dispone de evidencia documentada sobre alcance, causa, fecha o acciones de respuesta.	Crítica	Alto-Alto-Alto	Alta	Crítico	Documentar incidente, revisar logs disponibles, cambiar credenciales, auditar usuarios, verificar integridad de datos y segmentar accesos. ISO A.5.24, A.5.26 / NIST IR-4, AU-6.	Pendiente de documentación	20/3/2026	Unidad de TICs
VUL-006	SIG	Software / sistema institucional	Vulneración reportada sin registro formal	Control de acceso débil	Sistema reportado como vulnerado; no existe trazabilidad institucional del evento ni registro técnico de investigación.	Crítica	Alto-Alto-Alto	Alta	Crítico	Crear registro de incidente, revisar autenticación, validar integridad, fortalecer accesos y definir procedimiento de reporte. ISO A.5.24, A.5.26 / NIST IR-6.	Pendiente de documentación	20/3/2026	Unidad de TICs

Anexo 2. Ficha de evaluación de pruebas de penetración — Pretest

La presente ficha fue utilizada como instrumento de recolección de información técnica durante la fase de pretest del proyecto. Su propósito fue documentar los escenarios de prueba ejecutados antes de la implementación de controles de seguridad en el laboratorio virtual de ciberseguridad.

Este instrumento permitió registrar los escenarios de ataque, herramientas utilizadas, resultados obtenidos, controles evaluados y observaciones generales relacionadas con el estado inicial del entorno. La información recopilada sirve como evidencia para establecer la línea base de seguridad y posteriormente comparar los resultados con la fase postest.

Datos generales

Código de prueba	Fecha	Evaluador	Sistema evaluado	Tipo de prueba	Herramienta utilizada	Objetivo de la prueba
Identificador único de la prueba	Fecha de ejecución	Responsable de la prueba	Nombre del sistema / aplicación	Interna / Externa / Caja negra / Caja gris / Caja blanca	Ej: Kali Linux, Metasploit, Nmap, etc.	Descripción breve del objetivo
PT-PRE-001	29/4/2026	Victoria Guachán	Portal web institucional / servidor web	Caja blanca	Nmap	Identificar puertos abiertos, servicios expuestos y vulnerabilidades iniciales.
PT-PRE-002	29/4/2026	Victoria Guachán	Servicio de autenticación / SSH	Caja blanca	Hydra / SSH	Evaluar intentos de acceso no autorizado y debilidades en control de accesos.
PT-PRE-003	29/4/2026	Victoria Guachán	Servidor web institucional	Caja blanca	Nmap / curl / SSH	Generar tráfico sospechoso para observar la capacidad inicial de detección.
PT-PRE-004	29/4/2026	Victoria Guachán	Entorno de monitoreo y respuesta	Caja blanca	Wazuh / pfSense	Evaluar la capacidad inicial de monitoreo, detección y respuesta ante eventos de seguridad.

Escenario de ataque

Tipo de ataque	Vector de ataque	Vulnerabilidad explotada	Nivel de criticidad
Ej: Fuerza bruta, SQL Injection, XSS, Escaneo de puertos	Medio utilizado para el ataque	Identificada previamente o descubierta	Bajo / Medio / Alto / Crítico
Escaneo de vulnerabilidades	Escaneo de red y servicios sobre el servidor objetivo	configuraciones inseguras y posibles debilidades web	Alto
Intento de acceso no autorizado	Intentos controlados de autenticación fallida	Credenciales débiles y control de acceso insuficiente	Alto
Generación de tráfico sospechoso	Escaneo de puertos, intentos SSH y peticiones web sospechosas	Ausencia de monitoreo centralizado y correlación de eventos	Medio
Monitoreo y respuesta a eventos	Generación de evento controlado para medir detección y respuesta	Respuesta no estructurada y limitada capacidad de alerta	Alto

Resultados

Detección (1/0)	Tiempo de detección	Tiempo de respuesta	Ataque exitoso (1/0)	Nivel de impacto	Evidencia generada (1/0)
El sistema detectó el ataque	Tiempo en detectar el ataque	Tiempo en aplicar acción correctiva	El ataque logró su objetivo	Afectación generada	Registro en logs o alertas
Sí (1) / No (0)	Segundos / minutos	Segundos / minutos	Sí (1) / No (0)	Bajo / Medio / Alto	Sí (1) / No (0)
0	No detectado	No aplicada	1	Alto	1
0	No detectado	No aplicada	1	Alto	1
0	No detectado	No aplicada	1	Medio	1
1	9 min	20 min	1	Alto	1

Controles

Control evaluado	Estado (Eficiente/Deficiente)	Observación
Firewall	Deficiente	Control limitado; no existía segmentación efectiva ni reglas suficientes para contener tráfico no autorizado.
IDS/IPS	Deficiente	No se evidenció un mecanismo especializado de detección o prevención de intrusiones en la fase pretest.
Control de accesos	Deficiente	Se identificaron debilidades asociadas a autenticación, credenciales y ausencia de políticas robustas.
Monitoreo (SIEM/Wazuh)	Deficiente	La capacidad de monitoreo centralizado era inexistente o limitada antes de la implementación del laboratorio.

Observaciones

Observaciones técnicas
Durante el pretest se evidenciaron 26 vulnerabilidades totales y 15 vulnerabilidades críticas. Los principales hallazgos estuvieron asociados a servicios expuestos, configuraciones inseguras, controles de acceso débiles, ausencia de monitoreo centralizado y respuesta no estructurada ante incidentes. Solo se identificó un evento de forma tardía, con un tiempo aproximado de detección de 9 minutos y respuesta de 20 minutos. Se recomienda aplicar segmentación de red, endurecimiento de servicios, monitoreo mediante SIEM y documentación formal de incidentes.

Resultado General

Riesgo identificado	Nivel de seguridad	Riesgo asociado	Requiere mitigación (Sí/No)
	Bajo / Medio / Alto	Bajo / Medio / Alto / Crítico	Sí / No
Exposición de servicios	Bajo	Alto	Sí
Vulnerabilidad en autenticación	Bajo	Crítico	Sí
Falta de monitoreo centralizado	Bajo	Crítico	Sí
Tráfico sospechoso no correlacionado	Bajo	Alto	Sí
Respuesta a incidentes no estructurada	Bajo	Crítico	Sí

Anexo 3. Matriz pretest–postest.

La presente matriz se elaboró como instrumento de recolección y comparación de datos técnicos obtenidos antes y después de la implementación del laboratorio virtual de ciberseguridad. Su propósito fue medir la variación de los principales indicadores de seguridad, considerando vulnerabilidades detectadas, capacidad de detección, tiempo medio de detección, tiempo medio de respuesta y éxito de los ataques simulados.

Este instrumento permitió evidenciar el impacto de los controles implementados en el laboratorio, tales como segmentación de red, reglas de firewall, endurecimiento de servicios, monitoreo mediante Wazuh y respuesta ante eventos mediante pfSense.

Código de prueba	Indicador	Valor Pretest 0/1	Valor Postest	Diferencia	Mejora (%)	Interpretación
P01	Vulnerabilidades totales	26	11	-15	57,69%	Reducción global de vulnerabilidades
P02	Vulnerabilidades críticas	15	5	-10	66,67%	Disminución de vulnerabilidades críticas
P03	Tasa de detección	25,00%	100,00%	75,00%	75,00%	Mejora de 75 puntos porcentuales
P04	MTTD - tiempo de detección (seg.)	540	5	-535	99,07%	Reducción de 9 min a 5 segundos
P05	MTTR - tiempo de respuesta (seg.)	1200	198	-1002	83,50%	Reducción de 20 min a 3 min 18 s

Anexo 4. Guía de entrevista.

El objetivo de este instrumento fue recopilar información del área de Tecnologías de la Información sobre el estado actual de la ciberseguridad institucional, los controles existentes, los activos críticos, las amenazas identificadas y la necesidad de implementar un laboratorio virtual de ciberseguridad basado en estándares ISO/NIST.

Tabla 22.

Matriz de resultados del formulario aplicado al personal de TIC

Aspecto evaluado	Resultado obtenido	Relación con el proyecto
Estado actual de ciberseguridad	Se identifica un nivel inicial de madurez, con controles básicos y ausencia de una gestión formal de riesgos.	Este resultado respalda la necesidad de fortalecer la seguridad institucional mediante una propuesta estructurada.
Activos críticos institucionales	Se identifican sistemas académicos, sitio web, bases de datos, servidor principal, red	La información obtenida ayuda a priorizar los

	institucional, centro de datos e información administrada por TIC.	activos que requieren protección dentro del diagnóstico y del laboratorio virtual.
Amenazas e incidentes	Se reconocen amenazas como ataques web, SQL Injection, accesos no autorizados, malware, errores humanos e interrupción de servicios. No existen incidentes formalmente registrados, aunque se reporta contenido sospechoso en el sitio web.	Estos datos orientan la selección de escenarios de prueba y muestran la necesidad de mejorar el registro de incidentes.
Controles y monitoreo	Existen controles básicos de acceso mediante usuario y contraseña, pero no se cuenta con monitoreo centralizado mediante logs, alertas o SIEM.	Este resultado apoya la incorporación de controles de detección y monitoreo dentro del laboratorio virtual.
Limitaciones institucionales	Se identifican limitaciones técnicas, ausencia de políticas formales, falta de auditorías, baja gestión de riesgos y dependencia del área TIC.	Las brechas identificadas deben considerarse en el diseño de la propuesta.
Necesidad del laboratorio virtual	Se considera necesario para simular ataques, analizar vulnerabilidades, detectar eventos, practicar respuesta ante incidentes y evaluar controles sin afectar sistemas reales.	Este resultado respalda la pertinencia del proyecto y su relación con el objetivo general.

Nota. La matriz resume los principales resultados del formulario aplicado al personal de TIC.

Según el área TIC, el ISU Sucre sí tiene algunas medidas básicas, por ejemplo, controles de acceso con usuario y contraseña. El problema es que no hay monitoreo centralizado de logs ni alertas, tampoco hay un registro formal de incidentes ni un proceso que revise vulnerabilidades de vez en cuando.

Por eso el laboratorio virtual sirve como un espacio de prueba aparte de los sistemas reales. Ahí se pueden recrear situaciones de riesgo, revisar configuraciones y sacar evidencias técnicas. Toda esta información también se conecta con los criterios ISO/NIST del proyecto, sobre todo en lo que tiene que ver con vulnerabilidades, monitoreo y respuesta ante incidentes.

Anexo 5. Cuestionario estructurado.

Para este anexo se aplicó una encuesta con un formulario digital. Respondieron estudiantes y docentes del ISU Sucre. Se les preguntó sobre sus hábitos de seguridad digital, lo que saben de amenazas informáticas y cómo ven los riesgos cuando usan las plataformas de la institución.

Las respuestas se recibieron del 20 de abril al 11 de mayo de 2026. En total se consiguieron 337 respuestas válidas: 245 eran de estudiantes y 92 de docentes. Con estos resultados se complementó el diagnóstico técnico del proyecto y se identificaron varias necesidades: capacitación, uso de herramientas de seguridad, mejorar las contraseñas y tener políticas institucionales.

Tabla 23.

Resultados consolidados del cuestionario aplicado a estudiantes y docentes

Pregunta / indicador	Resultado principal
Uso de contraseñas diferentes	31,16 % respondió “A veces” 29,97 % “Frecuentemente” 29,38 % “Siempre” 7,12 % “Rara vez” 2,37 % “Nunca”.
Cambio de contraseñas	38,28 % cambia sus contraseñas una vez al año 29,67 % cada 6 meses 16,32 % cada 3 meses 15,73 % nunca las cambia.
Uso de autenticación en dos factores (2FA)	61,13 % sí utiliza autenticación en dos factores 23,44 % no la utiliza 13,06 % no sabe qué es 2,37 % respondió “Nunca”.
Conocimiento sobre phishing o malware	86,05 % ha escuchado sobre ataques como phishing o malware. El 13,95 % no los conoce.
Identificación de correos sospechosos	80,71 % considera que podría identificar un correo electrónico sospechoso. El 19,29 % indicó que no.
Víctima de incidente digital	32,05 % indicó haber sido víctima de algún incidente digital, como hackeo, robo de cuenta o virus

	El 67,95 % respondió que no.
Seguridad percibida de plataformas institucionales	65,28 % considera seguras las plataformas institucionales 21,36 % poco seguras 9,50 % muy seguras 3,86 % inseguras.
Detección de fallos en sistemas institucionales	33,83 % indicó haber detectado fallos o problemas de seguridad en los sistemas institucionales. El 66,17 % respondió que no.
Importancia de la ciberseguridad	83,38 % considera la ciberseguridad muy importante 15,73 % importante 0,89 % poco importante.
Capacitación recibida	68,25 % no ha recibido capacitación en ciberseguridad. El 31,75 % sí la ha recibido.
Interés en recibir capacitación	91,10 % indicó que sí le gustaría recibir capacitación en ciberseguridad. El 8,90 % respondió que no.
Acciones necesarias para mejorar la ciberseguridad	80,12 % señaló la necesidad de capacitaciones 76,85 % implementación de herramientas 38,58 % políticas institucionales 26,41 % mejora de contraseñas.

Nota. Para proteger la privacidad de los participantes, se presentan únicamente resultados consolidados, sin incluir correos electrónicos ni datos personales de los encuestados.

Anexo 6. Ficha de análisis documental.

Para este anexo se revisó la documentación disponible en la Unidad de TIC del Instituto Superior Universitario Sucre. La revisión se centró en conocer qué documentos existían sobre el manejo tecnológico de la institución y qué información podía servir como apoyo para el diagnóstico de seguridad.

En la Unidad de TIC se encontraron pocos documentos útiles para el diagnóstico. Entre ellos estaban una política de contraseñas aplicada hace poco, un inventario de activos tecnológicos que aún se estaba actualizando y un manual del sistema SIG. Aunque estos documentos ayudan a conocer parte del trabajo tecnológico de la institución, todavía no son suficientes para ordenar de manera completa la seguridad de la información.

En la Unidad de TIC no se ubicaron registros ni documentos suficientes sobre ciberseguridad. Faltaban reportes de vulnerabilidades, historial de incidentes, diagramas de red actualizados y procedimientos para responder ante eventos. Esta situación dificulta revisar casos anteriores y priorizar los controles que deberían organizarse en el ISU Sucre.

A partir de esta revisión, el laboratorio puede servir como base para empezar a documentar mejor la seguridad del ISU Sucre. En las pruebas se registraron vulnerabilidades, alertas y acciones de respuesta dentro de un entorno separado. Estos datos pueden ayudar luego a crear procedimientos internos y a organizar el seguimiento de eventos de seguridad.

Diagnóstico de Documentación en la Unidad de Tecnologías de la Información y Comunicación (TICs)				
Nombre del responsable:	Gabriel Caicedo			
Cargo:	Responsable de TICs			
Área / Unidad:	Unidad de Tecnologías de la Información y Comunicación (TICs)			
SECCIÓN 2: EXISTENCIA DE DOCUMENTACIÓN	**Existe**	**No existe**	**Desconoce**	
Política de seguridad de la información		X		
Política de control de accesos		X		
Política de contraseñas	X			
Plan de gestión de riesgos		X		
Plan de continuidad del negocio		X		
Plan de recuperación ante desastres		X		
Procedimiento de gestión de incidentes		X		
Inventario de activos tecnológicos	X			
Diagramas de red		X		
Manuales de sistemas	X			
Registro de incidentes		X		
Informes de auditoría o vulnerabilidades		X		

SECCIÓN 3: ESTADO DE LA DOCUMENTACIÓN	**Actualizado**	**Desactualizado**	**En elaboración**	**No aplica**
Política de seguridad de la información				X
Política de control de accesos				X
Política de contraseñas	X			
Plan de gestión de riesgos				X
Plan de continuidad del negocio				X
Plan de recuperación ante desastres				X
Procedimiento de gestión de incidentes				X
Inventario de activos tecnológicos	X			
Diagramas de red				X
Manuales de sistemas			X	
Registro de incidentes				X
Informes de auditoría o vulnerabilidades				X

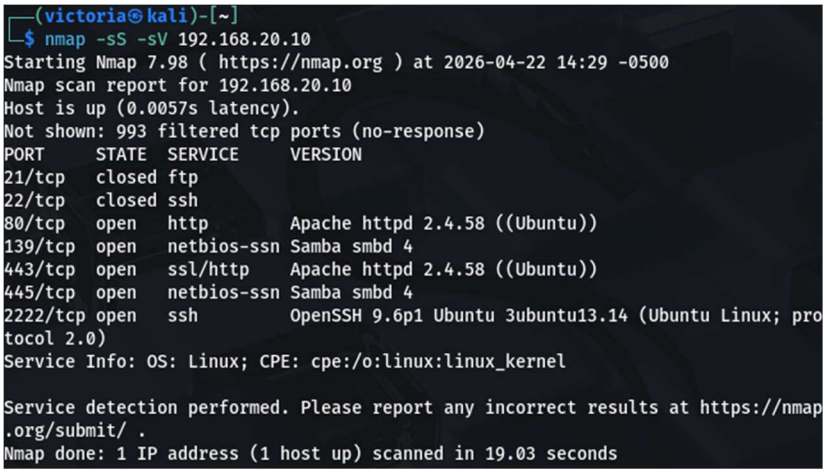
SECCIÓN 4: NIVEL DE APLICACIÓN	Se aplica completamente	Se aplica parcialmente	No se aplica	
Política de seguridad de la información			X	
Política de control de accesos			X	
Política de contraseñas		X		
Plan de gestión de riesgos			X	
Plan de continuidad del negocio			X	
Plan de recuperación ante desastres			X	
Procedimiento de gestión de incidentes			X	
Inventario de activos tecnológicos	X			
Diagramas de red			X	
Manuales de sistemas		X		
Registro de incidentes			X	
Informes de auditoría o vulnerabilidades			X	
SECCIÓN 5: GESTIÓN Y CONTROL	**SI**	**NO**		
¿La documentación TI se encuentra centralizada?		X		
¿Existe un responsable de mantener actualizada la documentación?		X		
¿Se revisa periódicamente la documentación?		X		
	Mensual	**Semestral**	**Anual**	**No se actualiza**
Frecuencia de actualización:				X

SECCIÓN 6: CIBERSEGURIDAD	SI	NO		
¿Existen políticas formales de seguridad de la información?		X		
¿Se documentan los incidentes de seguridad?		X		
¿Se han realizado auditorías de seguridad?		X		
Principales debilidades en la documentación TI	**OBSERVACIÓN**			
	La documentación de TICs es limitada y no está centralizada. Solo se evidencia política de contraseñas reciente, inventario de activos en consolidación y manual del SIG; no existen planes, procedimientos, diagramas, registros ni auditorías formales de ciberseguridad.			
Recomendaciones para mejorar la gestión documental	Crear un repositorio documental, designar responsable y definir revisiones periódicas. Priorizar políticas de seguridad y accesos, gestión de incidentes, continuidad, recuperación, diagramas de red y registros, alineados con ISO/IEC 27001:2022 y NIST.			

Anexo 7. Escenario 1: Escaneo de vulnerabilidades

Figura 2.

Escaneo de red (puertos + servicios)

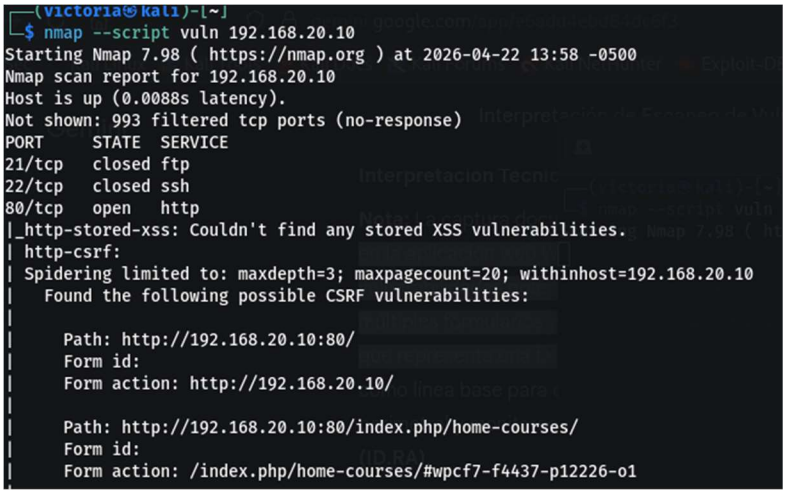


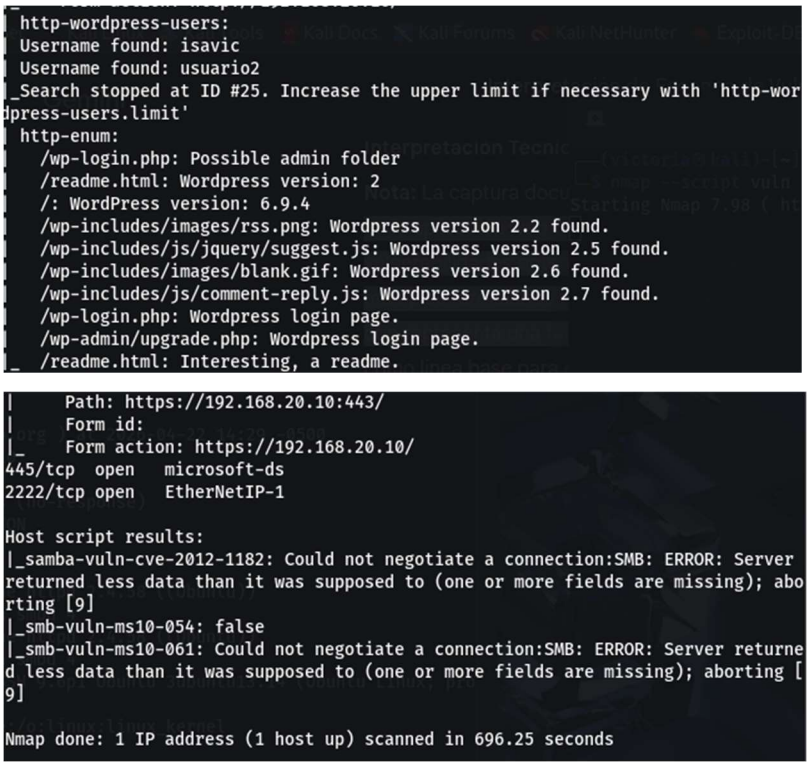
Nota. Escaneo de puertos y detección de versiones (`-sS -sV`) sobre el servidor institucional, identificando servicios críticos como Apache 2.4.58 y OpenSSH 9.6p1.

Justifica los controles de seguridad ISO/IEC 27001 (A.8.8) y NIST CSF (ID.AM).

Figura 3.

Vulnerabilidades detectadas





Nota. Identifica debilidades en la aplicación web WordPress y servicios de red del servidor institucional. Se detectaron vulnerabilidades potenciales en múltiples formularios y se realizó una enumeración de usuarios exitosa (isavic, usuario2), lo que representa una falla de seguridad en el control de acceso.

Con una máquina atacante que se configuró en Kali Linux, se realizó un escaneo de vulnerabilidades con Nmap. El análisis encontró servicios expuestos, puertos abiertos y posibles debilidades en la configuración del sistema objetivo.

Anexo 8. Escenario 2: Intento de acceso no autorizado (Fuerza bruta básica)

Para este escenario se crea un usuario

Usuario: usuario_test

Contraseña: 123456

Figura 4.

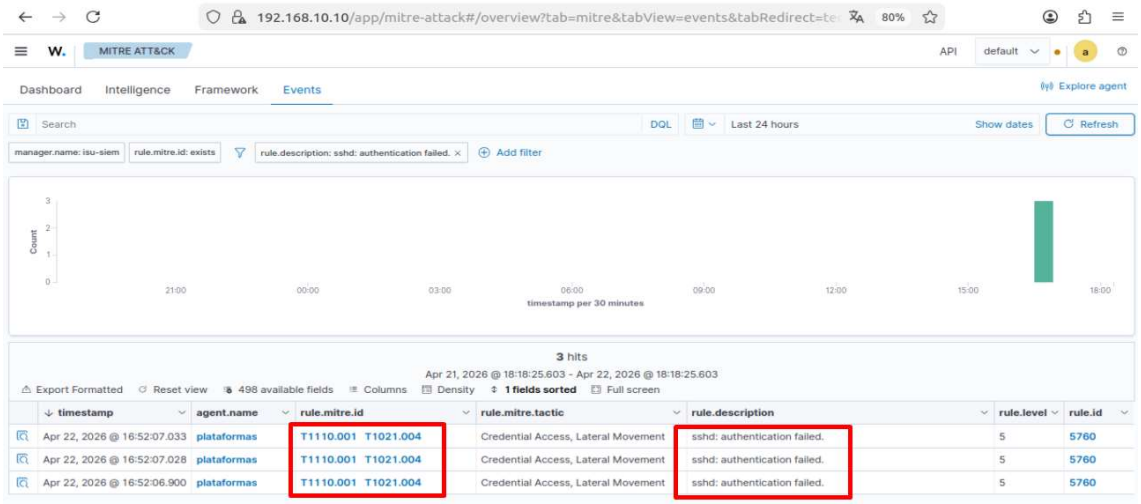
Ataque de fuerza bruta – usuario conocido

```
┌──(victoria㉿kali)-[~]
└─$ hydra -l usuario_test -P /usr/share/wordlists/escenario.txt -s 2222 -t 4 ssh
://192.168.20.10
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-04-22 16:37:
27
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tr
ies per task
[DATA] attacking ssh://192.168.20.10:2222/
[2222][ssh] host: 192.168.20.10   login: usuario_test   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-04-22 16:37:
31
```

Nota. Se observa el uso de la herramienta Hydra para realizar un ataque de fuerza bruta del servidor objetivo (192.168.20.10).

Figura 5.

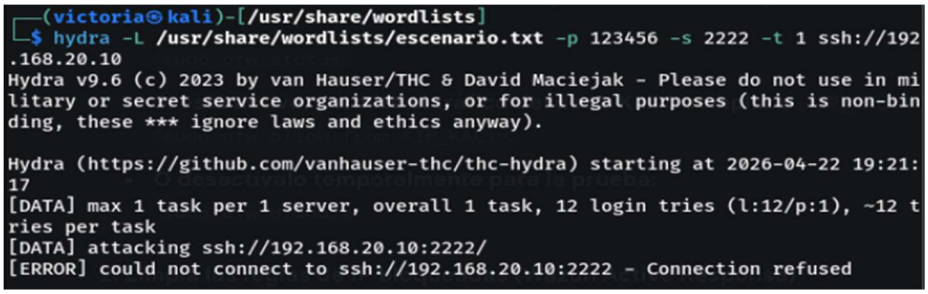
Detección de Ataque de Fuerza Bruta mediante Wazuh



Nota. El sistema ha identificado automáticamente el intento de acceso no autorizado realizado por la herramienta Hydra

Figura 6.

Ataque de fuerza bruta – usuario desconocido

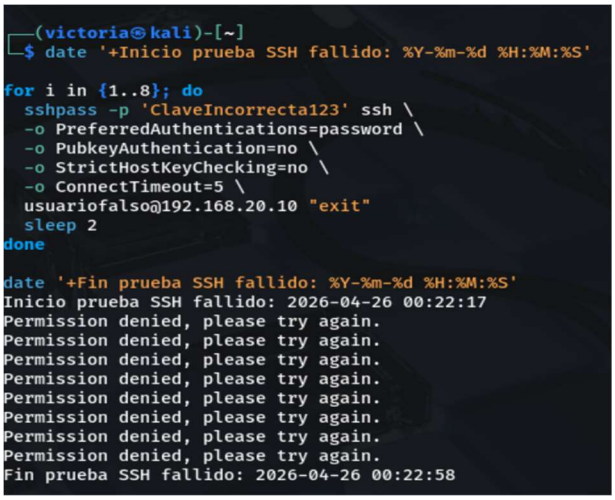


Nota. la ejecución de ataques de fuerza bruta dirigidos mediante Hydra activó un estado de denegación de servicio por protección.

Anexo 9. Escenario 3: Generación de tráfico sospechoso.

Figura 7.

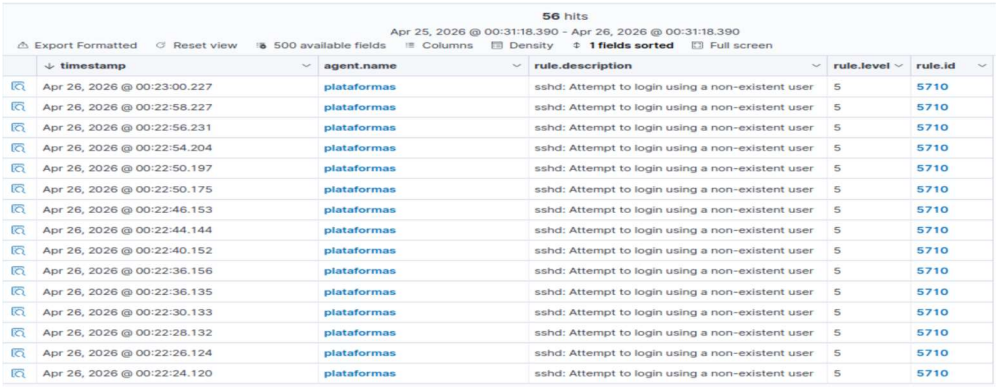
Generación de intentos fallidos de autenticación SSH desde Kali Linux.



Nota. Lo que muestra la figura son los intentos fallidos de autenticación SSH. Se ejecutaron de forma controlada con Kali Linux apuntando a un servidor que Wazuh tenía monitoreado. La idea de estos eventos era simular un acceso no autorizado dentro del laboratorio virtual.

Figura 8.

Detección de autenticación fallida SSH en Wazuh.



56 hits

Apr 25, 2026 @ 00:31:18.390 - Apr 26, 2026 @ 00:31:18.390

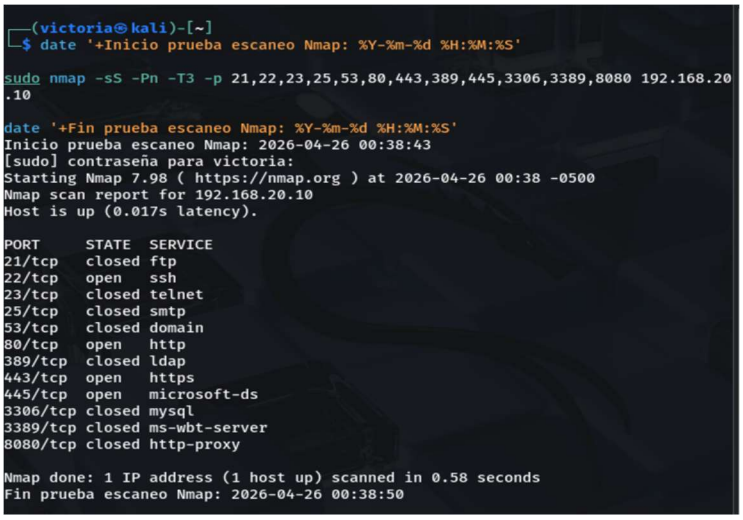
Export Formatted | Reset view | 500 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 26, 2026 @ 00:23:00.227	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:58.227	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:56.231	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:54.204	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:50.197	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:50.175	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:46.153	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:44.144	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:40.152	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:36.156	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:36.135	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:30.133	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:28.132	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:26.124	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 00:22:24.120	plataformas	sshd: Attempt to login using a non-existent user	5	5710

Nota. En la figura se observan los eventos que registró Wazuh durante los intentos fallidos de autenticación SSH desde Kali Linux hacia el servidor monitoreado. También se ve la regla 5710, que tiene que ver con intentos de inicio de sesión con un usuario que no existe.

Figura 9.

Generación de tráfico de reconocimiento mediante escaneo de puertos con Nmap.

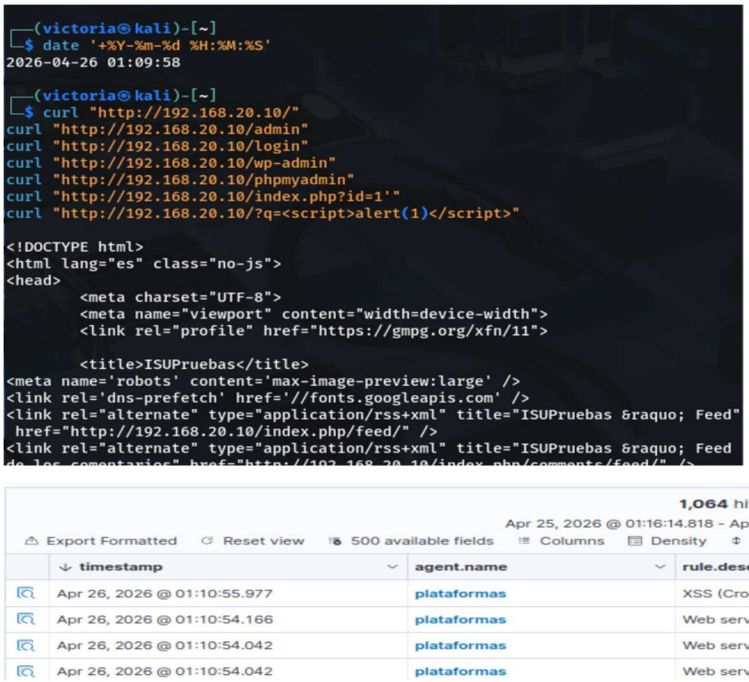


```
┌──(victoria㉿kali)-[~]
└─$ date '+Inicio prueba escaneo Nmap: %Y-%m-%d %H:%M:%S'

sudo nmap -sS -Pn -T3 -p 21,22,23,25,53,80,443,389,445,3306,3389,8080 192.168.20
.10

date '+Fin prueba escaneo Nmap: %Y-%m-%d %H:%M:%S'
Inicio prueba escaneo Nmap: 2026-04-26 00:38:43
[sudo] contraseña para victoria:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-26 00:38 -0500
Nmap scan report for 192.168.20.10
Host is up (0.017s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
445/tcp  open   microsoft-ds
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
Fin prueba escaneo Nmap: 2026-04-26 00:38:50
```

Nota. En la figura se observa el escaneo de puertos que se ejecutó desde Kali Linux hacia un activo interno del laboratorio. Esta prueba dejó tráfico sospechoso relacionado con actividades de reconocimiento de red.

Figura 10.

Generación de peticiones web sospechosas desde Kali Linux mediante comandos curl.

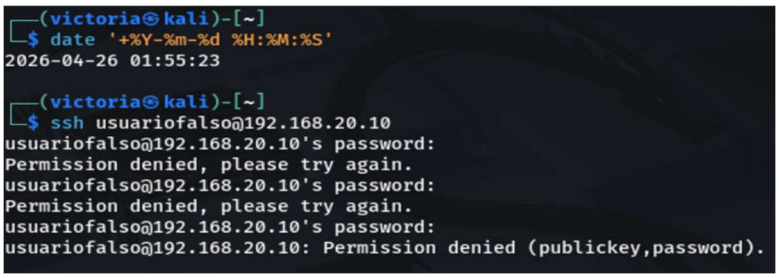


Nota. Los eventos fueron generados en un entorno controlado mediante comandos `curl` ejecutados desde Kali Linux hacia el servidor web interno. La detección de las reglas `31105` y `31101` en Wazuh evidencia que la plataforma identificó tráfico web sospechoso relacionado con intentos de exploración y prueba de entradas potencialmente maliciosas.

Anexo 10. Escenario 4: Monitoreo y respuesta ante eventos de seguridad

Figura 11.

Intento fallido de autenticación generado desde Kali Linux



Nota. La figura muestra los intentos fallidos de autenticación por SSH generados desde Kali Linux hacia el servidor Ubuntu. La prueba permitió revisar si Wazuh detectaba el evento dentro del laboratorio.

Figura 12.

Detección de intento fallido de autenticación en Wazuh

1,078 hits

Apr 25, 2026 @ 01:56:14.217 - Apr 26, 2026 @ 01:56:14.217

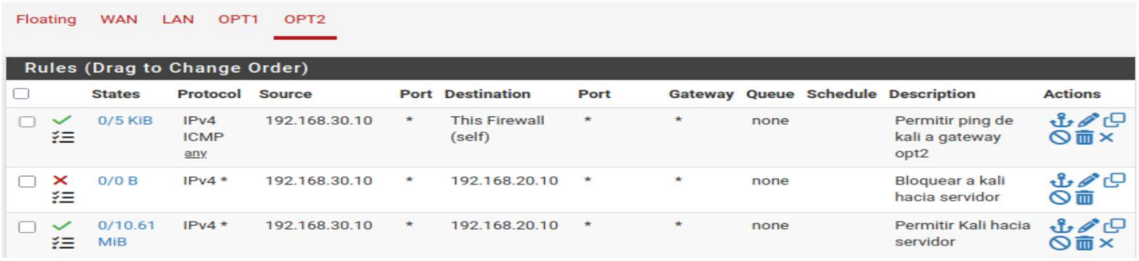
Export Formatted | Reset view | 500 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 26, 2026 @ 01:55:44.314	plataformas	syslog: User missed the password more than o...	10	2502
Apr 26, 2026 @ 01:55:44.310	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 01:55:40.307	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 01:55:36.303	plataformas	sshd: Attempt to login using a non-existent user	5	5710
Apr 26, 2026 @ 01:55:34.305	plataformas	PAM: User login failed.	5	5503
Apr 26, 2026 @ 01:55:32.299	plataformas	sshd: Attempt to login using a non-existent user	5	5710

Nota. La figura muestra la alerta registrada en Wazuh por los intentos fallidos de autenticación SSH. Con este evento se verificó el monitoreo y la correlación dentro del laboratorio. Fuente: Elaboración propia.

Figura 13.

Respuesta - Regla de bloqueo creada en pfSense



Floating | WAN | LAN | OPT1 | OPT2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/5 KiB	IPv4 ICMP any	192.168.30.10	*	This Firewall (self)	*	*	none		Permitir ping de kali a gateway opt2	
0/0 B	IPv4 *	192.168.30.10	*	192.168.20.10	*	*	none		Bloquear a kali hacia servidor	
0/10.61 MiB	IPv4 *	192.168.30.10	*	192.168.20.10	*	*	none		Permitir Kali hacia servidor	

Nota. En la figura se visualiza la regla que se configuró en pfSense para bloquear el tráfico que venía desde Kali Linux hacia el servidor de la zona DMZ. Fuente: Elaboración propia.

Tabla 24.

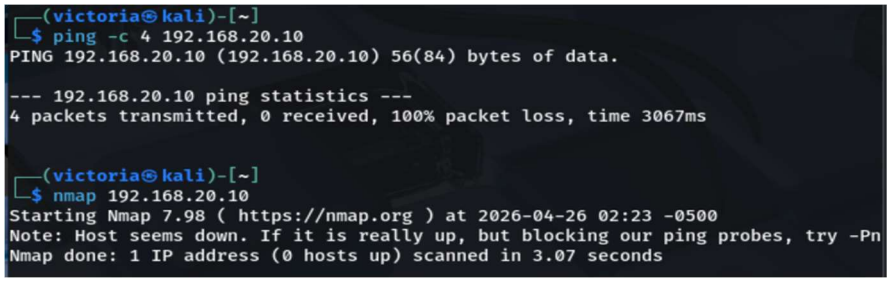
Resultados del escenario de monitoreo y respuesta a eventos de seguridad

Elemento	Cómo medirlo
Hora de generación del evento	01:55:23
Hora de detección en Wazuh	01:55:32
Tiempo de detección	9 segundos
Respuesta aplicada	Registro del evento en Wazuh, análisis de la IP origen y recomendación de bloqueo del acceso SSH desde la red de ataque

Nota. La tabla recoge el tiempo transcurrido entre el intento fallido de autenticación y su detección en Wazuh. También incluye la respuesta aplicada dentro del laboratorio para contener el evento. Fuente: Elaboración propia.

Figura 14.

Validación del bloqueo desde Kali Linux



Nota. En la figura se observa la prueba de conectividad que se hizo desde Kali Linux hacia el servidor DMZ. Al validar, se nota que el tráfico quedó bloqueado por la regla que se aplicó en pfSense. Fuente: Elaboración propia.

En esta prueba se realizaron varios intentos fallidos de acceso por SSH desde Kali Linux hacia el servidor Ubuntu. Se buscó comprobar si el evento salía primero en los registros del servidor y después en Wazuh, como parte del monitoreo que se configuró en el laboratorio.

Al mirar la alerta, se pudo ver la IP de origen, la regla que se activó y el nivel de severidad que asignó Wazuh. Con esos datos se registró el tiempo de detección, que fue de 9 segundos, como se ve en la Tabla 24. Después se aplicó una regla en pfSense para bloquear el tráfico de la máquina atacante y se validó que el acceso quedara restringido.

La prueba se relaciona con ISO/IEC 27001 porque trabajó el registro, monitoreo y respuesta ante un intento fallido de autenticación. Desde el NIST CSF, se vincula con Detect y Respond, ya que el evento fue observado en Wazuh y luego contenido con una regla en pfSense dentro del laboratorio.

Anexo 11. Postest

11.1 Hardening aplicado

Endurecimiento de SSH

En el servidor Ubuntu se revisó el acceso por SSH, porque este servicio se usaba en las pruebas de autenticación. Para hacerlo más seguro, se quitaron configuraciones débiles y se restringió el

ingreso remoto. También se deshabilitó el acceso directo con root, se limitaron los intentos fallidos y se dejó el ingreso solo para usuarios autorizados. Así, el laboratorio pudo probar un acceso remoto más controlado frente a intentos no autorizados.

```
PermitRootLogin no
MaxAuthTries 3
LoginGraceTime 30
X11Forwarding no
AllowUsers victoria
```

Endurecimiento de Apache: fortalece la seguridad del servidor web, evitando la exposición de información sensible y reduciendo vulnerabilidades. Permite controlar qué servicios, módulos y configuraciones están habilitados para proteger las aplicaciones publicadas.

```
victoria@plataformas:~$ sudo a2enmod headers rewrite
Enabling module headers.
Module rewrite already enabled
To activate the new configuration, you need to run:
  systemctl restart apache2
```

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off

<Directory /var/www/html>
    Options -Indexes
    AllowOverride All
    Require all granted
</Directory>

Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=(), camera=()"
```

Protección básica de WordPress: disminuye riesgos sobre el sitio web, como accesos indebidos, ataques de fuerza bruta, explotación de plugins vulnerables o modificación no autorizada del contenido. Incluye actualizar WordPress, temas y plugins, usar contraseñas seguras, limitar intentos de inicio de sesión y aplicar permisos adecuados.

- Desactivar edición de archivos desde WordPress: Esto reduce el riesgo de modificación directa de archivos desde el panel administrativo.

define('DISALLOW_FILE_EDIT', true);

- Proteger wp-config.php y xmlrpc.php

```
┌──(victoria㉿kali)-[~/posttest_vulnerabilidades]
└─$ curl -I http://192.168.20.10/xmlrpc.php
HTTP/1.1 403 Forbidden
Date: Thu, 30 Apr 2026 02:38:22 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Type: text/html; charset=iso-8859-1
```

- Corregir permisos

```
victoria@plataformas:~$ sudo chown -R www-data:www-data /var/www/html
victoria@plataformas:~$ sudo find /var/www/html -type d -exec chmod 755 {} \;
victoria@plataformas:~$ sudo find /var/www/html -type f -exec chmod 644 {} \;
victoria@plataformas:~$ sudo chmod 600 /var/www/html/wp-config.php
victoria@plataformas:~$
```

- Actualizar WordPress, temas y plugins

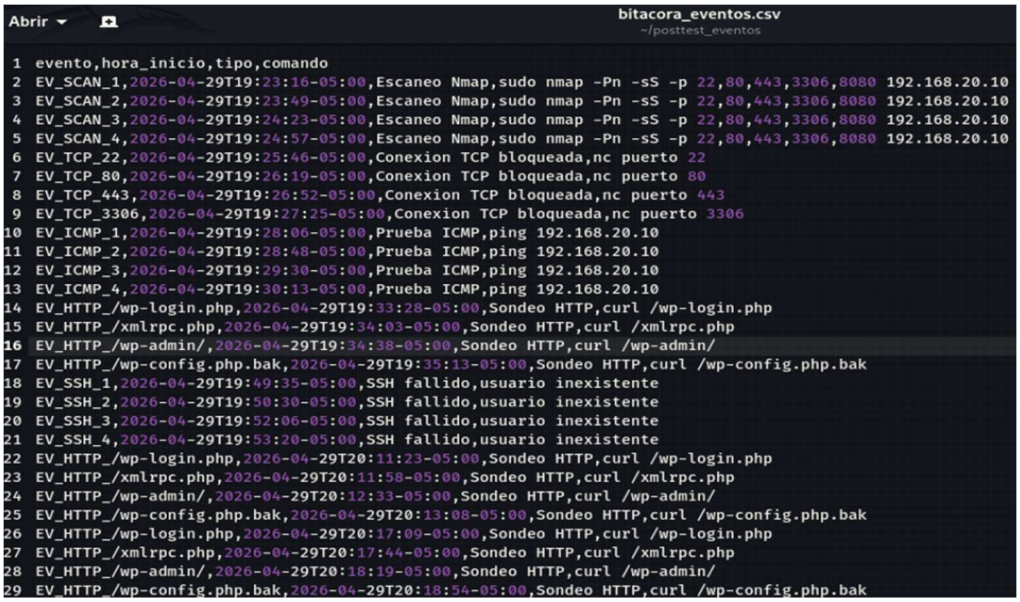
11.2 Reglas pfSense

Creación de reglas en pfsense:

✓	0/242.50 MiB	IPv4 TCP	192.168.30.10	*	192.168.20.10	POSTTEST_ PUERTOS_ WORDPRESS	*	none	POSTTEST_TEMP_ESCANEO_CONTROLADO
✗	0/7 KiB	IPv4 *	192.168.30.10	*	192.168.20.10	*	*	none	Bloquear a kali hacia servidor

Figura 15.

Ejecución postest: generación de eventos



Nota. La figura evidencia la generación de eventos durante la fase postest, posterior a la aplicación de controles de hardening y reglas de seguridad en pfSense. Fuente: Elaboración propia.

11.3 Cálculos MTTD / MTTR

Cálculo de tasa de detección

Evento	Hora inicio	Detectado en Wazuh	Hora alerta	Evidencia
EV_SCAN_1	19:23:16	Sí	19:23:22	Alerta pfSense/Wazuh
EV_SCAN_2	19:23:50	Sí	19:23:56	Alerta pfSense/Wazuh
EV_HTTP_1	19:33:28	Sí	19:33:28	Alerta pfSense/Wazuh
EV_SSH_1	19:49:35	Sí	19:49:39	Regla 5710

$$\text{Tasa de detección } = \frac{\text{eventos detectados}}{\text{eventos simulados}} * 100$$

$$\text{Tasa de detección } = \frac{20}{20} * 100 = 100\%$$

Cálculo del MTTD

$$\text{MTTD} = \text{hora de alerta en Wazuh} - \text{hora de inicio del evento}$$

Evento	Hora inicio	Hora alerta Wazuh	Tiempo de detección
EV_SCAN_1	19:23:16	19:23:22	6 seg.
EV_SCAN_2	19:23:50	19:23:56	6 seg.
EV_HTTP_1	19:33:28	19:33:32	4 seg.
EV_SSH_1	19:49:35	19:49:39	4 seg.

$$MDDT = \frac{(6 + 6 + 4 + 4)}{4} = 5\ seg.$$

Cálculo del MTTR

MTTR = hora de acción de respuesta - hora de alerta

Evento	Hora alerta	Hora acción completada	Tiempo de respuesta
EV_SCAN_1	19:23:22	19:23:24	2 seg.
EV_SCAN_2	19:23:56	19:30:20	6 min 24 s
EV_HTTP_1	19:33:32	19:35:22	1 min 50 s
EV_SSH_1	19:49:39	19:54:35	4 min 56 s

$$MTTR = \frac{(2\text{ s} + 384\text{ s} + 110\text{ s} + 296\text{ s})}{4} = 3\ min.\ 18\ seg.$$

Los resultados del postest permiten evidenciar que la aplicación de controles de hardening, reglas de filtrado en pfSense y monitoreo mediante Wazuh contribuyó a mejorar la capacidad de detección y respuesta ante eventos de seguridad generados en el laboratorio virtual.

Bloque 1: Matriz de Trazabilidad ISO/NIST → Componente del Laboratorio

Control ISO 27001:2022	Control NIST SP 800-53/CSF	Componente del laboratorio	Evidencia de validación
A.8.8 Gestión de vulnerabilidades	ID.AM, PR.IP-1	Kali Linux + Nmap	Tabla 11 Anexo 7
A.8.20/8.22 Seguridad y segregación de redes	SC-7, PR.AC-5	pfSense (LAN/DMZ/Ataque)	Tabla 6 Figura 13 Figura 14
A.5.15/5.16 Control de acceso e identidad	AC-2, AC-6	Ubuntu + WordPress + SSH	Fig. 4-8, Anexo 8
A.8.15/8.16 Registro y monitoreo	DE.CM-1, DE.CM-7	Wazuh SIEM	Tabla 19 Anexo 10
A.5.24/5.26 Respuesta a incidentes	RS.RP-1, RS.MI-1	pfSense + Wazuh	Tabla 20 Anexo 10 Tabla 24

Bloque 2: Declaración Ética y de Privacidad (2 líneas)

La aplicación del cuestionario digital (Anexo 5) se realizó bajo consentimiento informado implícito al acceder al formulario. No se recopilaron datos personales identificables, se garantizó el anonimato y los resultados se presentan únicamente de forma agregada, cumpliendo con los principios de protección de datos establecidos por la normativa institucional vigente.