UACM

Universidad Autónoma de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Auditoria de Seguridad en Redes y Sistemas de una Institución Académica: Evaluación, Mitigación y Mejora Continua

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A

ANA LAURA GARCÍA VICTORINO

D I R E C T O R

M. EN I. OSCAR RENÉ VALDEZ CASILLAS

Ciudad de México, septiembre de 2025.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

INTEGRACION DEL JURADO:

Presidente:

Lic. Jorge Mendoza Zavala, Casa Libertad

Secretario:

Mtro. David Estrada Espinosa, Casa Libertad

Vocal:

M.I. Oscar Rene Valdez Casillas, Casa Libertad

Plantel de adscripción: Casa Libertad

DIRECTOR DE TESIS.

M. en I. Oscar Rene Valdez Casillas

UACM, Plantel Casa Libertad.

Agradecimientos.

Mi más profundo agradecimiento a mi director de tesis Oscar Rene Valdez Casillas no solo por su conocimiento y orientación, sino también por su confianza en mí, por tenerme paciencia, alentarme y aconsejarme cuando lo necesitaba, sin su guía esto no habría sido posible.

Agradezco por su dedicación, tiempo, contribuciones y guía durante la realización de mi tesis y en cada etapa de este camino a mis 3 lectores Dra. Tejinder Kaur, M. en I. David Estrada Espinosa y Lic. Jorge Mendoza Zavala.

Le agradezco a mi madre Blanca Estela Victorino Mendoza sin tu apoyo, palabras de aliento, amor y enseñanza esto no seria posible, gracias por ser mi sostén cuando caía y dudaba, por mantenerte fuerte a mi lado, este logro es mas tuyo que mío.

Le agradezco a mi padre y ángel Víctor Hugo Hernández Pérez, fuiste mi fuente de inspiración, para siquiera soñarlo y hoy es una realidad, sin tu ejemplo, apoyo y amor no hubiera podido soñarlo y lograrlo, me diste los mejores consejos y ejemplos de vida para mantenerme fuerte y lograr mis metas y aunque hoy no estarás para presenciarlo hoy te digo, lo logramos.

A mi hermana, mi mas grande amor Diana Caren García Victorino, no hay palabras que puedan expresar lo agradecida que estoy contigo por tu apoyo, confianza, amor, consejos y palabras, gracias por creer en mi durante todo este camino, porque hubo veces que tu creíste mas en mi y en que esto era posible que yo misma ¡gracias!

A mi amada casa de estudios UACM por la oportunidad que me brindo y la gran experiencia que fue ser parte de ella.

Resumen.

La realización de auditorías a instituciones académicas es de suma importancia ya que mediante estas se puede comprobar la seguridad en la información que tienen las instituciones.

Los sistemas de dichas instituciones deben de cumplir con ciertas normativas y estándares de seguridad, los cuales son: NIST cibersecurity framework, OSI/IEC 27001, para complementar las medidas de seguridad se pueden implementar CIS controls y OWASP TOP 10.

La auditoría realizada será una auditoria informática interna, esta será realizada a la red interna, con dirección IP 172.18.12.70 y al servidor de informática dentro de las instalaciones del laboratorio de telecomunicaciones con dirección IP 192.168.1.1

Los softwares utilizados para la realización del escaneo fueron SCUBA de Imperva, Namp, Zenmap y OWASP.

Al realizar los escaneos se obtuvo un total de 31 vulnerabilidades, esto indica que se debe de mejorar el esta de seguridad del sistema, por esto se proponen diferentes medidas a implementar para la mejora de este.

ÍNDICE

OBJETIVOS DEL TRABAJO.

General: Evaluar y mejorar la seguridad en la infraestructura del laboratorio de telecomunicaciones.

Específicos:

- Identificar vulnerabilidades en redes y sistemas.
- Proponer medidas de mitigación basadas en estándares internacionales.
- Desarrollar un plan de mejora continua.

CAPITULO 1.

1. Introducción.

Las auditorías realizadas a instituciones académicas son de suma importancia, ya que mediante esta se puede comprobar la seguridad de la información en dichas instituciones.

Para entender más acerca de lo que abarca realizar una auditoría a instituciones, es necesario abarcar ciertos conceptos y normativas que son necesarias para verificar la seguridad de la información.

Lo primero a tomar en cuenta es la base que se debe tener para la protección de la información, confidencialidad, integridad y disponibilidad, ya que si se cumple con estas bases se puede decir que es un sistema efectivo.

La finalidad de este presente trabajo es hacer referencia a la importancia de la seguridad de la información en instituciones académicas, en este caso en un servidor de informática en las instalaciones del laboratorio de telecomunicaciones y como mediante una auditoria con los resultados que esta nos dé se pueden proponer medidas para la protección de datos y la continuidad operativa.

1.1. Contexto y justificación.

La principal función de la auditoria para la protección de datos es verificar si se cumple con la norma ISO (Organización Internacional de Normalización) 27001 y NIST Cybersecurity framework (Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología), así como las vulnerabilidades que puede tener el sistema.

Para poder cerciorarse de la seguridad aplicada a la protección de datos es necesario realizar auditorías periódicamente, la auditoria no solo nos ayudara a verificar que los datos están protegidos, sino que también haya continuidad operativa, también mediante estas se podrá evaluar que se cumpla con las leyes y regulaciones adecuadas para la protección de datos.

1.2. Alcance y limitaciones.

La auditoría que se estará realizando es una auditoria informática interna, la cual será a la red interna, con dirección IP 172.18.12.70 y al servidor de informática dentro de las instalaciones del laboratorio de telecomunicaciones con dirección IP 192.168.1.1

Lo que se realizara durante dicha auditoria es un escaneo a las direcciones ya mencionadas, generando los informes, en el cual se indicaran las vulnerabilidades y lo críticas que estas son, así como también las sugerencias para evitar la presencia de dichas vulnerabilidades.

CAPITULO 2.

2. Marco teórico.

2.1. Fundamentos de seguridad de la información.

Los conceptos básicos para comprender la seguridad de la información son confidencialidad, integridad y disponibilidad, esto ya que cuando se tiene alguna vulnerabilidad o amenaza tienden a atacar estos tres elementos.

Confidencialidad: el acceso a la información y recursos del sistema solo pueden ser leídos y utilizados por los usuarios autorizados.

Integridad: comprueba que la información y los recursos no fueron alterados por usuarios no autorizados.

Disponibilidad: la información puede ser utilizada en cualquier momento con la certeza de que esta no se perderá o bloqueará.

Una amenaza son las acciones que se realizan para sacar provecho de las vulnerabilidades que puede tener un sistema, las amenazas se pueden realizar sin necesariamente comprometer la seguridad del sistema.

Las amenazas se pueden clasificar en:

- Intencionales: se realizan con la intención de causar un daño.
- No intencionales: no buscan sacar provecho de las vulnerabilidades, sin embargo, pueden o no comprometer la seguridad.

Una vulnerabilidad consiste en un fallo y esta compromete la seguridad de la información en el que el usuario no autorizado puede dañar o comprometer la información del sistema.
Las vulnerabilidades se pueden consultar en NVD (National Vulnerability Database) ya que es donde se lleva el registro de las vulnerabilidades. Se emplea el estándar CVE (Common Vulnerabilities and Exposures) esto para facilitar el intercambio de información entre las diferentes bases de datos. [1]

Los tipos de vulnerabilidades más comunes son:

- Pérdida de control de acceso.
- Fallos criptográficos.
- Inyección.
- Diseño inseguro.
- Configuración de seguridad defectuosa.
- Componentes vulnerables y obsoletos.
- Fallos de identificación y autentificación.
- Fallos en el software y en la integridad de los datos.
- Fallos en el registro y la supervisión de la seguridad.
- Falsificación de solicitud del lado del servidor.

2.2. Normativas y Estándares de seguridad.

Las normativas y estándares de seguridad que se recomienda que cumplan las instituciones académicas para garantizar la seguridad de la información son: ISO/IEC 27001, NIST Cybersecurity Framework, CIS (Centro para la seguridad de Internet) Controls y OWASP Top y se describen a continuación.

ISO/IEC 27001.

La norma ISO/IEC 27001 se puede aplicar en cualquier empresa, ya que su aplicación es amplia.

Es una norma internacional la cual proporciona los controles y evaluaciones a realizar para los sistemas de gestión de la seguridad de información (SGSI).

El objetivo del SGSI es que las empresas puedan conservar su confidencialidad e integridad, como también su disponibilidad de la información y los activos de dicha información.

Un SGSI se implementa porque proporciona el marco de referencia que va a permitir tener una gestión de los riesgos, es decir, identificar y evaluar los posibles riesgos que puede haber sobre la seguridad de información.

Para establecer un SGSI se debe tener un proceso el cual según la norma ISO 27001se utiliza el modelo PDCA (Planear – Hacer – Chequear - Actuar). Los principales requisitos para implementar el SGSI son [2]:

- Comprender los requerimientos de seguridad de la información del sistema/organización, así como la política y objetivos para garantizar la seguridad de la información.
- Uso de los controles necesarios para identificar y dirigir los riesgos de la información.
- Monitoreo de la SGSI y su funcionamiento.

La norma ISO 27001 cuenta con controles, los controles son los encargados de los procesos y procedimientos necesarios para contrarrestar los riesgos a los que pueda estar expuesto el sistema, esto con el fin de garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información de dicho sistema.

Dicha norma cuenta con 114 controles de seguridad y están divididos en 14 secciones [3]:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Controles de acceso.
- Criptografía – cifrado y gestión de claves.
- Seguridad física y ambiental.
- Seguridad operacional.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento del sistema.

- Gestión de incidentes de seguridad de la información,
- Cumplimiento.

NIST Cybersecurity Framework.

El marco de ciberseguridad del NIST es publicado por el Instituto Nacional de Estándares y Tecnología (NIST), dicho marco puede ser aplicado a empresas de cualquier tamaño, organización o sistema, ya que se puede adaptar a los requerimientos de seguridad de la información de estos.

Sin embargo, este marco se debe complementar con más herramientas para garantizar la seguridad de la información.

El enfoque que se le dará al marco dependerá específicamente de los riegos, amenazas y vulnerabilidades en el sistema.

Las funciones centrales de NIST CSF son: gobernar, identificar, proteger, detectar, responder y recuperar [4].

- Gobernar (GV): esta función nos indica los resultados de las otras cinco funciones, estos resultados se dependerán de las especificaciones que son requeridas para el sistema en el que se aplican, con estos resultados se podrán proponer estrategias para la gestión de riesgos.
  La gobernanza analiza el contexto de la organización tomando en cuenta todas las cuestiones del entorno del sistema.
- Identificar (ID): se identifican los riesgos existentes actuales en el sistema; así como los activos y recursos del sistema; con dicha función se identifican las políticas, procesos, etc., manejando en conjunto las 6 funciones poder brindar una apropiada gestión de riesgos los activos tanto en hardware como en software.
- Proteger (PR): dicha función en primera instancia identificará los activos, en base a esto, se encargará de la seguridad a estos, brindando una protección adecuada tanto al hardware como al software.
- Detectar (DE): Implementa acciones de monitoreo para detectar y analizar posibles ataques y vulnerabilidades, al detectar a tiempo se puede proponer de manera oportuna una respuesta a estos incidentes.
- Responder (RS): se toman las medidas apropiadas para responder a los incidentes y poderlos contener, para que esto se lleve a cabo es necesario contar con una gestión de respuesta, análisis, mitigación, mejoras y comunicación de los incidentes.
- Recuperar (RC): si ya se tuvieron los incidentes esta función se encargará de la recuperación y de los activos afectados, para que estos se restablezcan con normalidad.

Fig. 1. Marco de Seguridad Cibernética del NIST [4].

La gobernanza es la que se encarga de informar cómo están implementadas las demás funciones, las otras 5 funciones trabajan simultáneamente.

Todas las funciones en conjunto nos indicaran como será el ciclo de vida del proceso de gestión de riesgos.

La flexibilidad que nos da este marco permite que se pueda tener una conexión con las funciones de otros marcos.

CIS controls: controles críticos aplicables.

Para poder explicar lo que son los CIS controls, es necesario entender lo que es un control.

Los controles son las medidas de seguridad que se implementan para proteger la información, estos controles pueden ser físicos o de información.

Los controles críticos de seguridad CIS son el conjunto de acciones que priorizan y simplifican las mejoras que puede haber en estrategias de ciberseguridad, dichas prácticas son para la mitigación de ataques en sistemas.

Se busca proteger el sistema antes de que se den los ataques, si no también cuando ya fueron atacadas, con el fin de poder ser mitigados estos ataques.

Está estructurado con 20 controles CIS los cuales se dividen en sub - controles [5]:

1. CIS control 1: Inventario de Dispositivos autorizados y no autorizados, cuenta 8 sub - controles.
2. CIS control 2: Inventario de software autorizado y no autorizado, cuenta con 10 sub - controles.
3. CIS control 3: Gestión continúa de vulnerabilidades, cuenta con 7 sub - controles.
4. CIS control 4: Uso controlado de privilegios administrativos cuenta con 9 sub - controles.

5. CIS control 5: Configuración segura para hardware y software en dispositivos móviles, computadores portátiles, estaciones de trabajo y servidores, cuenta con 5 sub – controles.
6. CIS control 6: Mantenimiento, monitoreo y análisis de logs de auditoría, cuenta con 8 sub – controles.
7. CIS control 7: Protección de correo electrónico y navegador web, cuenta con 10 sub – controles.
8. CIS control 8: Defensa contra malware, cuenta con 8 sub – controles.
9. CIS control 9: Limitación y control de puertos de red, protocolos y servicios, cuenta con 5 sub – controles.
10. CIS control 10: Capacidad de recuperación de datos, cuenta con 5 sub – controles.
11. CIS control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores, cuenta con 7 sub – controles.
12. CIS control 12: Defensa de borde, cuenta con 12 sub – controles.
13. CIS control 13: Protección de datos, cuenta con 9 sub – controles.
14. CIS control 14: Control de acceso basado en la necesidad de conocer, cuenta con 9 sub – controles.
15. CIS control 15: Control de acceso inalámbrico, cuenta con 10 sub – controles.
16. CIS control 16: Monitoreo y control de cuentas, cuenta con 13 sub – controles.
17. CIS control 17: Implementar un programa de concienciación en seguridad, cuenta con 9 sub – controles.
18. CIS control 18: Seguridad del software de aplicación, cuenta con 11 sub – controles.
19. CIS control 19: Respuesta y gestión de incidentes, cuenta con 9 sub – controles.
20. CIS control 20: pruebas de penetración y ejercicios de Equipo rojo, cuenta con 8 sub – controles.

OWASP Top 10: principales vulnerabilidades en aplicaciones web.

OWASP (Open Web Application Security) es una metodología la cual tiene como objetivo la seguridad de aplicaciones web, esta nos proporciona herramientas y documentaciones sobre la seguridad de las aplicaciones, es por esto que OWASP es utilizado como marco de referencia en auditorias de seguridad.

OWASP TOP 10 es una lista la cual se actualiza regularmente en la cual están los 10 riesgos de seguridad más críticos en aplicaciones web, dichos riesgos están principalmente orientados a los datos [6].

1. A01 – Pérdida de Control de Acceso.
2. A02 – Fallas Criptográficas.
3. A03 – Inyección.
4. A04 – Diseño Inseguro.
5. A05 – Configuración de Seguridad Incorrecta.
6. A06 – Componentes Vulnerables y Desactualizados.
7. A07 – Fallas de Identificación y Autenticación.
8. A08 – Fallas en el Software y en la Integridad de los Datos.
9. A09 – Fallas en el Registro y Monitoreo.
10. A10 – Falsificación de Solicitudes del Lado del Servidor.

2.3. Auditoria de seguridad.

Una auditoria se encarga de examinar y evaluar que la empresa funcione de una manera eficiente, se pueden tener varios puntos a considerar para decir que la auditoria se llevó a cabo de forma correcta algunos de ellos son: integridad, confidencialidad, independencia. Existen diferentes tipos de auditorías las cuales son [7]:

1. Interna: son realizadas por la empresa, tienen como finalidad identificar si está funcionando de manera correcta el sistema y que se cumplan con las normas que se deben aplicar en esta.
2. Externa: es realizada por personas externas a la empresa, generalmente se realiza para mostrar su buen funcionamiento y que cumplan con los requisitos que requieran subcontratistas o proveedores.
3. Informática: se encarga de recoger, agrupar y evaluar evidencias con las que determina si un sistema de información protege adecuadamente la integridad de los datos del sistema. [8]

Las auditorias se realizan con la finalidad de identificar si el sistema está funcionando de forma adecuada, esto reuniendo evidencia e información para identificar si se tiene fallas y se realicen observaciones para mejorar. Se puede auditar el funcionamiento de los sistemas informáticos y su entorno esto para prevenir ciberataques o que haya desvío de información, así como también se puede auditar los procesos informáticos y las normatividades vigentes.

Al realizar la auditoria el auditor se encargará de la recolección y análisis de datos, para esto deberá emplear una metodología de acuerdo a los objetivos y normativas que se deben de cumplir, no existe una metodología ya estructurada que se deba de seguir, esta se modifica de acuerdo a los requerimientos de la empresa que la solicita.

De manera general se tiene las siguientes etapas para llevar a cabo la auditoria [9]:

- Planificación de la auditoria.
- Ejecución de la auditoria.
- Elaboración de informes y recomendaciones.
- Seguimiento.

La auditoría se puede enfocar basada en los riesgos, en dado caso, se necesita identificar, analizar y evaluar las vulnerabilidades que se pueden tener en el sistema auditado.

Al contar con dicha información es posible realizar una matriz de riego en la cual se identifica que tan críticos son estos, teniendo los datos ya establecidos, serán la base para que se cree una metodología de auditoría.

CAPITULO 3.

3. Metodología.

3.1. Planificación de la auditoria.

Objetivos específicos de la auditoria.

- Definir y delimitar el sistema a auditar y los recursos necesarios para llevar la auditoria de manera eficiente.
- Identificar las amenazas y vulnerabilidades encontradas en el sistema.
- Identificar que tan riesgosos son los resultados obtenidos.
- Proponer las posibles mitigaciones a las amenazas y vulnerabilidades encontradas.

Sistemas y redes a auditar.

La red a auditar será la red con dirección IP 172.18.12.70, así como el servidor de informática que se encuentra dentro de las instalaciones de la UACM con dirección IP 192.168.1.1

3.2. Fases de la auditoria.

TABLA I.

Calendario De La Auditoria.

ACTIVIDAD	DURACIÓN
Preparación de la auditoria.	4 días.
Determinación de recursos y tiempo.	2 días.
Recopilación de información básica.	4 días.
Realización de auditoría.	14 días.
Realización de pruebas y obtención de resultados.	14 días.
Conclusión y comentarios.	7 días.
Redacción de informe de auditoría.	7 días.
Emisión y distribución del informe de auditoría.	1 día.
Audiencia del informe de auditoría.	3 días.

Nota. Es el calendario a seguir para la realización de la auditoria.

Actividades a realizar / evaluar durante la auditoria:

- Evaluación de contenido.
- Análisis de enlaces.
- Análisis de seguridad del sitio web.

3.3. Análisis de cumplimiento.

Al realizar un análisis de cumplimiento se revisa que los resultados obtenidos cumplan con las normativas y estándares aplicables vigentes, así como también se analiza que los objetivos de seguridad se estén cumpliendo.

La normativa específica es la norma ISO 27001, el estándar NIST Cybersecurity y se apliquen los controles adecuados de CIS controls.

Para poder llevar a cabo el análisis se siguen una serie de análisis de documentación que incluye la revisión de documentación, revisión de pruebas, se analizan los resultados obtenidos en las pruebas, análisis de informes técnicos y las recomendaciones que este nos indique.

Se analizan también las áreas de no conformidad, es decir todas aquellas áreas que no cumplan con la seguridad especificada en la auditoria, tomando en consideración que no se cuenta con un manual o serie de reglas que se deban de cumplir.

CAPITULO 4.

4. Desarrollo de auditoría.

4.1. Determinación de recursos y herramientas.

El escáner de vulnerabilidades se encarga de realizar un monitoreo de las amenazas y vulnerabilidades que pueda tener en el sistema. Es importante realizar el escaneo todos los días, ya que diariamente se descubren nuevas vulnerabilidades y así se puedan implementar medidas de seguridad para no ser afectadas por estas.

El escáner facilita el monitoreo de las vulnerabilidades ya que realizar este monitoreo de manera manual llevaría más tiempo.

El proceso que se realiza para el escaneo de vulnerabilidades es:

- Identificación de vulnerabilidades.
- Identificación de valoraciones de riesgos.
- Tratamiento de vulnerabilidades identificadas.
- Informe de vulnerabilidades.

Se pueden realizar diferentes tipos de escaneos, algunos de ellos son:

- Escaneo externo.
- Escaneo interno.
- Escaneo de vulnerabilidades autenticadas.
- Escaneo de vulnerabilidades no autenticadas.

A continuación, se describirán las herramientas utilizadas en el desarrollo de la auditoria.

1. Nmap.

Nmap es una herramienta de código abierto la cual es utilizada para el escaneo de direcciones IP, puertos en una red y aplicaciones instaladas. [10]

Fue diseñada para escanear redes grandes, pero también hosts individuales. Nmap hace uso de paquetes IP, para poder determinar los hosts disponibles en la red, así como los servicios ofrecidos por este, sistemas operativos en ejecución, tipos de firewall en uso, etc.

Nmap puede ser ejecutada en diferentes sistemas operativos, los cuales son: Linux, Windows y Mac OSX, etc.

Con Nmap se pueden realizar diferentes tipos de escaneos, el escaneo básico es el que se realiza durante el proceso de la auditoria.

- Escaneo básico: Escanea dispositivos y puertos de una red, comienza realizando un mapeo de la red, esto se puede realizar haciendo un escaneo Ping el cual escanea los dispositivos en una subred, o se puede realizar mediante el escaneo en un solo host y este es un solo host con diferentes puertos conocidos. [11]

Y hay otros tipos de escaneos posibles:

- Escaneo sigiloso.
- Escaneo de versiones.
- Escaneo del sistema operativo.
- Escaneo agresivo.
- Escaneo de varios hosts.
- Escaneo de puertos.
- Escaneo desde un archivo.

2. Zenmap

Nmap tiene un interfaz llamado Zenmap que nos da un visor de resultados. El uso de Zenmap ayuda a que los datos se muestren de una manera más clara y organizada, ya que facilita la visualización de los datos recopilados. [12]

Algunas de las funciones de Zenmap es el escaneo de puertos, hosts y los sistemas en una red, así como servicios y protocolos utilizados en estos, también detecta vulnerabilidades en los dispositivos y en la red; al obtener todos estos datos genera un informe con los resultados del escaneo.

3. SCUBA.

SCUBA de Imperva, es una herramienta gratuita, se encarga de escanear las bases de datos de una empresa, esto para encontrar vulnerabilidades y fallas de configuración, mostrando los resultados en un panel gráfico, así como también proporciona recomendaciones en forma de informes para así realizar acciones inmediatas. [13]

Algunas de las acciones que puede realizar son:

- Realizar el escaneo de base de datos empresariales para encontrar vulnerabilidades y fallas de configuración.
- Determinar las bases de datos que tienen riesgos.
- Recomendaciones para mitigar los riesgos.
- La implementación de las mitigaciones queda al criterio de los administradores de los servidores.

Este escáner se puede utilizar en Microsoft Windows, Apple MacOS, Linux (x32), y Linux (x64); también ofrece más de 2300 pruebas de evaluación para Oracle, Microsoft SQL server, SAP Sybase, IBM DB2, PostgreSQL, Informix y MySQL. [14]

4. OWASP.

OWASP (proyecto abierto de seguridad de aplicaciones web) es una organización de código abierto y sin fines de lucro, que está enfocada en la seguridad de las aplicaciones web. OWASP ofrece diferentes recursos, herramientas y documentaciones gratuitas y accesibles en su página

oficial, con el fin de identificar los riesgos y vulnerabilidades en aplicaciones web, así como su mitigación.

Los recursos que ofrece OWASP son [15]:

- OWASP Top 10.
- Guía de prueba de OWASP.
- Serie de trucos de OWASP.
- Herramientas de prueba.
- OWASP API Security Top 10.
- Recursos de capacitación.

Las herramientas que se utilizaran durante el proceso de la auditoria se eligieron por las técnicas que manejan, además del enfoque que tiene cada una de ellas, Scuba se utilizara para realizar el escaneo a la base de datos, por su lado para el escaneo del servidor se ocupara Zenmap de Nmap y OWASP además de que OWASP Top 10 nos da el marco de referencia de las vulnerabilidades más comunes en aplicaciones web y en conjunto con CWE las descripciones de dichas vulnerabilidades y las posibles mitigaciones.

Modo de ejecución de las herramientas utilizadas.

- Nmap.

Se esta ejecutando Nmap para realización de escaneo de la red.

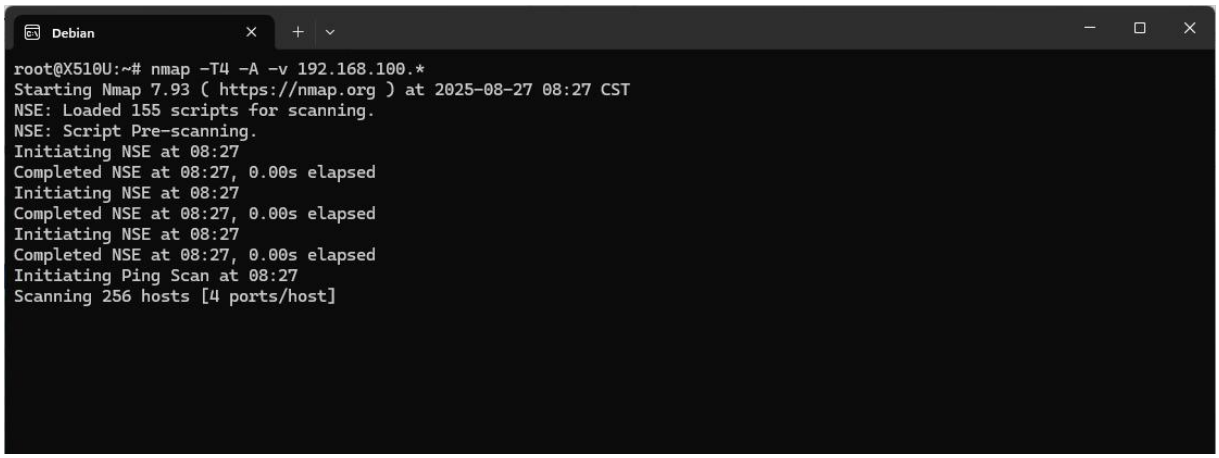


Fig. 2. Escaneo Nmap.

Esta ventana nos indica los puertos activos e inactivos que se encontraron al realizar el escaneo de la red.

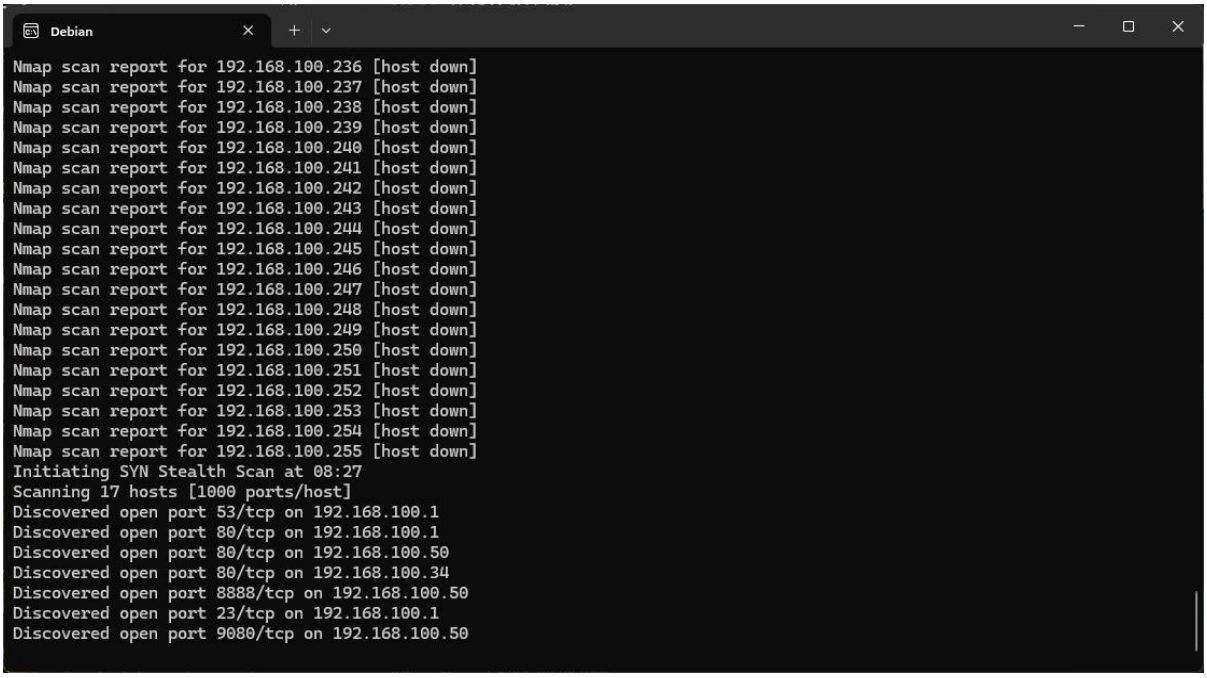


Figura 3. Resultado Nmap.

Para el caso de Nmap en la terminal no se aprecia la información separada, esto por como esta diseñado el software, pero nos arroja un reporte general.

- Zenmap.

En esta ventana se comenzó el escaneo de los puertos para determinar cuales están abiertos.

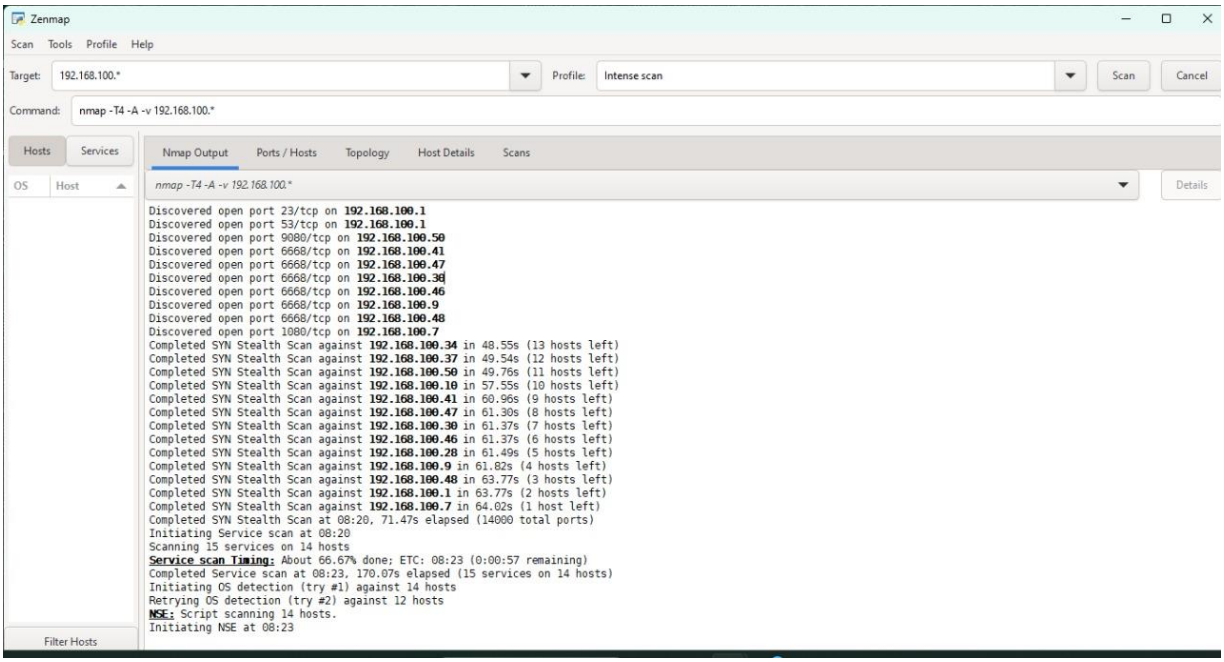


Fig. 4. Escaneo Zenmap.

En esta figura ya se obtuvo el resultado de los puertos que están activos, y con este resultado se da paso a realizar el escaneo de cada uno de los puertos para el proceso de la auditoria.

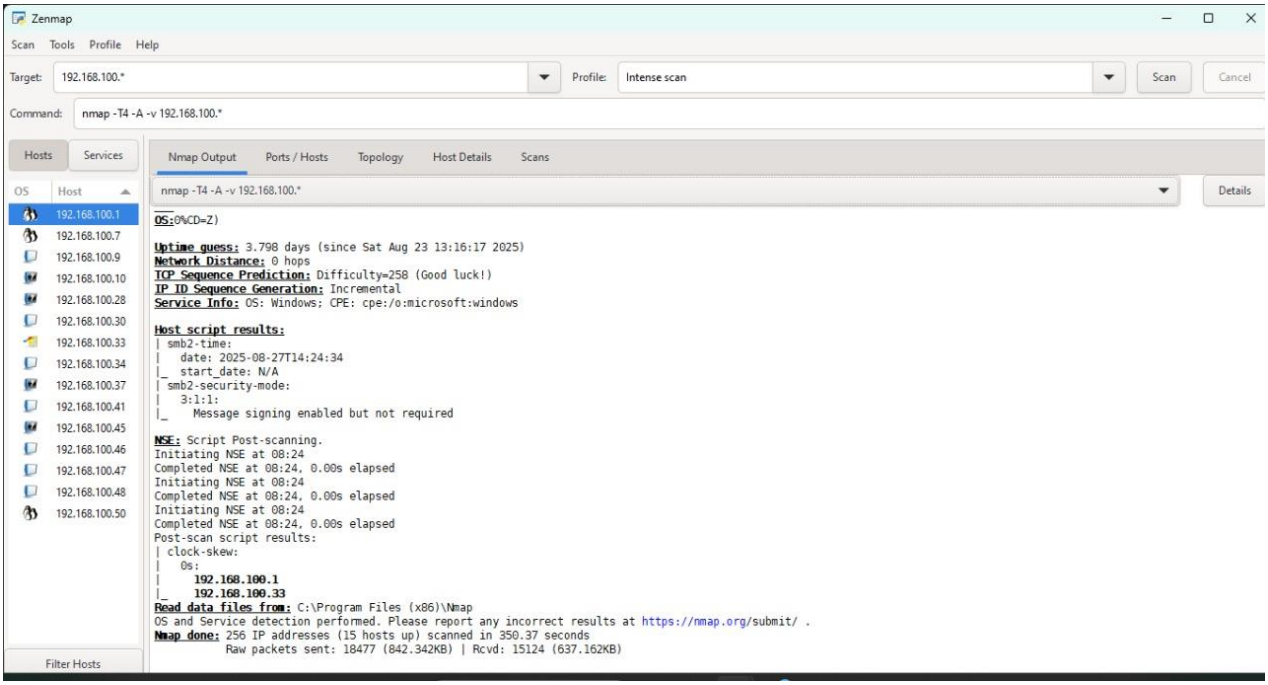


Fig. 5. Resultado Zenmap.

- SCUBA.

En la siguiente figura se mostrará el panel de control de SCUBA de Imperva, esta muestra de manera general el estado de seguridad en el que se encuentra la base de datos después de ser escaneada.

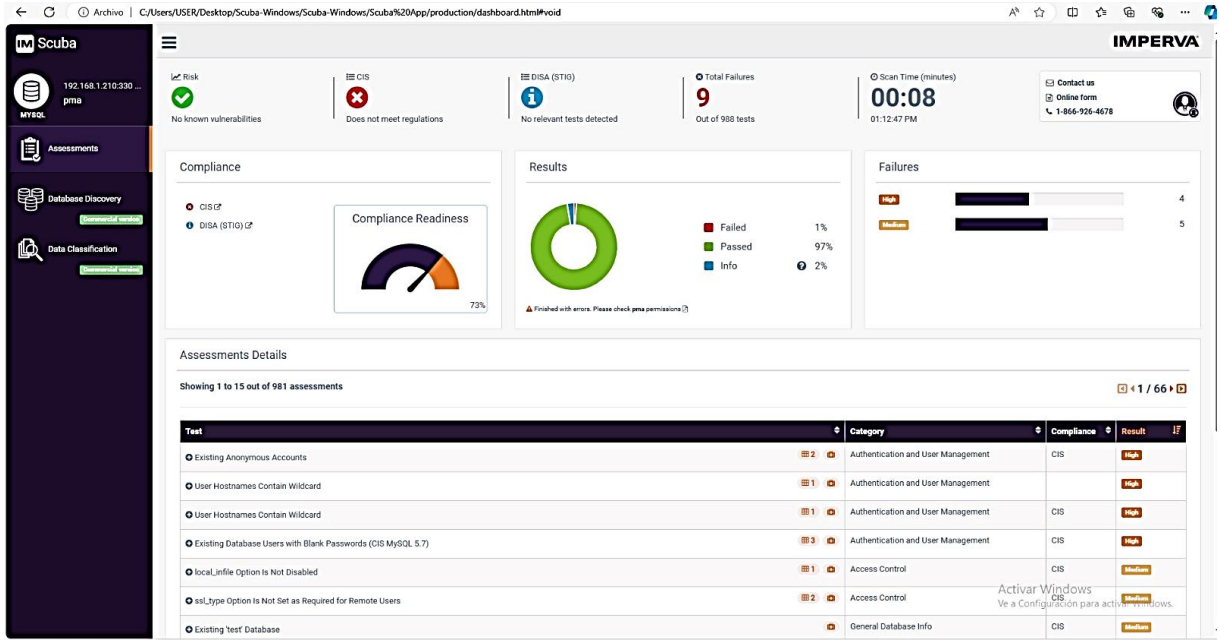


Fig. 6. SCUBA.

4.2. Topología encontrada.

Algunos de los datos recopilados para llevar a cabo el proceso de la auditoria son:

- *Enumeración de puertos.*

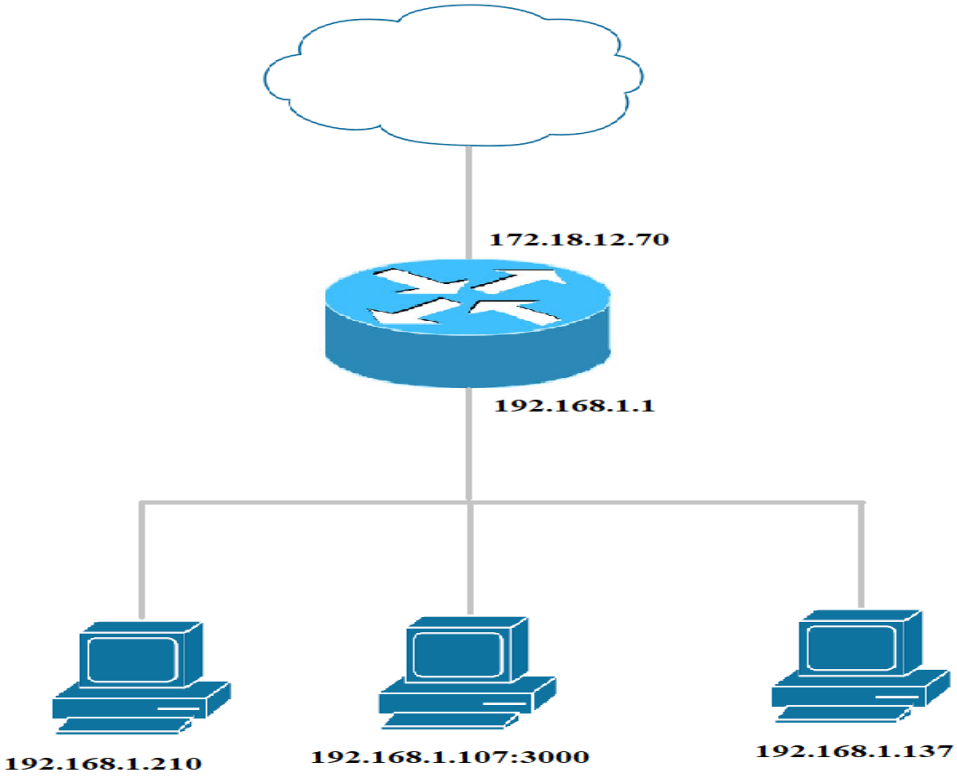


Fig. 7. Topología.

1) 172.18.12.70:80 → recibió el código de respuesta 401.
2) 172.18.12.70:3000
3) 172.18.12.70:8082 → recibió el código de respuesta 401.
4) 172.18.12.70:8085 → recibió el código de respuesta 401.
5) 172.18.12.70:8086 → recibió el código de respuesta 401.
6) 192.168.1.210
7) 192.168.1.107:3000
8) 192.168.1.137
9) 192.168.1.137:8080 → recibió el código de respuesta 401.
10) 192..168.1.120:8086 → recibió el código de respuesta 401.
11) 192.168.1.118 → fallo: conexión rechazada
12) 192.168.1.107 → fallo: conexión rechazada
13) 192.168.1.1 → recibió el código de respuesta 401.

- *Recopilación de vulnerabilidades en servidores y bases de datos.*

Las vulnerabilidades más comunes que se pueden encontrar en el los servidores web durante el proceso de una auditoria son:

- Errores de implementación.
- Problemas de contraseña.
- Ataques de inyección SQL.
- Parches de seguridad faltantes.
- Ataques de denegación de servicios (DDOS).
- Datos sin cifrar.
- Desbordamientos de buffer.
- Errores de configuración.
- Errores en la gestión y asignación de permisos.
- Componentes vulnerables y obsoletos.
- Pérdida de control de acceso.

4.3. Obtención de resultados.

Los resultados obtenidos al realizar las pruebas a las diferentes direcciones IP son los siguientes:

Servidor de informática en las instalaciones del laboratorio de telecomunicaciones.

Sitio 192.168.1.210

- Falsificación de solicitud entre sitios.
- Falla del mecanismo de protección.
- Restricción inadecuada de capas.
- Archivo oculto encontrado.
- Exposición de información confidencial a un autor no autorizado.
- Falla del mecanismo de protección.
- Obtener publicación.
- Validación de entrada incorrecta.

Sitio 192.168.1.107:3000 y 172.18.17.70:3000, tienen las mismas vulnerabilidades ya que sus puertos están redirigidos.

- Falla del mecanismo de protección.
- Archivo oculto encontrado.
- Exposición de información confidencial a un autor no autorizado.
- Falla del mecanismo de protección.
- Exposición de información confidencial a un autor no autorizado.

Sitio 192.168.1.137

- Falla del mecanismo de protección.
- Restricción inadecuada de capas.
- Exposición de información confidencial a un autor no autorizado.
- Falla del mecanismo de protección.

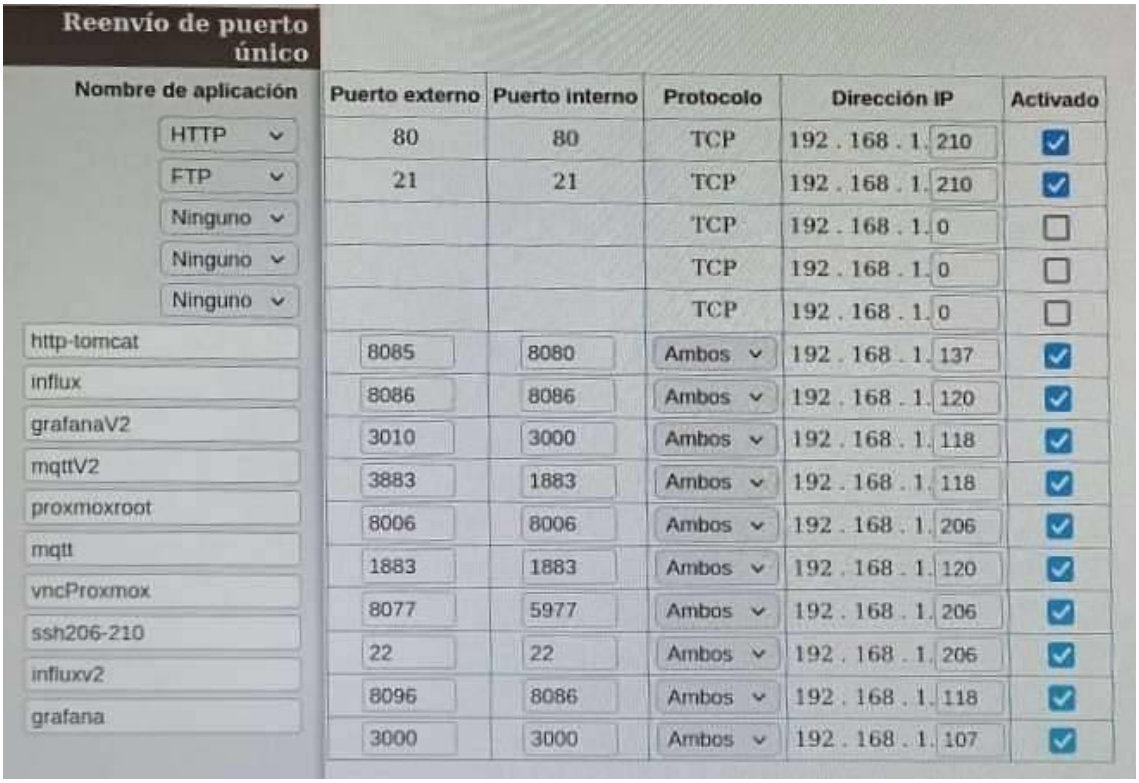
Escaneo con SCUBA.

Sitio 192.168.1.210

- Cuentas anónimas existentes.
- Los nombres de host de los usuarios contienen comodines.
- Los nombres de host de los usuarios contienen comodines.
- Usuario de base de datos existentes con contraseñas en blanco (CIS MySQL 5.7).
- La opción de archivo local no está deshabilitada.
- SSL_TYPE la opción no está configurada como necesaria para usuarios remotos.
- Base de datos de prueba existente.
- Contraseña predeterminada, la opción lifetime esta deshabilitada o configurada en 91 o superior.
- La opción de modo sql no está establecido en 'ESTRICTO TODAS LAS TABLAS'

4.4. Redireccionamiento de puertos.

A continuación, se mostrará una imagen la cual se tuvo acceso al router y en esta se puede observar el direccionamiento de los puertos.



Reenvío de puerto único

Nombre de aplicación	Puerto externo	Puerto interno	Protocolo	Dirección IP	Activado
HTTP	80	80	TCP	192 . 168 . 1. 210	☑
FTP	21	21	TCP	192 . 168 . 1. 210	☑
Ninguno			TCP	192 . 168 . 1. 0	☐
Ninguno			TCP	192 . 168 . 1. 0	☐
Ninguno			TCP	192 . 168 . 1. 0	☐
http-tomcat	8085	8080	Ambos	192 . 168 . 1. 137	☑
influx	8086	8086	Ambos	192 . 168 . 1. 120	☑
grafanaV2	3010	3000	Ambos	192 . 168 . 1. 118	☑
mqttV2	3883	1883	Ambos	192 . 168 . 1. 118	☑
proxmoxroot	8006	8006	Ambos	192 . 168 . 1. 206	☑
mqtt	1883	1883	Ambos	192 . 168 . 1. 120	☑
vncProxmox	8077	5977	Ambos	192 . 168 . 1. 206	☑
ssh206-210	22	22	Ambos	192 . 168 . 1. 206	☑
influxv2	8096	8086	Ambos	192 . 168 . 1. 118	☑
grafana	3000	3000	Ambos	192 . 168 . 1. 107	☑

Fig. 8. Configuraciones.

El puerto 192.168.1.107: 3000 y el puerto 172.18.12.70: 3000 al estar ambos redirigidos en su puerto interno 3000 nos mostraran las mismas vulnerabilidades, y es por este que en ambos casos se propondrán las mismas medidas de mitigación, las cuales se aplicaran dependiendo de los controles en los que sean necesarios.

CAPITULO 5.

5. Propuestas de mitigación.

5.1. Priorización de vulnerabilidades.

Los niveles de riesgo que se encontraron son de criticidad [16]:

- Alto: indica que la probabilidad de que las vulnerabilidades sean explotadas es alta y puede que al ser explotadas los beneficios obtenidos sean altos o que haya una gran pérdida de datos.
- Medio: indica que la probabilidad de que las vulnerabilidades sean explotadas es moderada y para que estas puedan ser explotadas debe de encontrarse en la red local del usuario afectado o su acceso es muy limitado.
- Bajo: las vulnerabilidades que se pueden explotar son de bajo impacto o son problemas de configuración en el sistema y para que las vulnerabilidades sean explotadas necesitan acceso local o físico al sistema.
- Informativo: estas no son consideradas un riesgo solo nos indica alguna información que puede ser necesaria para mejorar la seguridad del sistema.

Las vulnerabilidades se clasificaron dependiendo del nivel de riesgo en el que se encontraron.

Clasificación de las vulnerabilidades encontradas según su criticidad.

TABLA II.

Clasificación De Vulnerabilidades 192.168.1.210.

TIPO DE ALERTA	SITIO: 192.168.1.210			
	Alto	Medio	Bajo	Informativo
Falsificación de solicitud entre sitios (CSRF)		X		
Falla del mecanismo de protección		X		
Restricción inadecuada de capas		X		
Archivo oculto encontrado		X		
Exposición de información confidencial a un autor no autorizado			X	
Falla del mecanismo de protección			X	
Obtener publicación				X
Validación de entrada incorrecto.				X

Nota. Se clasificaron las vulnerabilidades encontradas durante el escaneo y su grado critico en el que se encontraron.

Al estar los puertos redirigidos se encuentran las mismas vulnerabilidades tanto para la dirección 192.168.1.107:3000 y 172.18.12.70:3000

TABLA III.

Clasificación De Vulnerabilidades 192.168.1.107:3000 Y 172.18.12.70:3000

TIPO DE ALERTA	SITIO: 192.168.1.107:3000; 172.18.12.70:3000			
	ALTO	MEDIO	BAJO	INFORMATIVO
Falla del mecanismo de protección		X		
Archivo oculto encontrado		X		
Exposición de información confidencial a un autor no autorizado			X	
Falla del mecanismo de protección			X	
Exposición de información confidencial a un autor no autorizado				X

Nota. Se clasificaron las vulnerabilidades encontradas durante el escaneo y su grado critico en el que se encontraron.

TABLA IV.

Clasificación De Vulnerabilidades 192.168.1.137

TIPO DE ALERTA	SITIO: 192.168.1.137			
	Alto	Medio	Bajo	Informativo
Falla del mecanismo de protección		X		
Restricción inadecuada de capas		X		
Exposición de información confidencial a un autor no autorizado			X	
Falla del mecanismo de protección			X	

Nota. Se clasificaron las vulnerabilidades encontradas durante el escaneo y su grado critico en el que se encontraron.

TABLA V.

Clasificación De Vulnerabilidades 192.168.1.210

SCUBA TIPO DE ALERTA	SITIO: 192.168.1.210			
	Alto	Medio	Bajo	informativo
Cuentas anónimas existentes.	X			
Los nombres de host de los usuarios contienen comodines.	X			
Los nombres de host de los usuarios contienen comodines.	X			
Usuario de base de datos existentes con contraseñas en blanco (CIS MySQL 5.7)	X			
La opción de archivo local no está deshabilitada.		X		
SSL_TYPE la opción no está configurada como necesaria para usuarios remotos.		X		
Base de datos de prueba existente.		X		
Contraseña predeterminada, la opción lifetime esta deshabilitada o configurada en 91 o superior.		X		
La opción de modo sql no está establecido en 'ESTRICTO TODAS LAS TABLAS'		X		

Nota. Se clasificaron las vulnerabilidades encontradas durante el escaneo y su grado critico en el que se encontraron.

5.2. Mejora de configuraciones de seguridad.

Para mejorar las configuraciones de seguridad primero se considerarán las mitigaciones establecidas en anexo A1. Estas tienen como objetivo mitigar o reducir las vulnerabilidades obtenidas durante el proceso de pruebas; así como la implementación de controles y políticas de seguridad, las cuales se describen en el punto 5.3.

Otras mediadas a considerar para mejorar las configuraciones de seguridad son:

- Herramientas y medidas de prevención, es decir se implementan con la intención de proteger al sistema antes de que surjan las amenazas.
- Herramientas de detección y monitoreo, estas con el fin de que se puedan mitigar las amenazas de una manera más rápida y eficaz.
- Herramientas de respuesta, estas se preparan con una respuesta adecuada con anticipación, en amenazas o vulnerabilidades ya conocidas y que puedan volver a surgir.
- Verificación del cumplimiento de normas y estándares de seguridad.

5.3. Implementación de controles adicionales.

Otra medida de implementación de seguridad son las políticas de seguridad y la autentificación multifactor (MFA), ambas van de la mano para que su función sea más precisa.

Una política de acceso son un conjunto de reglas las cuales controlarán el acceso de los usuarios, dichas políticas serán establecidas dependiendo de las necesidades del sistema y están pueden modificarse si las necesidades van cambiando. Implementando estas solo los usuarios autorizados podrán acceder a los datos.

Por su lado la autentificación multifactor evitara que los usuarios no autorizados puedan acceder al sistema, esta consiste en la realización de varios pasos y no solo la autentificación mediante la contraseña, en caso de que la contraseña haya sido expuesta, con este aun así no podrá acceder ya que necesitaría información adicional.

Estas propuestas en conjunto con los controles adicionales nos permitirán tener una mayor seguridad en el sistema.

Los controles que se indican aplicar se encuentran en el apartado del informe técnico, en el cual se enlistan los CIS controls que se aplicaran para cada dirección IP tomando en cuenta las vulnerabilidades y especificaciones para cada una de ellas.

CAPITULO 6.

6. Plan de mejora continua.

6.1. Establecimiento de un ciclo de auditoria regular.

Si el sistema informático ya está establecido las auditorias se pueden realizar anualmente, pero en el caso del sistema que se está auditando al manejar información personal y considerando que ya es un sistema establecido y tomando en cuenta que en los resultados obtenidos su grado de criticidad es medio se propone que la realización del ciclo de auditorías sea de cada 6 meses, si en las futuras realizaciones los resultados de la auditoria llegan a cambiar se puede acortar el tiempo entre cada auditoria.

Así como también se recomienda que se siga el calendario propuesto en [TABLA I] para el proceso de las auditorias.

Se deben de establecer revisiones de seguridad, que se puedan estar realizando de manera periódicamente frecuentes, ya que si se presentara el caso de que hay alguna amenaza se trate de manera inmediata.

Las revisiones de seguridad que se proponen a realizar son:

- Hardware.
- Sistemas de actualizaciones.
- Gestión de permisos.
- Monitorización de recursos.

6.2. Monitoreo continuo y respuesta ante incidentes.

Un sistema de monitoreo continuo se encarga de analizar y vigilar de manera continua, el sistema, sus redes y sus procesos, esto con el fin de detectar en tiempo real, vulnerabilidades, amenazas y riesgos que puedan surgir; para poder mitigarlos de manera inmediata, mediante el monitoreo también es posible verificar el cumplimiento de estándares y normativas.

Su funcionamiento se basa en:

- Recopilación de datos.
- Análisis de datos.
- Alertar.

El sistema de monitoreo continuo puede estar dirigido a diferentes enfoques, los cuales son:

- Monitoreo de red: Analiza el tráfico en la red, incluyendo su rendimiento.
- Monitoreo de infraestructura: Analiza la infraestructura, los cuales son servidores, dispositivos de red y almacenamiento.
- Monitoreo de aplicaciones: supervisa el rendimiento de las aplicaciones.

El software que se propone a utilizar es Splunk ya que está diseñado para la gestión de volúmenes grandes de datos, se complementara con el uso de Nagios el cual está enfocado en el monitoreo de servidores. A continuación, se describirán las características de cada software.

Splunk.

Con Splunk se monitorea tanto las aplicaciones como la infraestructura del servidor, funciona en Windows y Linux. Splunk tiene un costo el cual dependerá de las herramientas y características a utilizar.

Los tipos de monitoreo que puede realizar Splunk son [17]:

- Servidores web.
- Servidores de aplicaciones.
- Servidores de base de datos.
- Servidores de infraestructura.
- Máquinas virtuales.
- Sistemas operativos.
- Servidores de implementación.
- Servidor indexador.

Las características que maneja el que se propone que es para aplicaciones e infraestructura son:

- Monitoreo de infraestructura.
- Conexión de log observer.
- Explorador de redes.
- Monitoreo sintético de tiempo de actividad.
- APM.
- Monitoreo de API sintéticas.
- Monitoreo de usuarios reales.
- Monitoreo sintético del navegador.

Nagios.

Se encarga de monitorear de manera estándar los servidores, es de licencia libre, funcionando en servidores como Windows, Apple, Linux y Unix.

Las características y herramientas que nos ofrece Nagios son [18]:

- Instalación simplificada.
- Monitor de monitoreo de código abierto.
- Licencia libre.
- Estaciones de trabajo y servidores Windows, Apple, Linux y Unix.
- Complementos para ampliar las capacidades nativas.
- Servidores de correo electrónico, FTP, DNS, SSH.
- Aplicaciones y servicios.

La implementación de herramientas a utilizar para el monitoreo continuo permite que la seguridad en el sistema sea más eficiente y por lo tanto tener un tiempo de respuesta rápido ante cualquier riesgo.

Plan de respuesta ante desastres y recuperación ante incidentes.

Un plan de recuperación ante desastres consiste en un documento el cual contiene un grupo de herramientas y estrategias a utilizar, en las que se indican cómo se debe de actuar en caso de un desastre natural, ciberataque, errores humanos o ante cualquier amenaza, este se realiza con el fin de mitigar de manera inmediata y proteger la información ante cualquier imprevisto que se presente.

El DRP se enfoca en 3 elementos [19]:

- Prevención: realiza copias de seguridad de los datos y lleva un monitoreo continuo para la detección de amenazas.
- Detección: se encarga de la detección de las amenazas para responder de manera rápida.
- Corrección: se encarga de que cuando se detecte un incidente, se restauren los sistemas y datos a su funcionamiento normal.

Existen diferentes tipos de DRP, estos enfocados a necesidades específicas, los cuales son:

- Plan de recuperación de centro de datos.
- Plan de recuperación virtualizados.
- Plan de recuperación basado en la nube.
- Plan de recuperación basado en la red.

Los pasos que se proponen para que se lleve a cabo el plan de respuesta ante desastres son los siguientes:

- Definir un comité de planificación.
- Realizar un inventario.
- Evaluación de riesgos.
- Definir objetivos de recuperación.
- Definir estrategias de recuperación.
- Realizar copias de seguridad.
- Documentar el plan.
- Probar la funcionalidad del plan.

Plan de respuesta ante incidentes.

Un plan de respuesta ante incidentes es un documento en el cual se especifican que roles y responsabilidades se le asigna a un equipo para ejecutar en caso de que haya un incidente y se pueda responder y actuar de manera adecuada ante la presencia de cualquier incidente.

Un IRP es un tipo de DRP el cual está enfocado en las amenazas a sistemas de información y ciberseguridad.

El objetivo de este es minimizar el daño, reducir el tiempo de respuesta y recuperación, cumplimiento de normas y políticas, y prevención de incidentes futuros.

Los pasos establecidos para el plan de respuesta a incidentes son los siguientes:

- Clasificar los incidentes.
- Identificar los recursos y la prioridad que tienen.
- Asignar roles y responsabilidades para una adecuada respuesta ante los incidentes.
- Definir planes de comunicación.
- Definir estrategias de contención.
- Procedimientos para erradicación y recuperación.
- Informes.
- Análisis posterior al incidente.
- Capacitaciones.
- Pruebas periódicas del plan.

6.3. Capacitación y conciencia en seguridad.

Las capacitaciones para saber actuar ante los incidentes son importantes ya que mediante estos se sabrá la manera de actuar en caso de que se presente alguno; estos no necesariamente son exclusivos para personal especializado, si no que el que sea accesible tanto a personal como estudiantes permite que sean menos probables estos incidentes o que sepan actuar de una manera adecuada en caso de se den.

La plataforma de CISA (Agencia de Ciberseguridad y seguridad de las infraestructuras) tiene como objetivo la seguridad ante amenazas cibernéticas, ofrece cursos gratuitos de capacitación de respuesta a incidentes, cuenta con clases de 60 minutos cada uno, en el cual abordan orientaciones básicas para saber cómo responder de una manera adecuada antes, durante y después de los incidentes, así como a prevenirlos, no se necesitan contar con conocimientos técnicos como antecedentes, ya que sus cursos están diseñados para el público en general.

El tener una cultura de seguridad ayuda a reducir los riesgos/errores ocasionados por los humanos, al tener una cultura de seguridad se pueden establecer hábitos con el fin de mejorar la seguridad de la información.

Se deben de aplicar estrategias para llevar a cabo lo anterior mencionado, proponiéndose las siguientes:

- Implementación de políticas de seguridad.
- Capacitaciones.
- Implementación y uso de herramientas para apoyar la seguridad.
- Monitorización continua.
- Planes de respuesta ante desastres y planes de respuesta ante incidentes.
- Evaluaciones periódicas en seguridad.
- Auditorias.

CAPÍTULO 7.

7. Resultados y discusión.

7.1. Análisis de los resultados de la auditoria.

Las vulnerabilidades detectadas durante la realización de la auditoria se resumirán a continuación:

- Falsificación de solicitud entre sitios.
- Falla del mecanismo de protección.
- Restricción inadecuada de capas.
- Archivo oculto encontrado.
- Exposición de información confidencial a un autor no autorizado.
- Obtener publicación.
- Validación de entrada incorrecto.
- Cuentas anónimas existentes.
- Los nombres de host de los usuarios contienen comodines.
- Usuario de base de datos existentes con contraseñas en blanco (CIS MySQL 5.7).
- La opción de archivo local no está deshabilitada.
- SSL_TYPE la opción no está configurada como necesaria para usuarios remotos.
- Base de datos de prueba existente.
- Contraseña predeterminada, la opción lifetime esta deshabilitada o configurada en 91 o superior.
- La opción de modo sql no está establecido en ‘ESTRICTO TODAS LAS TABLAS’

Los resultados obtenidos fueron verificados al realizarse tres escaneos a cada dirección IP y resultando todos iguales en su resultado, con la información ya verificada se pudo realizar el análisis de los resultados obtenidos.

Algunas de las vulnerabilidades encontradas se repitieron en los diferentes escaneos realizados, la diferencia es que en algunos casos su grado de criticidad era medio y en otros bajos, es decir, por esto las medidas de mitigación se propones las mismas ya que no sería necesario algo adicional al no ser alto su grado de criticidad.

7.2. Impacto de las medidas implementadas.

Las principales propuestas a implementar para las mitigaciones de las vulnerabilidades encontradas durante la auditoria se encuentran en el anexo A2, al aplicarlas se espera que ya no se caiga en estos incidentes, es por esto y para tener una mayor confianza en que no se repitan se propusieron medidas adicionales las cuales darán una mayor confiabilidad al ser implementadas, a continuación, se mencionaran las demás medidas que se propone que se apliquen:

- Controles adicionales de seguridad (CIS controls).
- Políticas de seguridad.
- Autentificación multifactor.
- Monitoreo continuo.
- Plan de respuesta ante desastres.
- Plan de recuperación ante incidentes.
- Capacitaciones de seguridad.

Con la implementación de estas medidas en conjunto se espera que las vulnerabilidades encontradas puedan ser mitigadas de manera satisfactoria para que en la realización de futuras auditorias estas ya no se presentan o su criticidad sea de manera informativa, es decir, que no esté exponiendo la información de los servidores.

7.3. Desafíos y limitaciones del proceso de auditoría.

Durante el desarrollo de la preparación para realizar la auditoria se presentaron diferentes desafíos y limitaciones comenzando con el hecho de que durante el proceso de estudiante no se estudió los estándares y normativas que se ocupan para entender lo que se debe de cumplir en cuestión de la protección de la información, así mismo como lo es una auditoria informática y como esta se puede llevar a cabo.

Otro desafío fue el proceso de investigación y comparativa para elegir los softwares a utilizar durante los procesos de la auditoria.

Por su lado la limitación que se enfrento fue que al estar en la red de la universidad la auditoria se necesitó realizar en un ambiente controlado, para no exponer la información de la institución.

CAPITULO 8.

8. Conclusiones y recomendaciones.

8.1. Conclusiones generales.

La seguridad en los servidores escaneados no presento gran cantidad de vulnerabilidades con grado de criticidad alto, sin embargo, se encontraron un total de 31 vulnerabilidades, con esto se puede indicar que se tiene que mejorar el estado de seguridad del servidor, ya que esto compromete la seguridad de la información.

Es importante tomar en cuenta que las instituciones académicas deben de cumplir con políticas, normativas y controles de seguridad que garanticen la protección de la información tanto de estudiantes como de personal; para el caso de la problemática planteada estas normativas y estándares estarán basadas en el Marco de Ciberseguridad del NIST, la norma ISO 27001, Cis Controls y OWASP TOP 10.

Es por esto que la realización de auditorías a instituciones académicas son de suma importancia ya que mediante estas es posible detectar los problemas de seguridad que puedan tener los sistemas y así implementar diferentes medidas de mitigación para garantizar la seguridad en estos, así como es necesario desarrollar un plan de mejora continua, el propuesto se basa en 4 puntos que consisten en: el establecimiento regular de auditorías, monitoreo continuo y respuesta ante incidentes mediante el apoyo de softwares, un plan de respuesta ante desastres y recuperación ante incidentes, y capacitaciones.

Garantizar la protección de información debe ser la adecuada para que las instituciones académicas tengan una buena reputación y se consideren confiables, además de que esto cumple con garantizar que la información personal no sea expuesta ni utilizada de manera no adecuada.

8.2. Recomendaciones futuras.

Se propone la realización de auditorías periódicas, como se manejan grandes volúmenes de información estas se deben de realizar de manera periódica mínimo dos veces al año, así como la implementación de herramientas y recursos que poder garantizar la seguridad de la información, como lo son propuestas de softwares para el monitoreo continuo de los servidores y así mismo capacitaciones para entender y saber actuar en caso de que se presenten incidentes.

La implementación de herramientas de seguridad se debe aplicar y elegir de acuerdo a las características y necesidades de los servidores, en este caso se propusieron Nagios Y Splunk, Nagios por su parte está enfocado en el monitoreo continuo de los servidores pudiendo agregar más herramientas a utilizar en caso de que las necesidades del servidor así lo requiera; Splunk esta está dirigido a la monitorización a grandes volúmenes de información que se encuentran tanto en servidores como en aplicaciones, brindado informes técnicos constantes.

Mediante estas propuestas se pueden realizar análisis para identificar las mejoras que se requieran realizar de manera constante a la seguridad de los servidores de la institución.

8.3. Aportes del trabajo a la administración de la red y equipo de laboratorio de telecomunicaciones.

La presente investigación pretende dar a conocer la importancia de la seguridad de la información en instituciones, proponiendo una cultura en materia de seguridad en la población estudiantil y del personal.

Entendiendo la importancia del cumplimiento de la normativa ISO 27001 y el estándar NIST Cybersecurity, ya que al cumplir con estas se pude justificar la seguridad de la información.

La manera en que una institución académica puede gestionar los riesgos que se presenten es mediante la realización de auditorías, la monitorización continua, la implementación de softwares y herramientas necesarias, así como la capacitación constante a personal y estudiantes sobre seguridad, esto con el fin de que mediante el acceso a la información se presenten menor cantidad de incidentes.

Estas recomendaciones quedan criterio del encargo de los servidores si son implementadas o no, ya que son recomendaciones y propuestas de mejoras.

Bibliografía

[1] INCIBE CERT, «Vulnerabilidades,» INCIBE CERT, 2024. [En línea]. Available: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades. [Último acceso: 21 03 2024].

[2] Normas ISO, «ISO 27001 seguridad de la información,» Normas iso , 2024. [En línea]. Available: https://www.normas-iso.com/iso-27001/#section_refer. [Último acceso: 29 04 2024].

[3] C. M. Arévalo , «ISO 27001: ¿Cuántos controles necesitas para cumplir la norma?,» Pirani, 13 10 2020. [En línea]. Available: https://www.piranirisk.com/es/blog/cuantos-controles-tiene-la-norma-iso-27001. [Último acceso: 25 04 2024].

[4] National Institute of Standars and Technology, «El marco de seguridad cibernética (CSF) 2.0 del NIST,» 26 02 2024. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf. [Último acceso: 22 01 2025].

[5] Cis Center for Internet, «CIS controls V7,» 2025. [En línea]. Available: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf. [Último acceso: 26 01 2025].

[6] OWASP, «OWASP TOP 10,» OWASP.org, 2021. [En línea]. Available: https://owasp.org/Top10/es/. [Último acceso: 30 01 2025].

[7] Retos diretivos , «Tipos de auditoría que existen,» EAE, 08 03 2022. [En línea]. Available: https://retos-directivos.eae.es/conoces-los-principales-tipos-de-auditoria-que-existen/. [Último acceso: 22 01 2024].

[8] LaEdu, «Auditoria informática, objetivos, metodología e importancia,» LaEdu.digital, 07 09 2021. [En línea]. Available: https://laedu.digital/2021/09/07/auditoria-informatica-objetivos-metodologia-e-importancia/. [Último acceso: 22 01 2024].

[9] O. Kassandra, «Auditoría Informática: qué es, cuáles son sus fases y por qué es importante para las empresas,» SAINT LEO UNIVERSITY, 29 05 2024. [En línea]. Available: https://worldcampus.saintleo.edu/blog/fases-de-una-auditoria-informatica-y-en-que-consisten#:~:text=Es%20un%20proceso%20sistem%C3%A1tico%20que,objetivos%20y%20estrategias%20del%20negocio.. [Último acceso: 22 01 2025].

[10] S. Manish, «Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos,» freeCodeCamp, 23 04 2023. [En línea]. Available:

https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/. [Último acceso: 25 06 2024].

[11] Genuinocloud, «¿Qué es Nmap?,» microbit, 2025. [En línea]. Available: https://genuinocloud.com/blog/que-es-nmap/. [Último acceso: 01 05 2025].

[12] NMAP, «Zenmap,» NMAP.ORG, 2024. [En línea]. Available: https://nmap.org/zenmap/. [Último acceso: 25 06 2024].

[13] Exlusive Networks , «Imperva Scuba Database Vulnerability Scaner,» Exlusive Networks , 06 12 2018. [En línea]. Available: https://www.exclusive-networks.com/ch-fr/imperva-scuba-schwachstellenscanner-datenbanken/. [Último acceso: 20 03 2024].

[14] Imperva , «Escaner de vulnerabilidades de la base de datos de Scuba,» Imperva a Thales Company, 19 09 2012. [En línea]. Available: https://www.imperva.com/resources/free-cyber-security-testing-tools/scuba-database-vulnerability-scanner/. [Último acceso: 20 03 2024].

[15] OWASP, «OWASP proyectos,» OWASP, 2025. [En línea]. Available: https://owasp.org/projects/. [Último acceso: 02 05 2025].

[16] Atlassian, «Niveles de gravedad de las incidencias de seguridad,» ATLASSIAN, 2025. [En línea]. Available: https://www.atlassian.com/es/trust/security/security-severity-levels#:~:text=Nivel%20de%20gravedad:%20alto,un%20tiempo%20de%20inactividad%20significativos.. [Último acceso: 20 07 2025].

[17] Splunk , «Productos Splunk,» splunk a CISCO company , 2025. [En línea]. Available: https://www.splunk.com/en_us/products.html. [Último acceso: 30 04 2025].

[18] Nagios , «Plataforma de servicios básicos de Nagios,» Nagios , 2025. [En línea]. Available: https://www.nagios.org/. [Último acceso: 30 04 2025].

[19] zscaler, «¿Qué es un plan de recuperación ante desastres (DRP)?,» zscaler , 2025. [En línea]. Available: https://www.zscaler.com/mx/zpedia/what-is-a-disaster-recovery-plan. [Último acceso: 01 05 2025].

[20] CWE, «Enumeración de vulnerabilidades comunes Top 25,» CWE, 15 12 2024. [En línea]. Available: https://cwe.mitre.org/data/definitions.

[21] OWASP, «Serie de hojas de referencia de OWASP,» OWASP, 2024. [En línea]. Available: https://cheatsheetseries.owasp.org. [Último acceso: 20 11 2024].

[22] J. Costas Santos, Seguridad y alta disponibilidad (Grado superior), Madrid: RA-MA, 2011.

[23] F. J. Santa Pérez , S. Candela Sola, A. Quesada Arancebla, J. M. Santos Espino y R. García Carmelo , Fundamentos de sistemas operativos. Teoria y ejercicios resueltos, Madrid : Paraninfo , 2007.

[24] J. Areito Bertolin , Seguridad de la información. Redes, informática y sistemas de información., España: Paraninfo, 2008.

[25] Departamento de seguridad informatica , «Amenazas a la seguridad de la información,» Universidad Nacional de Lujan , [En línea]. Available: https://www.seguridadinformatica.unlu.edu.ar/?q=node/12. [Último acceso: 20 03 2024].

[26] E. Chicano Tejada , Auditoría de seguridad informática. IFCT0109, España: IC, 2023.

[27] ESGinnova Group, «Determinación del alcance de SGSI,» ESGinnova Group, 07 08 2020. [En línea]. Available: https://www.pmg-ssi.com/2020/08/determinacion-del-alcance-del-sgsi/. [Último acceso: 25 04 2024].

[28] IBM, «¿Qué es el marco de ciberseguridad del NIST?,» IBM, 2025. [En línea]. Available: https://www.ibm.com/mx-es/topics/nist. [Último acceso: 15 01 2025].

[29] O. Kassandra, «¿Cuáles son las funciones de un auditor informático y cuánto gana en Latinoamérica?,» SAINT LEO UNIVERSITY, 29 05 2024. [En línea]. Available: https://worldcampus.saintleo.edu/blog/funciones-de-un-auditor-informatico#:~:text=Un%20profesional%20que%20ejerce%20un,ganar%20hasta%201940%20d%C3%B3lares%20mensuales.. [Último acceso: 22 04 2025].

[30] GRCTools, «El nuevo paradgma de las auditorías basadas en riesgos,» ESGinnova Group, 2025. [En línea]. Available: https://grctools.software/2020/08/04/el-nuevo-paradigma-de-las-auditorias-basadas-en-riesgos/. [Último acceso: 05 02 2025].

[31] R. P. Manuela, Auditoria de seguridad informática MF0487_3, Madrid: Paraninfo, 2024.

[32] Fortra, «Qué es el escaneo de vulnerabilidades y cómo funciona,» Fortra, 25 06 2022. [En línea]. Available: https://www.fortra.com/es/blog/escaneo-vulnerabilidades. [Último acceso: 01 05 2024].

[33] C. Carlos, «¿Qué es un escaneo de vulnerabilidades?,» Keepcoding, 18 04 2024. [En línea]. Available: https://keepcoding.io/blog/que-es-un-escaneo-de-vulnerabilidades/. [Último acceso: 01 05 2024].

[34] Nmap, «Guía de referencia de Nmap,» nmap.org, 2024. [En línea]. Available: https://nmap.org/man/es/index.html. [Último acceso: 25 06 2024].

[35] D. L. Sergio, «Realizar escaneos de puertos con Nmap a cualquier servidor o sistema,» RedesZone, 20 06 2024. [En línea]. Available: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/. [Último acceso: 27 06 2024].

[36] P. Edinson, «Zenmap,» Academia de ciberseguridad, 24 06 2023. [En línea]. Available: https://aprende.academia-ciberseguridad.com/books/herramientas/page/zenmap. [Último acceso: 25 06 2024].

[37] portnox, «¿Qué es el OWASP TOP 10?,» portnox, 2025. [En línea]. Available: https://www.portnox.com/cybersecurity-101/what-is-the-owasp-top-10/. [Último acceso: 02 05 2025].

[38] G. d. Z. Fernán, «OWASP ¿Qué es y cómo usar esta metodologías?,» arsys, 16 20 2024. [En línea]. Available: https://www.arsys.es/blog/owasp. [Último acceso: 02 05 2025].

[39] IBM , «Políticas de acceso,» IBM, 24 04 2025. [En línea]. Available: https://www.ibm.com/docs/es/security-verify?topic=sign-access-policies. [Último acceso: 26 04 2025].

[40] «¿Qué es la autenticación multifactor (MFA)?,» AWS, 2024. [En línea]. Available: https://aws.amazon.com/es/what-is/mfa/#:~:text=es%20AWS%20Identity%3F-,%C2%BFEn%20qu%C3%A9%20consiste%20la%20MFA%20(autenticaci%C3%B3n%20multifactor)%3F,informaci%C3%B3n%20que%20simplemente%20una%20contrase%C3%B1a.. [Último acceso: 26 04 2025].

[41] AUDITOOL , «7 Buenas prácticas para auditar la seguridad de la información,» AUDITOOL, 09 04 2023. [En línea]. Available: https://www.auditool.org/blog/auditoria-de-ti/buenas-practicas-para-auditar-la-seguridad-de-la-informacion. [Último acceso: 30 04 2025].

[42] B. Keri, «Monitoreo continuo: Qué necesita saber y cómo empezar en 5 pasos,» pathlock, 15 01 2024. [En línea]. Available: https://pathlock.com/learn/continuous-monitoring/. [Último acceso: 30 04 2025].

[43] W. Shanika, «¿Qué es el Monitoreo Continuo?,» Splunk a CISCO company , 07 05 2024. [En línea]. Available: https://www.splunk.com/en_us/blog/learn/continuous-monitoring.html. [Último acceso: 30 04 2025].

[44] IBM, «¿Qué es un plan de recuperacion ante desatres (DRP)?,» IBM, 2025. [En línea]. Available: https://www.ibm.com/mx-es/topics/disaster-recovery-plan. [Último acceso: 01 05 2025].

[45] ATLASSIAN , «Gestión de incidentes para equipos de alta velocidad,» ATLASSIAN , 2025. [En línea]. Available: https://www.atlassian.com/es/incident-management#types-of-incident-management-processes. [Último acceso: 01 05 2025].

[46] Microsoft, «¿Qué es la respuesta a incidentes?,» Microsoft, 2025. [En línea]. Available: https://www.microsoft.com/es-mx/security/business/security-101/what-is-incident-response. [Último acceso: 02 05 2025].

[47] B. Chris, «¿Qué es un plan de Respuesta a Incidentes (PRI)?,» FORTRA , 2025. [En línea]. Available: https://www.digitalguardian.com/blog/what-incident-response-plan-irp. [Último acceso: 02 05 2025].

[48] CISA, «Capacitación en respuesta a incidentes,» America´s Cyber Defense Agency, 2025. [En línea]. Available: https://www.cisa.gov/resources-tools/programs/Incident-Response-Training. [Último acceso: 02 05 2025].

[49] S2GRUPO, «Cómo fomentar una cultura de ciberseguridad en la empresa,» S2GRUPO, 30 08 2024. [En línea]. Available: https://s2grupo.es/como-fomentar-una-cultura-de-ciberseguridad-en-la-empresa/. [Último acceso: 03 05 2025].

ANEXOS.

A1. Controles aplicables al caso de estudio de la norma ISO 27001.

A.9 Seguridad física y ambiental.

A.9.1 Áreas seguras.

A.9.1.1 Perímetro de seguridad física.

A.9.1.2 Controles de entrada físicos.

A.9.1.3 Seguridad de oficinas, habitaciones y medios.

A.9.1.5 Trabajo en áreas seguras.

A.9.1.6 Áreas de acceso público, entrega y carga.

A.9.2 Seguridad del equipo.

A.9.2.2 Servicios públicos.

A.9.2.6 Eliminación seguro o re-uso del equipo.

A.9.2.7 Traslado de propiedad.

A.10 Gestión de las comunicaciones y operaciones.

A.10.1 Procedimientos y responsabilidades operacionales.

A.10.1.1 Procedimiento de operaciones documentados.

A.10.1.3 Segregación de deberes.

A.10.2 Gestión de la entrega del servicio de terceros.

A.10.2.1 Entrega del servicio.

A.10.2.2 Monitoreo y revisión de los servicios de terceros.

A.10.2.3 Manejar los cambios en los servicios de terceros.

A.10.3 Planeación y aceptación del sistema.

A.10.3.1 Gestión de capacidad.

A.10.4 Protección contra software malicioso y código móvil.

A.10.4.1 Controles contra software malicioso.

A.10.4.2 Controles contra códigos móviles.

A.10.6 Gestión de seguridad en redes.

A.10.6.1 Controles de red.

A.10.6.2 Seguridad de los servicios de red.

A.10.7 Gestión de medios.

A.10.7.3 Procedimiento de manejo de la información.

A.10.7.4 Seguridad de la documentación del sistema.

A.10.8 Intercambio de información.

A.10.8.2 Acuerdos de intercambio.

A.10.8.4 Mensajes electrónicos.

A.10.8.5 Sistemas de información comercial.

A.10.9 Servicios de comercio electrónico.

A.10.9.2 Transacciones en línea.

A.10.10 Monitoreo.

A.10.10.1 Registro de auditoría.

A.10.10.4 Registros del administrador y operador.

A.10.10.5 Registro de fallas.

A.11 Control de acceso.

A.11.1 Requerimiento comercial para el control de acceso.

A.11.1.1 Política de control de acceso.

A.11.2 Gestión del acceso del usuario.

A.11.2.2 Gestión de privilegios.

A.11.2.3 Gestión de la clave de usuario.

A.11.3 Responsabilidad del usuario.

A.11.3.1 Uso de clave.

A.11.4 Control de acceso a redes.

A.11.4.1 Política sobre el uso de servicios en red.

A.11.4.2 Autenticación del usuario para conexiones externas.

A.11.4.4 Protección del puerto de diagnóstico remoto.

A.11.4.5 Segregación en redes.

A.11.4.6 Control de conexión de redes.

A.11.5 Control de acceso al sistema de operación.

A.11.5.2 Identificación y autentificación del usuario.

A.11.5.4 Uso de utilidades del sistema.

A.11.5.5 Sesión inactiva.

A.11.5.6 Limitación de tiempo de conexión.

A.11.6 Control de acceso a la aplicación e información.

A.11.6.1 Restricción al acceso a la información.

A.11.7 Computación móvil y tele-trabajo.

A.11.7.1 Computación móvil y comunicaciones.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.

A.12.2 Procesamiento correcto en las aplicaciones.

A.12.2.2 Control de procesamiento interno.

A.12.3 Controles criptográficos.

A.12.3.1 Política sobre el uso de controles criptográficos.

A.12.4 Seguridad de los archivos del sistema.

A.12.4.1 Control de software operacional.

A.12.4.3 Control de acceso al código fuente del programa.

A.12.5 Seguridad en los procesos de desarrollo y soporte.

A.12.5.1 Procedimientos de control de cambio.

A.12.5.4 Filtración de información.

A.12.5.5 Desarrollo de outsourced software.

A.12.6 Gestión de vulnerabilidad técnica.

A.12.6.1 Control de vulnerabilidades técnicas.

A.13 Gestión de incidentes en la seguridad de la información.

A.13.1 Reporte de eventos y debilidades en la seguridad de la información.

A.13.1.1 Reporte de eventos en la seguridad de la información.

A.13.2 Gestión de incidentes y mejoras en la seguridad de la información.

A.13.2.2 Aprendizaje de los incidentes en la seguridad de la información.

A.14 Gestión de la continuidad comercial.

A.14.1 Aspectos de la seguridad de la información de la gestión de la comunidad comercial.

A.14.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información.

A.14.1.4 Marco referencial para la planeación de la continuidad comercial.

A.15 Cumplimiento.

A.15.1 Cumplimiento con requerimientos legales.

A.15.1.3 Protección a los registros organizacionales.

A.15.1.5 Prevención del mal uso de medios de procesamiento de información.

A.15.2 Cumplimientos con las políticas y estándares de seguridad, y el cumplimiento técnico.

A.15.2.1 Cumplimiento con las políticas y estándares de seguridad.

A.15.2.2 Chequeo de cumplimiento técnico.

A.15.3 Consideraciones de auditoría de los sistemas de información.

A.15.3.1 Controles de auditoría a sistemas de información.

A.15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

A2. Controles aplicables al caso de estudio CIS controls.

Los CIS controls al ser muy extensa su descripción, se pondr la referencia a continuación, en el cual es en la página oficial de CIS controls V7.

[5] Cis Center for Internet, «CIS controls V7,» 2025. [En línea]. Available: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf. [Último acceso: 26 01 2025].

A3. Capturas de pantalla y logs.

Evidencias visuales de los análisis realizados.

TABLA VI.

Escaneo De la Dirección 192.168.1.210

192.168.1.210				
Vulnerabilidad	CWE	Descripción	Detalles	Remediación
Falsificación de solicitud entre sitios (CSRF)	352	La aplicación web no verifica, o no puede verificar, de manera suficiente si el usuario que envió la solicitud proporciono intencionalmente una solicitud bien formada, valida y consistente.	Cuando un servidor web está diseñado para recibir una solicitud de un cliente sin ningún mecanismo para verificar que se envió intencionalmente, es posible que un atacante engañe a un cliente para que realice una solicitud no intencional al servidor web que se tratara como una solicitud autentica. Esto se puede hacer a través de una URL, la carga de una imagen, XMLHttpRequest , etc. Y puede dar como resultado la exposición de datos o la ejecución no deseada de código.	1. Bibliotecas o frameworks: utilizar una biblioteca o un marco aprobado que no permita que ocurra esta debilidad o que proporcione construcciones que hagan que sea más fácil evitarla. Asegurarse de que la aplicación esté libre de problemas de secuencias de comandos entre sitios, porque la mayoría de las defensas CSRF se pueden eludir mediante secuencias de comando controladas por el atacante. 2. Generar un numero único para cada formulario, colocarlo en el formulario y verificar al recibirlo. Asegurarse de que el número no sea predecible. 3.Identificar operaciones especialmente peligrosas. Cuando

				el usuario realiza una operación peligrosa, enviar una solicitud de confirmación por separado para garantizar que el usuario tenía la intención de realizar esa operación. 4.Utilizar el método de “cookie de doble envió” descrito por Felten y Zeller: cuando un usuario visita un sitio, el sitio debe generar un valor pseudoaleatorio y configurarlo como una cookie en la máquina del usuario. El sitio debe exigir que cada envío de formulario incluya este valor como valor de formulario y también como valor de cookie. Cuando se envía una solicitud POST al sitio, la solicitud solo debe considerarse valida si el valor del formulario y el valor de la cookie son iguales. 5. No utilizar el método GET para ninguna solicitud que active un cambio de estado: verifique el encabezado HTTP Refer para ver si la

				solicitud se originó desde una página esperada. Esto podría, interrumpir la funcionalidad legítima, ya que los usuarios o servidores proxy puede haber deshabilitado el envío del Refer por razones de privacidad.
Falla del mecanismo de protección	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	Esta debilidad abarca tres situaciones distintas. Un mecanismo de protección "faltante" se produce cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo "ignorado" se produce cuando un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha aplicado en alguna ruta de código.	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidades significativamente diferentes de las que se pretende prevenir.

Restricción inadecuada de capas	1021	La aplicación web no restringe o restringe incorrectamente los objetos de marco o capas de UI que pertenecen a otra aplicación o dominio, lo que puede generar confusión en el usuario sobre con que interfaz esta interactuando.	Se espera que una aplicación web imponga restricciones sobre si permite que se la represente dentro de marcos, iframes, objetos, elementos incrustados o subprogramas. Sin las restricciones, los usuarios pueden verse engañados para que interactúen con la aplicación cuando no tenían intención de hacerlo.	El uso de X-Frame-Options permite a los desarrolladores de contenido web restringir el uso de aplicación en forma de superposiciones, marcos o iFrames. Un desarrollador puede utilizar un script "frame-breaker" en cada página que no debe de estar enmarcada. Esto resulta muy útil para los navegadores antiguos que no admiten la función de seguridad X-Frame-Options mencionada anteriormente. Esta técnica de defensa en profundidad se puede utilizar para evitar el uso indebido de marcos en aplicaciones web. Priorizar las fuentes validas de datos que se cargaran en la aplicación mediante el uso de políticas declarativas.
Archivo oculto encontrado	538	El servidor coloca información confidencial en archivos o directorios a los que pueden		No exponer información de archivos y directorios al usuario.

		acceder los actores que tienen permiso para acceder a los archivos, pero no a la información confidencial.		
Exposición de información confidencial a un autor no autorizado.	200	El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.	Existen muchos tipos distintos de errores que pueden exponer la información. La gravedad del error puede variar ampliamente, dependiendo del contexto en el que opera el producto, el tipo de información confidencial que se releva y los beneficios que puede proporcionar a un atacante. Desde la perspectiva de CWE, la perdida de confidencialidad es un impacto técnico que puede surgir de docenas de debilidades, como permisos de archivos inseguros o lectura fuera de los límites.	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentació n adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios.
Exposición de información confidencial a un autor no autorizado.	200	El servidor expone información confidencial a un actor que no está explícitamente autorizado a	Existen muchos tipos distintos de errores que pueden exponer la información. La gravedad del error puede variar ampliamente,	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No

		tener acceso a esa información.	dependiendo del contexto en el que opera el producto, el tipo de información confidencial que se releva y los beneficios que puede proporcionar a un atacante. Desde la perspectiva de CWE, la perdida de confidencialidad es un impacto técnico que puede surgir de docenas de debilidades, como permisos de archivos inseguros o lectura fuera de los límites.	permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentació n adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios.
Falla del mecanismo de protección.	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	Esta debilidad cubre tres situaciones distintas. Un mecanismo de protección "faltante" ocurre cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir.

			“ignorado” ocurre cuando un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha aplicado en alguna ruta de código.	
Obtener publicación	16	Las debilidades en esta categoría generalmente se introducen durante la configuración del software.		NOTA: esta entrada es una categoría, pero varias fuentes la asignan de todos modos, a pesar de la orientación de CWE de que no se deben asignar categorías. En este caso, no hay debilidades claras de CWE que se puedan utilizar.
Validación de entrada incorrecta.	20	El servidor recibe entrada o datos, pero no valida o validad incorrectamente que la entrada tenga las propiedades necesarias para procesar los datos de forma segura y correcta.	La validación de entrada es una técnica que se utiliza con frecuencia para comprobar entradas potencialmente peligrosas con el fin de garantizar que sean seguras para su procesamiento dentro del código o al comunicarse con otros componentes. Cuando el software no valida la entrada correctamente, un atacante puede crear la entrada de una forma que no	Utilizar técnicas como: 1.Reducción de la superficie. 2.Bibliotecas o Frameworks. 3.Reducción de la superficie de ataque. 4.Validación de entrada.

			espera el resto de la aplicación. Esto hará que partes del sistema reciban una entrada no deseada, lo que puede provocar un flujo de control alterado, un control arbitrario de un recurso o la ejecución de código arbitrario.	

Nota. Son los resultados obtenidos de las amenazas y vulnerabilidades durante el escaneo a 192.168.1.210

TABLA VII.

Escaneo de la dirección 192.168.107:3000 y 172.18.12.70:3000

192.168.1.107:3000				
Vulnerabilidad	CWE	Descripción	Detalles	Remediación
Falla del mecanismo de protección.	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	Esta debilidad cubre tres situaciones distintas. Un mecanismo de protección "faltante" ocurre cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo "ignorado" ocurre cuando	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir.

			un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha aplicado en alguna ruta de código.	
Archivo oculto encontrado.	538	El servidor coloca información confidencial en archivos o directorios a los que pueden acceder los actores que tienen permiso para acceder a los archivos, pero no a la información confidencial.		No exponer información de archivos y directorios al usuario.
Divulgación de la marca de hora – Unix.	200	El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.	Existen muchos tipos distintos de errores que pueden exponer la información. La gravedad del error puede variar ampliamente, dependiendo del contexto en el que opera el producto, el tipo de información confidencial que se releva y los beneficios que puede proporcionar a un atacante. Desde la perspectiva de CWE, la perdida de confidencialidad	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentación adecuada en el diseño del sistema y que esta permita

			es un impacto técnico que puede surgir de docenas de debilidades, como permisos de archivos inseguros o lectura fuera de los límites.	reforzar la funcionalidad de separación de privilegios.
Falla del mecanismo de protección.	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	Esta debilidad cubre tres situaciones distintas. Un mecanismo de protección "faltante" ocurre cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo "ignorado" ocurre cuando un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha aplicado en alguna ruta de código.	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir.

Divulgación de información – comentarios sospechosos.	200	El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.	Existen muchos tipos distintos de errores que pueden exponer la información. La gravedad del error puede variar ampliamente, dependiendo del contexto en el que opera el producto, el tipo de información confidencial que se releva y los beneficios que puede proporcionar a un atacante. Desde la perspectiva de CWE, la perdida de confidencialidad es un impacto técnico que puede surgir de docenas de debilidades, como permisos de archivos inseguros o lectura fuera de los límites.	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentación adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios.

Nota. Son los resultados obtenidos de las amenazas y vulnerabilidades durante el escaneo a 192.168.1.107:3000 y 172.18.12.70:3000

TABLA VIII.

Escaneo De La Dirección 192.168.1.137

192.168.1.137				
Vulnerabilidad	CWE	Descripción	Detalles	Remediación
Falla del mecanismo de protección	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección	Esta debilidad cubre tres situaciones distintas. Un mecanismo de	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no

		que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	protección "faltante" ocurre cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo "ignorado" ocurre cuando un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha aplicado en alguna ruta de código.	se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir.
Restricción inadecuada de capas	1021	La aplicación web no restringe o restringe incorrectamente los objetos de marco o capas de UI que pertenecen a otra aplicación o dominio, lo que puede generar confusión en el usuario sobre	Se espera que una aplicación web imponga restricciones sobre si permite que se la represente dentro de marcos, iframes, objetos, elementos incrustados o subprogramas. Sin las restricciones, los	El uso de X-Frame-Options permite a los desarrolladores de contenido web restringir el uso de aplicación en forma de superposiciones, marcos o iFrames. Un desarrollador puede utilizar un script "frame-breaker" en cada página que no debe

		con que interfaz esta interactuando.	usuarios pueden verse engañados para que interactúen con la aplicación cuando no tenían intención de hacerlo.	de estar enmarcada. Esto resulta muy útil para los navegadores antiguos que no admiten la función de seguridad X-Frame-Options mencionada anteriormente. Esta técnica de defensa en profundidad se puede utilizar para evitar el uso indebido de marcos en aplicaciones web. Prioriza las fuentes validas de datos que se cargaran en la aplicación mediante el uso de políticas declarativas.
Exposición de información confidencial a un autor no autorizado	200	El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.	Existen muchos tipos distintos de errores que pueden exponer la información. La gravedad del error puede variar ampliamente, dependiendo del contexto en el que opera el producto, el tipo de información confidencial que se releva y los beneficios que puede proporcionar a un atacante. Desde la perspectiva de	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentación

			CWE, la perdida de confidencialidad es un impacto técnico que puede surgir de docenas de debilidades, como permisos de archivos inseguros o lectura fuera de los límites.	adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios.
Falla del mecanismo de protección	693	El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.	Esta debilidad cubre tres situaciones distintas. Un mecanismo de protección "faltante" ocurre cuando la aplicación no define ningún mecanismo contra una determinada clase de ataque. Un mecanismo de protección "insuficiente" puede proporcionar algunas defensas, pero no protege contra todo lo que se pretende. Por último, un mecanismo "ignorado" ocurre cuando un mecanismo está disponible y en uso activo dentro del producto, pero el desarrollador no lo ha	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir.

			aplicado en alguna ruta de código.	

Nota. Son los resultados obtenidos de las amenazas y vulnerabilidades durante el escaneo a 192.168.1.137.

TABLA IX.

Escaneo Con SCUBA De la Dirección 192.168.1.210

SCUBA. SITIO: 192.168. 1.210			
Vulnerabilidad	Descripción	Detalles	Remediación
Cuentas anónimas existentes.	Permiten inicios de sesión predeterminados y estos permisos a veces pueden ser utilizados por otros usuarios. Compruebe si existen usuarios sin nombre.	Evitar el uso de cuentas anónimas garantiza que solo los usuarios de confianza puedan acceder a la cuenta.	Verificar y eliminar cuentas anónimas.
Los nombres de host de los usuarios contienen comodines.	Compruebe si los nombres de host de los usuarios contienen un comodín.	Evitar el uso de comodines dentro de los nombres de host garantiza que solo los principales confiables puedan interactuar con MySQL.	Verificar si los usuarios tienen un comodín (%) en el nombre de host.
Los nombres de host de los usuarios contienen comodines.	Compruebe si los nombres de host de los usuarios contienen un comodín.	Evitar el uso de comodines dentro de los nombres de host garantiza que solo los principales confiables puedan interactuar con MySQL.	Verificar si los usuarios tienen un comodín (%) en el nombre de host.
Usuario de base de datos existentes con contraseñas en blanco (CIS MySQL 5.7)	Compruebe si existen usuarios de la base de datos con	Sin una contraseña, con solo conocer el nombre de	Para cada fila devuelta del procedimiento de auditoría, establezca una contraseña para el usuario dado

	contraseñas en blanco.	usuario y la lista de host permitidos, alguien podrá conectarse al servidor y asumir la identidad del usuario. Esto, en efecto, evita los mecanismos de autenticación.	utilizando la siguiente declaración (como ejemplo) ESTABLECER LA CONTRASEÑA PARA <usuario>@<host><borrar contraseña" NOTA: Remplace <usuario>, <host> y <contraseña clara> con los valores apropiados.
La opción de archivo local no está deshabilitada.	Compruebe si la opción local_infile está configurada en ON.	Deshabilitar el archivo de entrada local reduce la capacidad de un atacante de leer archivos confidenciales del servidor afectado a través de una vulnerabilidad de inyección SQL.	Agregar la siguiente línea a la sección [mysqld) del archivo de configuración de MySQL y reinicie el servidor MySQL: local-infile=0
SSL_TYPE la opción no está configurada como necesaria para usuarios remotos.	Compruebe si la opción de tipo SSL está configurada en cualquiera, X50% o especificado para todos los usuarios.	El protocolo MySQL protegido con SSL/TLS ayuda a prevenir escuchas clandestinas y ataques de intermediarios.	Utilizar la declaración GRANT para requerir el uso de SSL. Uso de GRANT en mi usuario@app1.example.com REQUIRE SSL. Tener en cuenta que REQUIRE SSL solo aplica SSL. Hay opciones como REQUIRE X509, REQUIRE ISSUER, REQUIRE SUBJET pueden utilizarse para restringir aún más las opciones de conexión.
Base de datos de prueba existente.	Compruebe si existe la base de datos 'test'.	Eliminar los componentes no utilizados eliminara la capacidad de un atacante de utilizarlos.	Eliminar la base de datos de prueba.

Contraseña predeterminada, la opción lifetime esta deshabilitada o configurada en 91 o superior.	Compruebe si la opción de duración de la contraseña predeterminada esta deshabilitada (0) o establecida en 91 o superior.	La caducidad de contraseña proporciona contraseñas con una duración limitada en el tiempo. Evitar que una contraseña se establezca por un periodo indefinido, reduciendo así el tiempo disponible durante el cual un atacante puede conocer una contraseña comprometida.	Realizar las siguientes acciones: Establecer global duración de contraseña predeterminada de 90 y en el archivo de configuración: contraseña predeterminada lifetime-90 Como parte de la instalación y planificación, considere establecer una política de vencimiento para usuarios específicos. Esto tendrá prioridad sobre la configuración especificada en la duración de la contraseña predeterminada. Por ejemplo: Modificar usuario jeffrey@localhost' INTERVALO DE EXPIRACION DE CONTRASEÑA 90 DIAS.
La opción de modo sql no está establecido en 'ESTRICTO TODAS LAS TABLAS'	Compruebe si la opción 'modo sql' no contiene el valor 'STRICT ALL TABLES'	Sin el modo estricto, el servidor intenta continuar con la acción cuando un error podría haber sido una opción más segura. Por ejemplo, de forma predeterminada, MySQL truncara los datos si no caben en un campo, lo que puede generar un comportamiento desconocido o ser aprovechado por un atacante para eludir la	Realizar la siguiente acción para corregir esta configuración Agregar STRICT ALL TABLES al modo sql en el archivo de configuración del servidor.

		validación de datos.	

Nota. Nota. Son los resultados obtenidos de las amenazas y vulnerabilidades durante el escaneo con SCUBA a 192.168.1.210

A4. Informe técnico completo.

En el informe técnico se va a encontrar las vulnerabilidades encontradas durante el proceso de la auditoria, además de que ahí se describirán a profundidad las mitigaciones que se proponen que se apliquen para que el sistema auditado tenga una mejor seguridad en la información.

Así como también se especifican los controles adiciones de CIS control a aplicar para que en conjunto con las mitigaciones la seguridad sea mayor.

Dicho informe se decidió poner en un anexo para que no se presenten confusiones al momento de leerlo.

UACM Universidad Autónoma de la Ciudad de México NADA HUMANO ME ES AJENO	**INFORME TÉCNICO DE AUDITORIA**	Informe Nº: 1 Fecha: 2024/11/23
Centro:	Laboratorio de telecomunicaciones en Universidad Autónoma de la Ciudad de México, plantel Casa Libertad	
Titulo:	Auditoria informática	

OBJETIVOS DE LA AUDITORIA
• Definir y delimitar el sistema a auditar y los recursos necesarios para llevar la auditoria de manera eficiente. • Identificar las amenazas y vulnerabilidades encontradas en el sistema. • Identificar con que normativas y estándares cumple la UACM para los sistemas de información. • Identificar que tan riesgosos son los resultados obtenidos. • Proponer las posibles mitigaciones a las amenazas y vulnerabilidades encontradas.

ALCANCE DE LA AUDITORIA
Analizar las amenazas y vulnerabilidades de los servidores de la red interna en el laboratorio de telecomunicaciones para generar informes sobre los resultados de los escaneos.

AUDITOR LIDER
Oscar René Valdez Casillas

EQUIPO AUDITOR
Ana Laura García Victorino

DESARROLLO DE LA AUDITORIA

Durante el proceso de auditoria se realizó el escaneo al servidor ya establecido, usando softwares como herramientas de escaneo, los cuales son Zenmap, Scuba y OWASP.
Se obtuvieron los informes en los cuales se pudieron evaluar las amenazas que se presentaron y su grado de criticidad, constatando los resultados en el presente informe.

HALLAZGOS		
Escaneo con Zenmap Sitio 192.168.1.210		
1	Tipo de hallazgo: Descripción:	Falsificación de solicitud entre sitios. (ID CWE 352) La aplicación web no verifica, o no puede verificar, de manera suficiente si el usuario que envió la solicitud proporciono intencionalmente una solicitud bien formada, valida y consistente.
2	Tipo de hallazgo: Descripción:	Falla del mecanismo de protección. (ID CWE 693) El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.
3	Tipo de hallazgo: Descripción:	Restricción inadecuada de capas. (ID CWE 1021) La aplicación web no restringe o restringe incorrectamente los objetos de marco o capas de UI que pertenecen a otra aplicación o dominio, lo que puede generar confusión en el usuario sobre con que interfaz esta interactuando.
4	Tipo de hallazgo: Descripción:	Archivo oculto encontrado. (ID CWE 538) El servidor coloca información confidencial en archivos o directorios a los que pueden acceder los actores que tienen permiso para acceder a los archivos, pero no a la información confidencial.
5	Tipo de hallazgo: Descripción:	Exposición de información confidencial a un autor no autorizado. (ID CWE 200) El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.
6	Tipo de hallazgo: Descripción:	Obtener publicación. (ID CWE 16) Las debilidades en esta categoría generalmente se introducen durante la configuración del software.
7	Tipo de hallazgo: Descripción:	Validación de entrada incorrecta. (ID CWE 20) El servidor recibe entrada o datos, pero no valida o validad incorrectamente que la entrada tenga las propiedades necesarias para procesar los datos de forma segura y correcta.
Escaneo con Zenmap Sitio 192.168.1.107:3000 y 172.18.12.70:3000		
8	Tipo de hallazgo: Descripción:	Falla del mecanismo de protección. (ID CWE 693)

		El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.
9	Tipo de hallazgo: Descripción:	Archivo oculto encontrado. (ID CWE 538) El servidor coloca información confidencial en archivos o directorios a los que pueden acceder los actores que tienen permiso para acceder a los archivos, pero no a la información confidencial.
10	Tipo de hallazgo: Descripción:	Exposición de información confidencial a un actor no autorizado. (ID CWE 200) El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.
Escaneo con Zenmap Sitio 192.168.1.137		
11	Tipo de hallazgo: Descripción:	Falla del mecanismo de protección. (ID CWE 693) El servidor no utiliza o utiliza incorrectamente un mecanismo de protección que proporcione suficiente defensa contra ataques dirigidos contra el servidor.
12	Tipo de hallazgo: Descripción:	Restricción inadecuada de capas. (ID CWE 1021) La aplicación web no restringe o restringe incorrectamente los objetos de marco o capas de UI que pertenecen a otra aplicación o dominio, lo que puede generar confusión en el usuario sobre con que interfaz esta interactuando.
13	Tipo de hallazgo: Descripción:	Exposición de información confidencial a un autor no autorizado. (ID CWE 200) El servidor expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.
Escaneo con Scuba sitio 192.168.1.210		
14	Tipo de hallazgo: Descripción:	Cuentas anónimas existentes. Permiten inicios de sesión predeterminados y estos permisos a veces pueden ser utilizados por otros usuarios. Compruebe si existen usuarios sin nombre.
15	Tipo de hallazgo: Descripción:	Los nombres de host de los usuarios contienen comodines. Compruebe si los nombres de host de los usuarios contienen un comodín.
16	Tipo de hallazgo: Descripción:	Usuario de base de datos existentes con contraseña en blanco (CIS MySQL 5.7) Compruebe si existen usuarios de la base de datos con contraseñas en blanco.
17	Tipo de hallazgo: Descripción:	La opción de archivo local no está deshabilitada. Compruebe si la opción local_infile está configurada en ON.
18	Tipo de hallazgo: Descripción:	SSL_TYPE la opción no está configurada como necesaria para usuarios remotos. Compruebe si la opción de tipo SSL está configurada en cualquiera, X50% o especificado para todos los usuarios.
19	Tipo de hallazgo:	Base de datos de prueba existente.

	Descripción:	Compruebe si existe la base de datos 'test'.
20	Tipo de hallazgo: Descripción:	Contraseña predeterminada, la opción lifetime esta deshabilitada o configurada en 91 o superior. Compruebe si la opción de duración de la contraseña predeterminada esta deshabilitada (0) o establecida en 91 o superior.
21	Tipo de hallazgo: Descripción:	La opción de modo sql no está establecido en 'ESTRICTO TODAS LAS TABLAS' Compruebe si la opción 'modo sql' no contiene el valor 'STRICT ALL TABLES'

RECOMENDACIONES	
192.168.1.210	
1	1. Bibliotecas o frameworks: utilizar una biblioteca o un marco aprobado que no permita que ocurra esta debilidad o que proporcione construcciones que hagan que sea más fácil evitarla. Asegurarse de que la aplicación esté libre de problemas de secuencias de comandos entre sitios, porque la mayoría de las defensas CSRF se pueden eludir mediante secuencias de comando controladas por el atacante. 2. Generar un numero único para cada formulario, colocarlo en el formulario y verificar al recibirlo. Asegurarse de que el número no sea predecible. 3.Identificar operaciones especialmente peligrosas. Cuando el usuario realiza una operación peligrosa, enviar una solicitud de confirmación por separado para garantizar que el usuario tenía la intención de realizar esa operación. 4.Utilizar el método de "cookie de doble envió" descrito por Felten y Zeller: cuando un usuario visita un sitio, el sitio debe generar un valor pseudoaleatorio y configurarlo como una cookie en la máquina del usuario. El sitio debe exigir que cada envío de formulario incluya este valor como valor de formulario y también como valor de cookie. Cuando se envía una solicitud POST al sitio, la solicitud solo debe considerarse valida si el valor del formulario y el valor de la cookie son iguales. 5. No utilizar el método GET para ninguna solicitud que active un cambio de estado: verificar el encabezado HTTP Refer para ver si la solicitud se originó desde una página esperada. Esto podría, interrumpir la funcionalidad legítima, ya que los usuarios o servidores proxy puede haber deshabilitado el envío del Refer por razones de privacidad. [20], [21]
2	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidades significativamente diferentes de las que se pretende prevenir. [20]
3	El uso de X-Frame-Options permite a los desarrolladores de contenido web restringir el uso de aplicación en forma de superposiciones, marcos o iFrames. Un desarrollador puede utilizar un script "frame-breaker" en cada página que no debe de estar enmarcada. Esto resulta muy útil para los navegadores antiguos que no admiten la función de seguridad X-Frame-Options mencionada anteriormente. Esta técnica de defensa en profundidad se puede utilizar para evitar el uso indebido de marcos en aplicaciones web. Priorizar las fuentes validas de datos que se cargaran en la aplicación mediante el uso de políticas declarativas. [20]
4	No exponer información de archivos y directorios al usuario. [20]
5	Dividir el sistema en compartimentos para tener áreas "seguras" donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura.

	Asegurarse de que se incorpore una compartimentación adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios. [20]
6	NOTA: Esta entrada es una categoría, pero varias fuentes la asignan de todos modos, a pesar de la orientación de CWE de que no se deben asignar categorías. En este caso, no hay debilidades claras de CWE que se puedan utilizar. [20]
7	Utilizar técnicas como: 1.Reducción de la superficie. 2.Bibliotecas o Frameworks. 3.Reducción de la superficie de ataque. 4.Validación de entrada. [20], [21]

192.168.1.107:3000 y 172.18.12.70:3000	
8	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir. [20]
9	No exponer información de archivos y directorios al usuario. [20]
10	Dividir el sistema en compartimentos para tener áreas “seguras” donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentación adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios. [20]

192.168.1.137	
11	NOTA: el concepto de mecanismos de protección está bien establecido, pero sus fallos no se han estudiado exhaustivamente. Se sospecha que los mecanismos de protección pueden tener tipos de debilidad significativamente diferentes de las que se pretende prevenir. [20]
12	El uso de X-Frame-Options permite a los desarrolladores de contenido web restringir el uso de aplicación en forma de superposiciones, marcos o iFrames. Un desarrollador puede utilizar un script “frame-breaker” en cada página que no debe de estar enmarcada. Esto resulta muy útil para los navegadores antiguos que no admiten la función de seguridad X-Frame-Options mencionada anteriormente. Esta técnica de defensa en profundidad se puede utilizar para evitar el uso indebido de marcos en aplicaciones web. Prioriza las fuentes validas de datos que se cargaran en la aplicación mediante el uso de políticas declarativas. [20]
13	Dividir el sistema en compartimentos para tener áreas “seguras” donde se puedan establecer límites de confianza inequívocos. No permitir que los datos confidenciales salgan del límite de confianza y siempre tenga cuidado al interactuar con un compartimiento fuera del área segura. Asegurarse de que se incorpore una compartimentación adecuada en el diseño del sistema y que esta permita reforzar la funcionalidad de separación de privilegios. [20]

SCUBA 192.168.1.210	
14	Verificar y eliminar cuentas anónimas
15	Verificar si los usuarios tienen un comodín (%) en el nombre de host.
16	Para cada fila devuelta del procedimiento de auditoría, establezca una contraseña para el usuario dado utilizando la siguiente declaración (como ejemplo) ESTABLECER LA CONTRASEÑA PARA <usuario>@<host><borrar contraseña” NOTA: Remplace <usuario>, <host> y <contraseña clara> con los valores apropiados.

17	Agregar la siguiente línea a la sección [mysqld) del archivo de configuración de MySQL y reinicie el servidor MySQL: local-infile=0
18	Utilizar la declaración GRANT para requerir el uso de SSL. Uso de GRANT en mi usuario@app1.example.com REQUIRE SSL. Tener en cuenta que REQUIRE SSL solo aplica SSL. Hay opciones como REQUIRE X509, REQUIRE ISSUER, REQUIRE SUBJET pueden utilizarse para restringir aún más las opciones de conexión.
19	Eliminar la base de datos de prueba.
20	Realizar las siguientes acciones: Establecer global duración de contraseña predeterminada de 90 y en el archivo de configuración: contraseña predeterminada lifetime-90 Como parte de la instalación y planificación, considere establecer una política de vencimiento para usuarios específicos. Esto tendrá prioridad sobre la configuración especificada en la duración de la contraseña predeterminada. Por ejemplo: Modificar usuario jeffrey@localhost' INTERVALO DE EXPIRACION DE CONTRASEÑA 90 DIAS.
21	Realizar la siguiente acción para corregir esta configuración Agregar STRICT ALL TABLES al modo sql en el archivo de configuración del servidor.

A continuación, se indicarán los CIS controls que se propone que se implementen para complementar la seguridad del servidor auditado.

192. 168.1.210	
1	Control 14, sub – control 1.
2	Control 14, sub – control 8.
3	Control 14, sub – control 9.
4	Control 17, sub – control 7.
5	Control 18.
6	Control 18, sub – control 10.
192.168.1.107:3000	
7	Control 12, sub – control 12.
8	Control 13, sub – control 4.
9	Control 14, sub – control 9.
10	Control 16, sub – control 2.
192.168.1.137	
11	Control 12, sub – control 9.
12	Control 14, sub – control 1.
13	Control 14, sub – control 4.
14	Control 14, sub – control 8.
15	Control 15, sub – control 6.
16	Control 17, sub – control 7.
17	Control 17, sub – control 8.
172.18.12.70:3000	
18	Control 12, sub – control 12.
19	Control 13, sub – control 14.
20	Control 14, sub – control 9.
21	Control 16, sub – control 2.
192.168.1.210	
22	Control 4, sub – control 2.

23	Control 4, sub – control 4.
24	Control 7, sub – control 9.
25	Control 8, sub – control 2.
26	Control 8, sub – control 7.
27	Control 14, sub – control 6.
28	Control 18, sub – control 2.

CONCLUSIONES
Durante las pruebas realizadas con Zenmap en la red se encontró solo una vulnerabilidad con grado de criticidad alto la cual es metadatos de la nube potencialmente expuesta, por su lado en el caso del escaneo a la base de datos con Scuba se encontraron 4 las cuales son cuentas anónimas existentes, los nombres de host de los usuarios contienen comodines, en este caso esta se repite y por ultimo usuario de base de datos existentes con contraseña en blanco, las otras vulnerabilidades en la red encontrados durante el proceso de escaneos su grado critico fue medio, bajo o informativos, para todas se propusieron la forma en que estas pueden ser mitigadas al igual que las implementaciones de controles especificados en CIS controls. Con los resultados obtenidos se concluye que la red y los recursos en esta están expuestos, por esto es necesario la implementación de las recomendaciones, así como la realización de auditorías de manera periódica para comprobar que las medidas de seguridad que se toman se estén cumpliendo y funcionando de manera eficiente.

Bibliografía de informe técnico.

[1] CWE, «Enumeración de vulnerabilidades comunes Top 25,» CWE, 15 12 2024. [En línea]. Available: https://cwe.mitre.org/data/definitions.

[2] OWASP, «Serie de hojas de referencia de OWASP,» OWASP, 2024. [En línea]. Available: https://cheatsheetseries.owasp.org. [Último acceso: 20 11 2024].