UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

AUDITORÍA DE CIBERSEGURIDAD Y DETECCIÓN DE VULNERABILIDADES EN PLATAFORMAS DE EDUTAINMENT: UN ENFOQUE PARA LA PROTECCIÓN DE DATOS SENSIBLES Y EL FORTALECIMIENTO DE LA PRIVACIDAD

AUTORES:

PEDRO JOSE ORELLANA JARAMILLO
JONATHAN MARCELO MORAN VELASCO

DIRECTOR:

OMAR GUSTAVO BRAVO QUEZADA

CUENCA-ECUADOR
2025

Autores:

Pedro Jose Orellana Jaramillo
Ingeniero en Ciencias de la Computación.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
porellanaj@est.ups.edu.ec

Jonathan Marcelo Moran Velasco
Ingeniero en Electrónica y Redes de Comunicación.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
Jmoranv9@est.ups.edu.ec

Dirigido por:

Omar Gustavo Bravo Quezada
Doctor en Tecnologías de la Información.
Magister en Gestión de Telecomunicaciones.
obravo@ups.edu.ec

Auditoría de ciberseguridad y detección de vulnerabilidades en plataformas de edutainment: un enfoque para la protección de datos sensibles y el fortalecimiento de la privacidad

AUDITORÍA DE CIBERSEGURIDAD Y DETECCIÓN DE VULNERABILIDADES EN PLATAFORMAS DE EDUTAINMENT: UN ENFOQUE PARA LA PROTECCIÓN DE DATOS SENSIBLES Y EL FORTALECIMIENTO DE LA PRIVACIDAD

1st Pedro Jose Orellana Jaramillo
Maestría de Seguridad de la Información
Universidad Politécnica Salesiana
Cuenca, Ecuador
porellanaj@est.ups.edu.ec

2nd Jonathan Marcelo Moran Velasco
Maestría de Seguridad de la Información
Universidad Politécnica Salesiana
Cuenca, Ecuador
jmoranv9@est.ups.edu.ec

3rd Omar Gustavo Bravo Quezada
Maestría de Seguridad de la Información
Universidad Politécnica Salesiana
Cuenca, Ecuador
obravo@ups.edu.ec

Resumen— **La plataforma de Edutainment se presenta como una solución innovadora para transformar la enseñanza histórica en Ecuador y Latinoamérica, abordando la falta de una comprensión profunda y conectada de los eventos pasados. Sin embargo, la digitalización de la educación conlleva desafíos relacionados con la ciberseguridad, ya que la recopilación de datos sensibles de los usuarios requiere una protección efectiva. Este estudio propone una auditoría de ciberseguridad enfocada en identificar vulnerabilidades y fortalecer la seguridad de la plataforma, garantizando la integridad y confidencialidad de la información personal. A través de métodos como el análisis de vulnerabilidades, pruebas de penetración con herramientas como Nmap, Metasploit y Kali Linux, y la implementación de políticas de seguridad basadas en la norma ISO 27001, se logró identificar múltiples puntos vulnerables y establecer medidas de mitigación eficaces. Los resultados demostraron que un enfoque proactivo y sistemático, incluyendo escaneos de red, auditorías de configuraciones SSH y ataques simulados de fuerza bruta, puede mejorar significativamente la postura de seguridad de la plataforma. La investigación, liderada por el Grupo de Investigación en Cloud Computing, Smart Cities & High Performance Computing (GIHP4C), enfatiza la importancia de integrar la ciberseguridad en las soluciones educativas para asegurar un entorno de aprendizaje digital confiable, atractivo y resiliente frente a nuevas amenazas.**

Keywords— *Edutainment, ciberseguridad, vulnerabilidades, politicas, payloads.*

I. INTRODUCCIÓN

La plataforma de Edutainment promueve la necesidad de transformar la enseñanza a través de la historia, tanto en Ecuador como en Latinoamérica, la cual, no fomenta una comprensión profunda y global, lo que impide ver el pasado como una experiencia compartida. Además, la mayoría de las experiencias históricas disponibles para el público están fragmentadas en silos, lo que limita la visión completa de los eventos históricos y su interconexión.

A través de los años, el auge de la tecnología ha llevado a un incremento significativo en el uso de plataformas de realidad aumentada o realidad virtual, la cual combinada con la educación generan experiencias de aprendizaje más atractivas y efectivas para el ser humano. Estas plataformas permiten a los usuarios acceder a contenidos educativos y actividades interactivas de manera digital, lo que ha llevado a una mayor digitalización y manejo de datos sensibles, incluyendo información personal y de aprendizaje de los usuarios, como nombres, sitios de interés, preferencias de aprendizaje, entre otros.[1]

La auditoría de ciberseguridad y detección de vulnerabilidades surge como una respuesta a las

distintas problemáticas que se desarrollan dentro de las plataformas de educación. Enfocándose en realizar una evaluación de la seguridad e identificando posibles puntos débiles y riesgos de seguridad que podrían poner en peligro la integridad y confidencialidad de los datos sensibles manejados en dichas plataformas. Siendo una parte de la investigación el fortalecer la resistencia de estas plataformas frente a posibles ataques cibernéticos y vulnerabilidades, asegurando que la información confidencial de los usuarios, como datos personales y de aprendizaje, está protegida de manera efectiva.

Por esta razón, la auditoría de ciberseguridad y detección de vulnerabilidades enfocada en la plataforma de Edutainment, pretende realizar evaluaciones periódicas y exhaustivas de la seguridad para identificar y abordar posibles debilidades, fortaleciendo así sus defensas contra posibles amenazas y manteniendo la confianza de los usuarios en la integridad de sus datos mientras participan en actividades educativas y de entretenimiento en línea.[2]

El incorporar la plataforma de Edutainment en la educación es una respuesta efectiva para mantener el interés y la motivación de los estudiantes en el proceso de aprendizaje, es así como surge el Grupo de Investigación en Cloud Computing, Smart Cities & High Performance Computing GIHP4C el cual conformado por docentes y estudiantes realizan investigaciones para enfrentar los retos del actuales de la tecnología de manera creativa y proactiva. [20]

Para el análisis de datos y detección de vulnerabilidades, se utilizaron herramientas clave que facilitaron nuestro proceso.[15] Entre ellas, Nmap, una popular herramienta de código abierto que permite explorar redes, identificar puertos abiertos y detectar posibles vulnerabilidades [16] También se utilizó Metasploit, una plataforma versátil para realizar pruebas de penetración simulando ataques controlados, lo que nos ayudó a evaluar la seguridad de los sistemas.[18] Por último, Kali Linux, una distribución de Linux diseñada para pruebas de seguridad, sirvió como el entorno principal donde se ejecutaron Nmap [19] y Metasploit, integrando todas las herramientas en un solo sistema operativo.

La educación en el ecuador ha crecido durante los últimos años, creando nuevas plataformas que combinan la realidad aumentada y la realidad virtual tal como nos muestra endutainment que ha logrado combinar el entretenimiento con el aprendizaje; sin embargo, esto trae consigo nuevas problemáticas dentro del ámbito de ciberseguridad ya que esta maneja informacion sensible de los usuarios como informacion personal y registros de actividad, entre otros.
El informe de EdTech Hub (2023) nos indica que el 68% de las plataformas educativas en América latina no cumplen con la seguridad básica para la protección de datos provocando que estas plataformas se vuelvan vulnerables a una mayor filtración de datos y ataques cibernéticos.
En nuestro país la situación no es diferente ya que al mismo tiempo que la tecnología avanza conjuntamente con los ataques cibernéticos estos han desarrollado conjuntamente afectar a varios sectores productivos obligando a los usuarios a la suspensión de sus actividades; siendo Ecuador el país con más ataques de phishing en Latinoamérica tal como lo menciona ESET (2023) dentro de los comunicados oficiales emitidos por la empresa evidenciando la falta de compromiso por las empresas dentro de la protección de datos sensibles.
En este contexto, la auditoría de ciberseguridad y la detección de vulnerabilidades son esenciales para identificar, evaluar y mitigar riesgos en las plataformas como Endutainment. Las mismas que nos permiten detectar las vulnerabilidades de una infraestructura digital y reforzar las defensas contra amenazas emergentes garantizando un mejor manejo de la protección de datos.
La urgencia de implementar medidas de protección robustas dentro del ámbito digital es

palpable tal como nos menciona Cybersecurity Ventures (2023) que el costo global del cibercrimen crecerá en 10.5 billones de dólares al 2025.

Es así, que el presente trabajo busca incentivar a un mejor manejo y protección de datos dentro de la plataforma educativa Endutainment, identificando vulnerabilidades e implementando medidas preventivas y correctivas nos permitirá una mayor seguridad e integridad de los datos fortaleciendo la confianza de los usuarios.

II. Objetivo Principal

Desarrollar una auditoría interna de ciberseguridad para la protección de datos y la privacidad de la información, enfocada en evaluar los posibles riesgos y la detección de las vulnerabilidades dentro de la plataforma de Edutainment.

III. Objetivos Secundarios

Realizar un análisis exhaustivo de la plataforma de Edutainment para identificar posibles vulnerabilidades en su infraestructura, aplicaciones y configuraciones.

Llevar a cabo pruebas de penetración controladas para evaluar la resistencia de la plataforma ante posibles ataques cibernéticos y para simular posibles escenarios de ataque.

Definir políticas y procedimientos de seguridad en la plataforma para proteger los datos sensibles de los usuarios y mantener su privacidad.

Trabajar en la implementación de la mejoras y correcciones necesarias para fortalecer la seguridad y privacidad de la información.

Establecer un proceso de monitoreo y evaluación continua de la seguridad de las plataformas de Edutainment para garantizar que se mantenga actualizada y protegida ante nuevas amenazas y desafíos de seguridad.

IV. Antecedentes

A. Topología y Servicios del sistema.

Dentro de esta topología de red simple donde un estudiante actuando como hacker de sombrero blanco, está probando la seguridad de un servidor (cloudcomputing.ups.edu.ec). El estudiante usa una conexión desde su PC para analizar las vulnerabilidades del servidor Apache, todo el tráfico se redirecciona a varios dispositivos, incluyendo un servidor de archivos.[7]

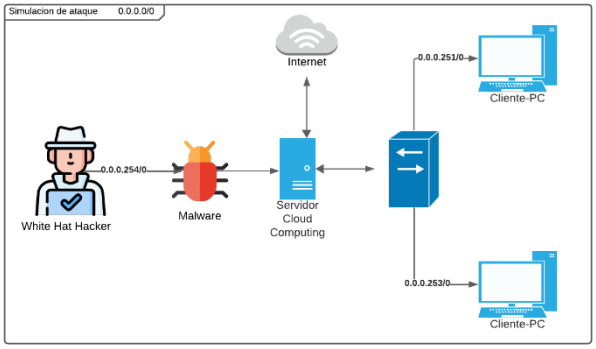


Ilustración 1. Simulación de ataque

Uno de los servicios más importantes es el Protocolo de Transferencia de Hipertexto, conocido como HTTP, y su versión segura, HTTPS. Si estás manejando datos sensibles, como contraseñas o información de tarjetas de crédito, usar HTTPS es un "must". Este protocolo cifra la información mientras viaja por la red, lo que significa que los atacantes tienen mucha más dificultad para interceptarla. Para lograr esto, necesitas instalar certificados SSL/TLS que garanticen que tus conexiones sean seguras.[3]

Los servidores de aplicaciones también son clave en este ecosistema. Estos servidores son responsables de manejar la lógica de negocio de tus aplicaciones, lo que les permite procesar solicitudes complejas y realizar análisis de seguridad. Gracias a lenguajes de programación como Java, Python o PHP, puedes construir aplicaciones que no solo son funcionales, sino que también integran buenas prácticas de

seguridad, como la autenticación de usuarios y el manejo seguro de sesiones.[4]

No podemos olvidar los servidores de bases de datos, que son el lugar donde guardas toda tu información crítica. Utilizando sistemas como MySQL o PostgreSQL, puedes gestionar datos sobre usuarios y configuraciones. Es fundamental implementar controles de acceso y encriptar los datos almacenados para evitar que caigan en manos equivocadas.

Además, el monitoreo constante es esencial para detectar cualquier actividad sospechosa. Aquí es donde entran en juego los sistemas de detección y prevención de intrusos. Estos sistemas pueden alertarte si algo raro está sucediendo, permitiéndote actuar antes de que se convierta en un problema mayor.[8]

Hablando de seguridad, la autenticación robusta es una parte crucial del juego. Usar métodos como la autenticación multifactor (MFA) y protocolos como OAuth 2.0 añade capas extra de protección. Esto asegura que solo los usuarios autorizados puedan acceder a datos sensibles.[5]

Otra cosa importante es tener un plan de respaldo y recuperación de datos. Implementar copias de seguridad regulares significa que si algo sale mal, como un ataque cibernético o un fallo del sistema, puedes recuperar la información sin demasiados problemas. Esto es clave para mantener la continuidad del negocio y proteger tus datos más valiosos.

B. Politicas de seguridad del ambiente virtual.

Las políticas funcionan como un marco que orienta a las organizaciones en la gestión de riesgos. Definen claramente los roles y responsabilidades del personal, así como los procedimientos a seguir para asegurar la información. Una política de seguridad bien estructurada incluye aspectos esenciales como la gestión de contraseñas, controles de acceso, y protocolos para el manejo de incidentes de seguridad.[6]

La importancia de las políticas de seguridad radica en su capacidad para reducir la probabilidad de incidentes de seguridad. Al establecer requisitos claros para contraseñas seguras y la capacitación del personal, las organizaciones pueden mitigar el riesgo de accesos no autorizados. Además, las políticas deben incluir mecanismos de respuesta a incidentes, que son vitales para minimizar el impacto de una brecha de seguridad cuando ocurre.[7]

Además, la conformidad con normativas y estándares de la industria es otra razón fundamental para desarrollar e implementar políticas de seguridad. Muchas organizaciones operan bajo regulaciones específicas que exigen medidas de seguridad. No cumplir con estas normativas puede resultar en sanciones significativas y daños a la reputación de la organización.[9]

Otro aspecto esencial de las políticas de seguridad es su carácter dinámico. A medida que el panorama de amenazas evoluciona, las políticas deben ser revisadas y actualizadas regularmente para abordar nuevas vulnerabilidades y tipos de ataques. Esto implica realizar auditorías y evaluaciones periódicas para asegurar que las políticas sigan siendo efectivas y relevantes.[10]

C. Que son las vulnerabilidades y sus tipos

Cuando hablamos de ciberseguridad, hay varias vulnerabilidades que pueden dar pie a problemas graves si no se manejan adecuadamente. Vamos a ver algunas de las más comunes que todos deberían conocer.

1. **Vulnerabilidades de Software**: Estas son como agujeros en el código de programas y sistemas operativos. Imagina un **buffer overflow**, donde un programa se vuelve loco porque recibe más datos de los que puede manejar. También están las

inyecciones de código, donde los hackers cuelan código malicioso en una consulta SQL para robar información. ¡No queremos eso![12]

2. **Configuraciones Incorrectas**: Muchas veces, las cosas vienen con configuraciones por defecto que no son seguras. Por ejemplo, si un router tiene su contraseña original, es un festín para los atacantes. Siempre hay que revisar y ajustar las configuraciones de seguridad de cualquier dispositivo o software que usemos.[13]

3. **Falta de Actualizaciones**: No actualizar el software es como dejar la puerta de tu casa abierta. Los parches de seguridad son vitales para arreglar fallos conocidos que pueden ser aprovechados por hackers. Mantenerse al día con las actualizaciones es esencial.[11]

4. **Autenticación Inadecuada**: Las contraseñas débiles son un imán para los hackers. Si usamos contraseñas fáciles o no aplicamos la autenticación multifactor (MFA), estamos abriendo la puerta a intrusos. Siempre es mejor usar contraseñas fuertes y activar la MFA.[14]

5. **Ingeniería Social**: A menudo, los problemas no vienen del software, sino del comportamiento humano. Los ataques de ingeniería social, como el phishing, juegan con nuestra confianza para obtener información sensible. La educación sobre estos temas es clave para proteger a los usuarios. [17]

6. **APIs Inseguras**: Si las APIs no están bien protegidas, pueden permitir a los hackers acceder a datos o realizar acciones no autorizadas. Es esencial aplicar controles de seguridad en estas interfaces para mantener la información a salvo.

7. **Falta de Monitoreo y Respuesta a Incidentes**: Si no hay un buen sistema de monitoreo, podríamos tardar en detectar un ataque. Tener herramientas de detección de intrusiones y un plan de respuesta bien preparado puede marcar la diferencia.

V. REVISIÓN DE LA LITERATURA

1. "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua – Ecuador" [25]
Resumen: Este estudio combina el marco de control en ciberseguridad de la norma ISO27032:2012 y la metodología MAGERIT v3.0 para identificar áreas de afectación en aplicaciones web educativas y propone salvaguardas para mitigar riesgos de seguridad.

2. "Programa de auditoría de seguridad en redes sociales y plataformas digitales" [26]
Resumen: Este programa ofrece un enfoque estructurado para implementar auditorías que evalúen la efectividad de las políticas y controles de seguridad en redes sociales y plataformas digitales.

3. "Auditoría de ciberseguridad: claves para la protección digital empresarial" [27]
Resumen: Este artículo destaca la importancia de las auditorías de ciberseguridad como medio para detectar vulnerabilidades, medir el nivel de exposición a riesgos y establecer estrategias preventivas en entornos digitales empresariales.

4. "Plan de ciberseguridad para educación básica ecuatoriana contra ciberataques" [28]
Resumen: Este artículo propone un esquema para elaborar un plan de ciberseguridad destinado a frenar los ciberataques en la educación en línea,

detallando su desarrollo, implementación y retroalimentación para mantenerlo actualizado.

5. "Ciberseguridad en la educación digital: desafíos del aprendizaje remoto" [29]
Resumen: Este artículo aborda los riesgos cibernéticos en entornos educativos digitales y sugiere estrategias como auditorías periódicas para identificar y corregir vulnerabilidades en plataformas y redes educativas.

6. "La importancia de la ciberseguridad en la educación" [30]
Resumen: Este artículo explora los riesgos cibernéticos comunes en instituciones educativas debido a la adopción de nuevas tecnologías y ofrece estrategias para crear entornos de aprendizaje en línea seguros.

7. "La importancia de la educación en ciberseguridad para niños" [31]
Resumen: Este estudio indica que la educación temprana en ciberseguridad fomenta habilidades críticas en los niños, permitiéndoles reconocer y manejar riesgos en línea de manera efectiva.

8. "Seguridad en plataformas educativas basado en 4 conceptos"
Resumen: Este artículo ofrece consejos prácticos para el uso seguro de plataformas educativas, enfocándose en aspectos clave de seguridad para proteger la información y garantizar un entorno de aprendizaje seguro.

9. "**Estrategia Nacional de Ciberseguridad de Ecuador"** [32]
Resumen: Este documento oficial detalla la estrategia nacional de Ecuador en materia de ciberseguridad, incluyendo formación y educación para garantizar que las personas posean las habilidades adecuadas para protegerse en el entorno digital.

10. "Auditoría de ciberseguridad: guía definitiva desde cero"
Resumen: Este curso práctico ofrece una guía paso a paso para aprender sobre auditorías de ciberseguridad, proporcionando conocimientos fundamentales para implementar evaluaciones de seguridad efectivas.

11. "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua – Ecuador" [33]
Resumen: Este estudio desarrolla un procedimiento de gestión de seguridad para plataformas educativas, con el objetivo de reducir vulnerabilidades y riesgos de ciberseguridad en institutos tecnológicos superiores públicos.

12. "Ecuador necesita formar a más profesionales en ciberseguridad"
Resumen: Este artículo destaca la posición de Ecuador en el ranking mundial de ciberseguridad y la necesidad de formar más profesionales en el área para fortalecer la seguridad digital en el país.

13. Auditoría de plataformas educativas
Resumen: Este artículo analiza los riesgos y sanciones asociados con el uso de soluciones digitales en la nube por parte de instituciones educativas, enfatizando la importancia de auditorías para garantizar la protección de datos.

14. "La cibercriminalidad sube un 151% en los últimos cinco años" [34]
Resumen: Este artículo reporta el aumento significativo de la cibercriminalidad en Valladolid, destacando la importancia de la formación en riesgos digitales y la implementación de medidas de seguridad.

16. "Análisis de ciberseguridad en plataformas e-learning: revisión sistemática" [35]
Resumen: Este estudio realiza una evaluación exhaustiva de la seguridad de la información en plataformas de aprendizaje en línea, identificando riesgos y vulnerabilidades, y

proponiendo medidas para fortalecer la protección de datos en entornos educativos digitales.

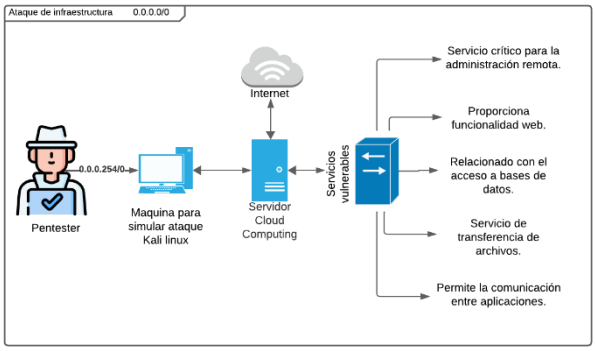
17. "Ley Orgánica de Protección de Datos Personales" [36]
Resumen: Esta legislación ecuatoriana tiene como objetivo garantizar el derecho a la protección de datos personales, estableciendo principios, derechos y obligaciones para el tratamiento adecuado de la información personal en diversos sectores, incluyendo el educativo.

18. "Reglamento General a la Ley Orgánica de Protección de Datos Personales" [37]
Resumen: Este reglamento complementa la Ley Orgánica de Protección de Datos Personales en Ecuador, detallando procedimientos y directrices para el tratamiento seguro de datos personales, aplicables a instituciones educativas que manejan información sensible de sus usuarios.

VI. METODOLOGÍA

A. *Procedimiento de ejecución.*

El proceso de ejecución para la auditoría de ciberseguridad de la plataforma de Edutainment se formó con un análisis exhaustivo de la plataforma para identificar vulnerabilidades en su infra- estructura, aplicaciones y configuraciones (OE1). Una vez identificadas las debilidades del sistema, se definieron políticas y procedimientos de seguridad para proteger los datos de los usuarios y su privacidad (OE2). A continuación, se llevó a cabo pruebas de penetración controladas para evaluar la resistencia de la plataforma ante posibles ataques cibernéticos y simular diferentes escenarios de ataque (OE3). Con base en los resultados de las pruebas, se trabajó en la implementación de mejoras y correcciones para fortalecer la seguridad y privacidad de la información en la plataforma (OE4). Finalmente, se estableció un proceso de monitoreo y evaluación continua para garantizar que la plataforma se mantenga actualizada y protegida frente a nuevas amenazas de seguridad (OE5).



B. *Metodos, tecnicas e instrumentos para recoleccion de datos y medicion.*

Entre los distintos métodos, técnicas e instrumentos que se utilizaran para la recolección de datos y medición dentro de la plataforma se definió los siguientes.

Para el Objetivo Especifico número 1 se utilizó el método de análisis de vulnerabilidades y escaneo de red, haciendo uso de los instrumentos para el escaneo y análisis de vulnerabilidades, como Nmap y Kali Linux, para identificar puertos abiertos, servicios y posibles debilidades en la configuración de la plataforma.

En el segundo Objetivo Especifico se usó el método de revisión de políticas y documentos de seguridad, utilizando las técnicas de análisis para políticas de seguridad y la revisión de normativas de protección de datos (por ejemplo, GDPR), como guías de buenas prácticas en ciberseguridad.

El Objetivo Especifico número 3 tendrá como método las pruebas de penetración controladas (ethical hacking), en la cual haciendo uso de la herramienta de Metasploit se simulo ataques

cibernéticos controlados para probar la resistencia de la plataforma.

El cuarto Objetivo Especifico se manejó el método de implementación de políticas de seguridad y correcciones. Utilizando las mejores prácticas en ciberseguridad y las recomendaciones de organizaciones reconocidas como: NIST, ISO

Y el ultimo Objetivo Especifico sería el monitoreo y evaluación continua de la seguridad utilizando instrumentos tales como: análisis de archivos logs o soluciones de prevención y detección de intrusos (IDS/IPS).

VII. RESULTADOS

En esta sección se presentan los resultados obtenidos en el análisis de ciberseguridad, utilizando herramientas como **Nmap** para el descubrimiento de puertos abiertos y **Metasploit** para la explotación de vulnerabilidades. Mediante **Nmap**, se identificaron los servicios activos en los sistemas analizados, y con **Metasploit** se intentó explotar las vulnerabilidades detectadas. Sin embargo, a pesar de los intentos realizados, no se logró explotar ninguna vulnerabilidad, lo que resalta la robustez de las medidas de seguridad implementadas en el sistema del grupo de investigación de **Cloud Computing,** así como en el servidor dedicado.
Adicionalmente, se revisaron y aplicaron diversas políticas de seguridad que contribuyeron a fortalecer la protección del sistema. Los procesos utilizados, tanto en la identificación de posibles vulnerabilidades como en los intentos de explotación controlada, dando como resultado que estas prácticas han permitido reforzar el sistema ante posibles amenazas y elevando su nivel de resistencia frente a ataques externos.

A. Búsqueda de información de vulnerabilidades del sistema

Durante nuestro análisis de ciberseguridad, se identificó una potencial vulnerabilidad en una aplicación visible al público desde internet: **Edutainment UPS**.

1) Disponibilidad en la Play Store: Edutainment UPS.

La aplicación **Edutainment UPS**, enfocada en ofrecer contenido educativo interactivo, está fácilmente accesible en la Play Store. Aunque esto facilita que los usuarios la descarguen, también abre la puerta a riesgos si no se ha revisado bien el código antes de lanzarla. La disponibilidad pública siempre implica tener medidas de seguridad en el código y en el manejo de datos.

2) *Contacto personal relacionado a la aplicación*

El encargado de la aplicación es **Vinicio Veletanga**, quien también tiene otros proyectos bajo su responsabilidad. Por lo que estos proyectos públicos, contiene datos sensibles como la educación, es importante que los desarrolladores mantengan buenos hábitos de seguridad. Además, siempre es recomendable hacer una auditoría de los proyectos previos que el desarrollador haya publicado para asegurarse de que sigue buenas prácticas.

3) *Repositorio público de Github*

Aunque **Edutainment UPS** no tiene un repositorio público directo, se encontró un repositorio ***Repositorio-GitHub-Developer***, también relacionado con el mismo contacto. Por lo que es esencial que los desarrolladores protejan estos repositorios de posibles vulnerabilidades o fugas de información. Exponer código o datos sensibles en un repositorio público puede atraer a

actores maliciosos, por lo que este tipo de acceso debe manejarse con precaución. El enlace al repositorio ha sido ofuscado por seguridad.

https://github[.]com/usuario/proyecto

4) ***Acceso sin credenciales***

El acceso a la aplicación **AR Edutainment UPS** se realiza simplemente presionando el botón de **Login**, lo que nos permitió examinar el flujo de autenticación. Dado que estos datos están expuestos públicamente y no hay barreras significativas en el acceso inicial, podría representar una gran vulnerabilidad para el sistema si no se implementan controles de seguridad adecuados.

A. Evaluación comparativa de herramientas.

Herramienta	**Pros**	**Contras**	**Precio**
Nmap	Excelente para escaneo de redes y detección de puertos abiertos; fácil de usar.	No detecta vulnerabilidades específicas; limitado a descubrimiento de red.	Open Source
Metasploit	Potente para explotación de vulnerabilidades; amplia base de datos de exploits.	Complejo de utilizar sin experiencia; puede ser peligroso si no se usa correctamente.	Open Source (Community), de pago (Pro)
OpenVAS	Enfoque en escaneo de vulnerabilidades; análisis detallado de amenazas.	Configuración y uso inicial pueden ser complejos; necesita recursos significativos.	Open Source
Wireshark	Análisis en tiempo real de tráfico de red; excelente para redes internas.	Limitado a redes internas; no diseñado para detección de vulnerabilidades de seguridad.	Open Source

Tabla 1. Comparación de Herramientas

Nmap fue elegido porque es excelente para descubrir dispositivos en la red y escanear puertos abiertos, lo cual resulto en la resolución del servidor a través del análisis, aunque no identifica vulnerabilidades detalladas. Metasploit, en cambio, es potente para realizar pruebas de explotación y encontrar vulnerabilidades específicas, aunque es algo complejo y requiere cierta experiencia para no cometer errores. Wireshark fue usado de manera limitada debido a su enfoque en análisis de tráfico de redes internas, que no cubría nuestras necesidades externas en esta auditoría de seguridad. OpenVAS fue una opción valiosa para realizar un análisis más exhaustivo de vulnerabilidades en la red, pero su configuración inicial requiere tiempo y más recursos, lo cual no estaba previsto en este caso. En el futuro, se ha decido incluir herramientas que permitan una evaluación cuantificable de las vulnerabilidades detectadas que ayudarían a optimizar los resultados de una manera más efectiva en contextos de seguridad.

B. Puertos vulnerables encontrados usando la herramienta NMAP

El análisis de la seguridad de los servicios expuestos en el servidor se realizó mediante un escaneo de puertos con Nmap, una herramienta ampliamente utilizada en el ámbito de la ciberseguridad. El objetivo de este escaneo fue identificar los servicios activos y su

configuración, así como evaluar posibles vulnerabilidades asociadas a estos.

Número de Puerto	Protocolo	Servicio	Descripción
Puerto 1	TCP	Servicio X	Servicio crítico para la administración remota.
Puerto 2	TCP	Servicio Y	Proporciona funcionalidad web.
Puerto 3	TCP	Servicio Z	Relacionado con el acceso a bases de datos.
Puerto 4	TCP	Servicio A	Servicio de transferencia de archivos.
Puerto 5	TCP	Servicio B	Permite la comunicación entre aplicaciones.

Tabla 2. Descripción de Puertos

Este comando permitió identificar no solo los puertos abiertos, sino también las versiones de los servicios que se estaban ejecutando. Se observó que varios de estos servicios pueden ser susceptibles a vulnerabilidades conocidas, lo que resalta la necesidad de mantenerlos actualizados y debidamente configurados.

C. Explotación de vulnerabilidades y uso de Payloads mediante Metaslpoit

En el presente estudio, se utilizó un enfoque sistemático para identificar y explotar potenciales vulnerabilidades en una aplicación web objetivo. El proceso comenzó con la clonación de un repositorio que contiene listas de recursos útiles para pruebas de penetración utilizando el siguiente comando:

git clone https://github.com/danielmiessler/SecLists.git

A continuación, se llevó a cabo un escaneo inicial utilizando **Feroxbuster**, una herramienta para descubrir directorios y archivos ocultos en la web:

feroxbuster --url [URL]

Se instaló un conjunto de listas para realizar búsquedas más específicas, repitiendo el escaneo con directorios medios listados en un archivo designado:

install seclists
feroxbuster --url [URL] SecLists/Discovery/Web-Content/raft-medium-directories.txt

Asimismo, se utilizó **Gobuster** para identificar directorios comunes y archivos en la aplicación web, empleando listas predefinidas:

gobuster dir -u [URL] -w SecLists/Discovery/Web-Content/common.txt
gobuster dir -u [URL] -w SecLists/Discovery/Web-Content/raft-medium-files-lowercase.txt > raft-medium-files-lowercase.txt

Para realizar un análisis más exhaustivo de las configuraciones de SSH, se clonó un repositorio especializado y se ejecutó el script correspondiente:

git clone https://github.com/sodomak/sshenum.git
python3 sshenum.py rhost[URL]:[PUERTO] -w wordlist.txt

Finalmente, se llevó a cabo un ataque de fuerza bruta utilizando **Hydra** para intentar acceder a la

interfaz SSH del servidor, empleando una lista de contraseñas de gran volumen:

hydra -l [USUARIO] -P SecLists/Passwords/xato-net-10-million-passwords-100000.txt [URL] -s [PUERTO] -t 4 [SERVICIO]

Estos métodos demostraron ser eficaces en la identificación de puntos vulnerables en la aplicación, destacando la importancia de la detección proactiva de vulnerabilidades en entornos web.

D. Corrección de vulnerabilidades mediante la implementación de políticas de seguridad.

En la siguiente sección se detallan las políticas a utilizar para la corrección de vulnerabilidades en el sistema. Estas políticas están diseñadas para abordar diversas amenazas que podrían comprometer la seguridad y funcionalidad de la infraestructura tecnológica. Al implementar medidas adecuadas, se busca no solo mitigar los riesgos actuales, sino también fortalecer el entorno de seguridad a largo plazo. La correcta adopción de estas políticas será esencial para garantizar la integridad, disponibilidad y confidencialidad de la información gestionada por la organización.

a) POLITICAS DE RESPALDO DE LA INFORMACIÓN

Es responsabilidad del grupo de investigación en Cloud Computing, Smart Cities & Perfomance computing GIHP4C dar cumplimiento al procedimiento de respaldo de información, en donde se establezca acciones sobre como respaldar la información digital y física.
Dichas buenas prácticas de respaldo de información se establecen en la ISO 27001 en la subsección de dominios A5 Políticas de seguridad de la información. [21]
Se detalla políticas establecidas para su aplicación.

Para la ubicación del respaldo:

- Los respaldos deberán estar en servidores independientes a los servidores de producción en el Datacenter principal o a su vez buscar mecanismos de respaldos en nube.
- La ubicación del respaldo de la base de datos y los sistemas de producción o pruebas deberán mantenerse respaldados y ubicarse en un Datacenter alterno o nube que cumpla con las características de: redundancia de energía, climatización, telecomunicaciones, espacios adecuados, ingreso mediante huella, videovigilancia y sistema de intrusión; basada en la norma en la norma Los estándares ANSI/EIA/TIA 606, 607 y 942 especifican los requerimientos mínimos para la infraestructura de telecomunicaciones, cableado estructurado, y cuartos de cómputo o data centers, entre otros estándares.

Para el acceso a las instalaciones de acceso a los servidores

- Los respaldos físicos de información deberán estar ubicado en un lugar con las capacidades necesarias para el almacenamiento con medidas de seguridad contra incendios e ingreso de personal no autorizado.
- El acceso para validar dicha información deberá estar debidamente autorizada y registrada
- El personal a cargo de las seguridades físicas estará a cargo de asignación y configuraciones de acceso a dicha

ubicación únicamente con el registro de huella digital.
- Para acceso a la ubicación física de los servidores solo se permitirá el acceso mediante claves de acceso entregadas por el personal autorizado para acceder a trabajar en este sitio y una vez culminada las actividades es obligación de la persona responsable dejar con las seguridades correspondientes.

Para respaldos de información física:

- Los respaldos físicos deberán almacenado, escaneado y codificados al etiquetamiento de información realizada por el departamento de sistemas.
- El etiquetado de la información física será en base al proceso de clasificación de información

Para respaldos de información digital:

El respaldo de toda la información deberá ser evaluada en base a la matriz de gestión de riesgos. Esto criterios serán evaluados según su confidencialidad, integridad y disponibilidad. La frecuencia de respaldo será basada en la valorización del activo calcula en la matriz de riesgos:

- En caso del VA sea bajo, la frecuencia de respaldo será de manera semestral
- En caso de VA se medió, la frecuencia de respaldo será de manera trimestral
- En caso del VA se alto, la frecuencia de respaldo será de manera mensual o diaria.
- Dicho análisis debe tener el departamento de sistemas para proceder con los respaldos necesarios en los sistemas de producción.

Para respaldo de datos de producción y pruebas:

- El respaldo de la base de datos principal deberá respaldar en tiempo real la información todos los cambios que mantiene dicho acceso (Configuraciones, Cambios, Transacciones, entre otros)
- El seguimiento del funcionamiento de la estructura contingente y el respaldo de datos deberá ser liderado por el departamento de sistemas y deberá informarse de manera mensual mediante un informe con las novedades pertinentes.
- El respaldo de la base de pruebas deberá estar almacenado en un disco externo y en custodia del departamento, según la valorización de activos se asignará la frecuencia.

Para respaldos de servidores de producción:

- El administrador de la plataforma debe mantener respaldada la información de servidores en el Datacenter alterno mediante las configuraciones necesarias para el funcionamiento
- El departamento de sistemas gestionara la disponibilidad de equipamiento necesario para la escalabilidad de respaldos de información.

Procedimiento

1. Ejecutar el proceso de gestión de riesgos de seguridad de la información para detección de los activos críticos, el responsable es el oficial de seguridad de la información
2. Evaluar el resultado mediante la matriz de gestión de riesgos en base a la valoración de activos generando una tabla resumen con detalles analizados correspondientes a respaldos, el responsable es el oficial de seguridad de la información
3. Aplicar las consideraciones de retención para la frecuencia del resguardo y

conservación, el responsable es el departamento de sistemas

4. Ejecutar el procedimiento para el respaldo de la infraestructura tecnológica, asegurando las copias de seguridad en múltiples ubicaciones seguras, el responsable es el departamento de sistemas
5. Almacenar las copias de respaldo en lugares seguros, utilizando mecanismos de cifrado y acceso controlado, el responsable es el departamento de sistemas
6. Controlar los respaldos en cumplimiento procedimiento para el respaldo de la infraestructura tecnológica y a la consideración establecida en el procedimiento, el responsable es el oficial de seguridad de la información
7. Revisar y actualizar periódicamente el respaldo y resguardo, adaptándolos a nuevas amenazas y tecnologías, el responsable es el oficial de seguridad de la información
8. Socializar a todo el personal sobre los lineamientos de respaldo y resguardo de la información, el responsable es el oficial de seguridad de la información

b) POLITICAS DE ACCESOS TECNOLOGICOS

- La responsabilidad del oficial de seguridad de la información enviar las claves en un plazo aproximado de tres días y entregar mediante el correo institucional
- El responsable del oficial de seguridad de la información debe mantener actualizado el instructivo del uso de la plataforma para el manejo de claves (Guía de utilización de caja fuerte de claves), y todos los requirentes deben utilizar esta plataforma para el almacenamiento seguro de contraseñas.
- Los acuerdos de confidencialidad firmados y entregados de manera digital y física deben ser almacenados y custodiados por el departamento legal
- Es responsabilidad del oficial de seguridad de la información establecer y disponer la configuración de estándar para la actualización de claves por un periodo de 90 días.

Dichas buenas prácticas sobre accesos tecnológicos se establecen en la iso 27001 en la subsección de dominios A5 Políticas de seguridad de la información [21]
Los procedimientos de accesos se dividen en dos partes los personal interno y accesos privilegiados

Para los accesos la plataforma se seguirá el siguiente procedimiento

1. Llenar un Formato de acta entrega – recepción de claves y entregar al solicitante, el responsable es el oficial de seguridad de la información
2. Cambiar de forma inmediata todas las claves entregadas, es responsable el personal interno
3. Mantener en custodia las claves entregadas, es responsable el personal interno
4. Guardar las claves generadas en la plataforma de caja fuerte de claves vigente, es responsable el personal interno
5. Monitorear de manera trimestral y detectar si existe novedades reportar un informe con las novedades, es responsabilidad del oficial de seguridad de la información

Para los usuarios privilegiados

1. Firmar el acuerdo de responsabilidades y confidencialidad del manejo de usuarios privilegiados, es responsable el personal interno con el área de talento humano
2. Definir accesos juntamente con el director de sistemas definiendo limitantes para acceder a servidores y bases de datos en uso de la plataforma endutanmeint, es responsable el departamento de sistemas y oficial de seguridad de la información
3. Crear usuarios en servidores de prueba para bases de datos si fuese necesario, es responsable el departamento de sistemas
4. Crear usuarios en servidores con acceso limitados si fuese necesario, es responsable el departamento de sistemas
5. Cambiar de manera inmediata las claves otorgadas, es responsable del usuario con privilegios
6. Mantener en custodia las claves entregadas, es responsable del usuario con privilegios
7. Guardar las claves generadas en la caja fuerte de claves vigente, es responsable del usuario con privilegios
8. Monitorear de manera trimestral y detectar si existe novedades reportar las novedades, es el responsable el oficial de seguridad de la información.

c) POLITICAS DE GESTIÓN DE VULNERABILIDADES

- El escenario del ejercicio práctico anual será definido por el oficial de seguridad de la información previo coordinación con el departamento de sistemas
- Las áreas involucradas en los planes de acciones deben priorizar la gestión para ofrecer una solución de manera prioritaria.
- El acceso a los sistemas críticos durante los ejercicios prácticos debe ser supervisado por el departamento de sistemas y el oficial de seguridad de la información, y debe realizarse fuera del horario laboral.

Es responsabilidad del oficial de seguridad de la información validar lo siguiente:

i. Asegurar que el personal esté cualificado en ciberseguridad, demostrado a través de cursos.
ii. Firmar un acuerdo de confidencialidad sobre las vulnerabilidades detectadas.
iii. Solicitar las vulnerabilidades según el enfoque de caja blanca, caja gris o caja negra, según el alcance del ejercicio:
iv. Mantener las vulnerabilidades en una plataforma que administre y evidencie dichas gestiones por parte de los involucrados.

- La criticidad de las vulnerabilidades debe ser evaluada de forma automatizada y se deben tomar acciones según la escala de riesgos que se maneje por cada empresa.

Si hay actividades que no se pueden completar en un plazo de 6 meses, el oficial de seguridad deberá presentar las gestiones a largo plazo que se llevarán a cabo.
Dichas buenas prácticas de gestión de vulnerabilidades se establecen en la ISO 27001 en la subsección de dominios A5 Políticas de seguridad de la información [21]

1. Identificar equipamiento critico en base al análisis de riesgo, es responsable del oficial de seguridad de la información
2. Generar propuesta de activos críticos a realizar el análisis de vulnerabilidades, es responsable el oficial de seguridad de la información

3. Gestionar la contratación y adquisición de servicios, es responsable el departamento de contrataciones
4. Trabaja en conjunto con el proveedor externo para establecer las etapas que deben completarse durante el ejercicio práctico, el responsable es el departamento de sistemas
5. Evalúa el cronograma presentado, es responsable el oficial de la seguridad de la información
6. Realiza pruebas de penetración en un entorno controlado utilizando un enfoque de evaluación para obtener información. Si se logra obtener información mediante los métodos de caja negra y caja gris, es responsable la empresa especializada
7. Crea un usuario con los privilegios para acceso a la infraestructura, es responsable el departamento de sistemas
8. Controla el funcionamiento del equipo que presta un servicio a los clientes mientras se lleva a cabo la coordinación del ataque, es responsable el departamento de sistemas
9. Comprueba la culminación de todas las actividades especificadas en el cronograma propuesto, es responsable el oficial de la seguridad de la información
10. Entrega documento – Informe de vulnerabilidades detallado los hallazgos encontrados, es responsable la empresa especializada y el oficial de seguridad de la información
11. Establece tareas con distintos plazos (corto, mediano y largo plazo) junto con las personas encargadas de su ejecución, es responsable el oficial de la seguridad de la información

d) POLITICAS DE GESTIÓN DE RIESGOS

El oficial de seguridad de la información será el encargado de elaborar la gestión de riesgos en la infraestructura actual, mediante un análisis de los activos de información, en este se involucra de manera inicial el levantamiento de información actual y, la valorización de cada activo en base a la confidencialidad, disponibilidad y la integridad

Dichos activos mantendrán el análisis de la amenazas y tratamiento de cada activo de información con las medidas que se tomarán para que no se materialice el impacto de la amenaza

Dichas buenas prácticas sobre la clasificación y manejo de información se establecen en la iso 27001 en la subsección de dominios A6 Organización de la seguridad de la información [22]

Procedimiento:

1. Ejecutar plan de gestión de riesgos de seguridad de la información, se aplica la base a la metodología ISO/IEC 27005 y sus prácticas establecidas para tratamiento de riesgos, el responsable es el oficial de seguridad de la información
2. Elaborar plan de acción, se cataloga los activos priorizados en el plan de gestión de riesgos tomando en cuenta fechas y presupuesto para ser presentado a departamento de sistemas en un informe con las medidas de acción a tomar, responsable oficial de seguridad de la información, el responsable es el oficial de seguridad de la información
3. Aprobar plan de acción, se analiza los planes de acción presentado en el informe tomando en cuenta el recurso tiempo y recurso económico para su aprobación, el responsable el departamento de sistemas.
4. Socializar plan de acción, se comunica el plan de acción con las actividades planificadas, el responsable es el oficial de seguridad de la información.
5. Poner en marcha en plan de acción, se desarrolla cada una de las etapas y acciones, citadas en el plan de acción con

el fin de prevenir o a la vez corregir los diferentes riesgos, el responsable es el oficial de seguridad de la información.

6. Monitorear los planes de acción, se verifica la efectividad de los planes ejecutados, evaluando sus resultados mediante un informe de efectividad, el responsable es el oficial de seguridad de la información.

e) POLITICAS DE CLASIFICACION DE INFORMACIÓN

- La lista maestra de documentos del área de procesos será material de trabajo para el análisis de la clasificación de información, esta será actualizada mensualmente.
- El oficial de procesos tiene la responsabilidad de proporcionar el etiquetado de toda la documentación que haya sido revisada y aprobada de manera mensual para la clasificación de la información.
- Las diferentes Áreas que se relacionan como dueños de la información resguardar la misma mediante mecanismos internos provistos
- El usuario en el levantamiento de la información deberá proveer dicha recursos de manera completa sin omitir ningún dato ya que puede ser importante en su momento. Dicha información se debe presentar de manera clara y concisa.
- Es responsabilidad de todos quienes conforman la institución comprometerse y brindar el apoyo al oficial de seguridad de la información en los requerimientos solicitados, en el menor tiempo posible.
- Todo el personal que realice digitalización de información deberá cargar y mantener actualizada, utilizando los parámetros establecidos por el Oficial de Seguridad de la Información en el gestor documental.
- Es responsabilidad del Oficial de la Seguridad de la Información, evaluar y plasmar los resultados en base a los datos obtenidos en las tablas, generando un insumo de trabajo (lista maestra actualizado de manera mensual).

Dichas buenas prácticas sobre el análisis de riesgos se establecen en la ISO 27001 en la subsección de dominios A8 Gestión de activos [23]

Procedimiento

1. Entregar información, se envía mediante correo electrónico información correspondiente a la matriz con inventario de procesos actualizada dentro de los 5 primero días de cada mes, el responsable es el área de procesos
2. Analizar información, se coordina reuniones con jefaturas para determinar qué información es crítica en su puesto de trabajo y como afecta la pérdida de esta información, redactando las decisiones tomadas en un correo electrónico y enviando al encargado del área, el responsable es el oficial de seguridad de la información
3. Distribuir información, se clasifica información de la lista maestra según la recolección de información.
4. Asignar valores, se coloca de acuerdo con criterio del oficial de seguridad de la información en base a la metodología de análisis de riesgos de seguridad de la información ISO/IEC 27005, el responsable es el oficial de seguridad de la información
5. Valorizar información, se obtiene el valor de clasificación de información de acuerdo con la confidencialidad, disponibilidad, integridad y privacidad, el

responsable es el oficial de seguridad de la información

6. Clasificar información, se coloca en la lista maestra de documentos los criterios según el etiquetado de la información en: confidencial, restringido, uso interno y público, el responsable es el oficial de seguridad de la información
7. Capacita sobre clasificación de información, se detalla las políticas de etiquetado al personal de la institución para su etiquetado, el responsable es el oficial de seguridad de la información
8. Reportar novedades del proceso de clasificación, se presenta las novedades dentro del desarrollo del proceso de clasificación de información, el responsable es el oficial de seguridad de la información

f) POLITICAS DE SEGURIDADES EN OPERACIONES

Para una eficiente gestión de versiona miento debe asegurar las siguientes políticas:

- Estén correctamente justificados, registrados, categorizados y documentados.
- Se lleven a cabo sin perjuicio de la calidad del servicio TI y sean cuidadosamente testeados en ambientes de pruebas.
- Cualquier modificación y/o creación de servicios tecnológicos o elementos de configuración, debe seguir de forma obligatoria el proceso para el control de versiona miento.
- No se implementarán cambios si no se han autorizado previamente autorizados.
- Los proveedores externos sólo podrán proponer solicitudes de cambio a través de los especialistas de la Institución.
- El análisis de riesgo e impacto es obligatorio para la gestión de versiona miento.
- Todo cambio debe ser categorizado como normal o emergente, mismo que debe pasar por el conocimiento y autorización de las áreas involucradas.
- Todo cambio emergente debe tener como entrada un incidente asociado como crítico y de solución inmediata.
- Los cambios que sean rechazados o queden pendientes para verificación, deberán tener el estado correspondiente y el motivo por el que se toma la decisión.
- Los cambios deberán tener un tiempo estimado de trabajo y ser notificados al área solicitante.
- Todo cambio y versiona miento del core financiero se debe registrar en la bitácora del área de sistemas

En toda solicitud de cambio se debe realizar una reunión previa entre el jefe del área solicitante, jefe de sistemas con apoyo del oficial de seguridad de la información; una vez analizada la viabilidad del cambio, el solicitante debe gestionar la aprobación para el inicio del desarrollo.

Los responsables del área solicitante deberán socializar los cambios realizados al personal a su cargo.

Dichas buenas prácticas de cambios de versiones se establecen en la ISO 27001 en la subsección de dominios A12 Seguridad de operación [#25#]

Procedimiento

1. Se analiza la factibilidad del cambio y realizar la solicitud de cambios firmarla digitalmente, el responsable es el área solicitante
2. Notificar para autorización, legalización del documento de aprobación, el responsable es el área solicitante
3. Revisar el tipo de solicitud, autorizar o negar la solicitud de cambio, en caso de negar la solicitud de cambio finaliza el

proceso, en caso de aprobar la solicitud continuar con la actividad 4, el responsable es la autoridad competente

4. Notificar la aprobación y definir con el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C las actividades para la programación y los tiempos que tomará su implementación; ajustadas a los requerimientos y criterios técnicos acordados con el personal involucrado. El departamento deberá legalizar la documentación mediante firmas y definir el tiempo aproximado para el desarrollo y/o implementación, el responsable es el departamento de sistemas
5. Desarrollar la programación requerida aplicando los métodos necesarios, y ejecutar las pruebas de desarrollo con el área solicitante, el responsable es el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C
6. Validar pruebas de los cambios realizados con el área solicitante. En caso de que las pruebas cumplan con el requerimiento del área solicitante continuar con la actividad 8, en caso de que no cumplan con el requerimiento proceder a la actividad 7, el responsable es el departamento de sistemas
7. Identificar, desarrollar las mejoras y ajustar a los cambios, evaluar los resultados de acuerdo a los parámetros establecidos en la solicitud de cambios, el responsable es el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C
8. Validar las con el área solicitante las mejoras realizadas. En caso de que las mejoras sean satisfactorias continuar con la actividad 9. En caso de que los cambios realizados no cumplan con los requerimientos, el jefe de sistemas debe analizar con el responsable es el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C las posibilidades de mejora, los responsables son el departamento de tecnología y el responsable es el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C
9. Disponer a el responsable es el grupo de investigación en Cloud Computing, Smart Cities & Perfomance Computing GIHP4C el paso a producción de la nueva versión y registrar en la bitácora digital con el número de solicitud creada
10. Notificar mediante correo electrónico la implementación realizada para que los responsables del área solicitante puedan socializar a sus equipos de trabajo

g) POLITICAS DE GESTION DE INCIDENTES

- Identificar e informar los eventos sucedidos y afectan la operatividad de la plataforma de Edutainment
- Levar un histórico de incidentes repetitivos mismos que debe ser registrados en una bitácora para una fácil validación
- Recolectar información de los eventos mediante logs, monitoreo entre otros

Dichas buenas prácticas de gestión de vulnerabilidades se establecen en la ISO 27001 en la subsección de dominios A16 Gestión de incidentes de seguridad de la información [24]

Procedimiento

1. Informa al departamento de tecnología el evento suscitado en la parte tecnológica, es responsabilidad de todo el personal
2. Elaborar un informe detallando por lo mínimo: objetivos, antecedentes, tiempo de problema, tiempos de respuesta,

personal que intervino en la solución, protocolos de comunicación, planes de acción si se lo necesita, lecciones aprendidas, el responsable es el departamento de tecnología

3. Valoriza el incidente mediante la confidencialidad, disponibilidad e integridad, el responsable es el oficial de seguridad de la información.
4. Elabora informe con detalles y los planes de acción con los responsables para el seguimiento, el responsable es el oficial de seguridad de la información.
5. Monitorear de manera mensual y detectar si existe novedades reportar las novedades, el responsable es el oficial de seguridad de la información.

Vulnerabilidad	**Amenaza**	**Solución**
Contraseña insegura	Acceso al sistema con una contraseña insegura	Al menos 8 caracteres, una letra mayúscula, alfanuméricos y un carácter especial
Sin antivirus	Infección por malware	Instalar antivirus en todos los servidores y validar incidentes
Falta de actualizaciones	Explotación de vulnerabilidades	Actualizar sistemas operativos y paquetería de manera semestral
Acceso no autorizado al servidor	Acceso no autorizado a través de conexiones inseguras	Uso de conexiones autenticadas por IP y credenciales seguras
Falta de registros de acceso	Difícil identificación de accesos no autorizados	Mantener bitácoras de accesos y actividades en el sistema
Sin monitoreo constante	Actividades sospechosas no detectadas a tiempo	Implementar monitoreo integral y continuo de accesos y transacciones

Tabla 3. Identificación de Vulnerabilidades

1) Contraseñas inseguras

Una contraseña débil es una de las principales causas de brechas de seguridad. Para mitigar este riesgo, se ha implementado una expresión regular (RegEx) a nivel de BackEnd que valida que las contraseñas proporcionadas cumplan con requisitos de seguridad mínimos, como longitud, uso de caracteres especiales, mayúsculas, minúsculas y números. Esta estrategia asegura que los usuarios creen contraseñas más seguras, reduciendo el riesgo de ataques de fuerza bruta.

```
@field:Size(min = 8, message = "La contraseña debe tener al menos 8 caracteres")
@field:Pattern(
    regexp = "^(?=.*[a-z])(?=.*[A-Z])(?=.*\\d)(?=.*[@\$!%*?&])[A-Za-z\\d@\$!%*?&]{8,
     }\$",
    message = "La contraseña debe contener al menos una letra mayúscula, una letra
     minúscula, un número y un carácter especial"
)
val password: String
```

Ilustración 2. Prueba de contraseñas

Complejidad de la Contraseña	**Tiempo Estimado para Romperla**
Contraseña básica (mayúsculas y minúsculas)	30 minutos
Complejidad media (mayúsculas, minúsculas, números)	1 año
Mayor complejidad (mayúsculas, minúsculas, números, símbolos)	100 años
Contraseña larga con alta variabilidad	278 años
Contraseña compleja (12+ caracteres, todos los tipos)	10,000 años

Contraseña extremadamente compleja (14+ caracteres, todos los tipos, alta entropía)	1 millón de años
Contraseña de máxima seguridad (16+ caracteres, complejidad total)	46 millones de años

Tabla 4. Complejidad de Contraseñas

Estos valores muestran cómo una combinación de longitud, diversidad de caracteres (mayúsculas, minúsculas, números y símbolos) y alta entropía puede aumentar exponencialmente la seguridad de una contraseña, dificultando su ruptura por ataques de fuerza bruta.

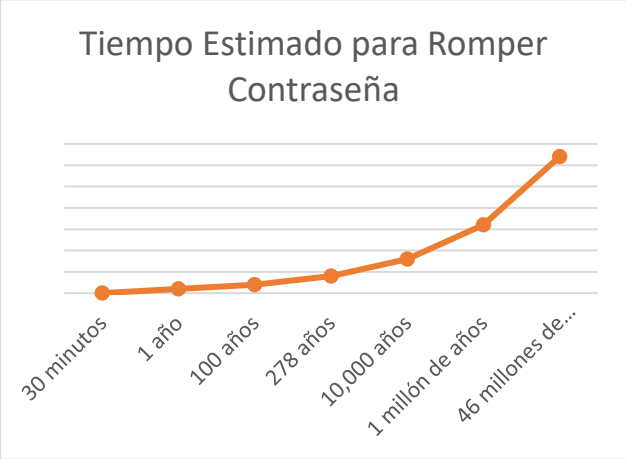


Ilustración 3. Tiempo de solución contraseña

2) *Sin antivirus*

Aunque la falta de un antivirus en un servidor Linux, como Ubuntu, no siempre representa una amenaza crítica, se ha decidido implementar **ClamAV**, un software antivirus de código abierto, como medida adicional. **ClamAV** proporciona escaneo y análisis de archivos para detectar posibles amenazas, ayudando a mantener la integridad del servidor, especialmente cuando se maneja contenido externo que pueda tener riesgos asociados.

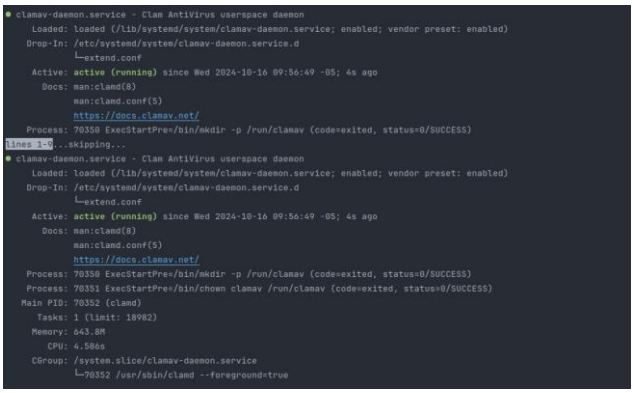


Ilustración 4. Ejecución de ClamAV

3) *Falta de actualizaciones*

Las actualizaciones regulares son esenciales para mantener un servidor protegido contra vulnerabilidades conocidas. Se ha implementado un proceso automatizado mediante comandos, lo que asegura que el servidor Ubuntu esté constantemente actualizado con los últimos parches de seguridad. Esta práctica minimiza el riesgo de ataques basados en vulnerabilidades obsoletas.

sudo apt update && sudo apt upgrade -y

4) *Acceso no autorizado al servidor*

Para evitar accesos no autorizados al servidor mediante SSH, se ha deshabilitado el acceso al usuario root y se ha implementado la autenticación basada en claves. Este método de autenticación es mucho más seguro que el uso de contraseñas, ya que las claves SSH son más difíciles de comprometer. Los comandos usados para estas configuraciones incluyen **PermitRootLogin** no y **PasswordAuthentication** no en el archivo de configuración */etc/ssh/sshd_config*, además de generar claves públicas y privadas mediante ssh-keygen.

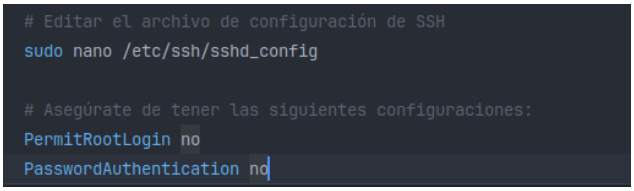


Ilustración 5. Configuración SSH

5) Falta de registros de acceso

Los registros de acceso son esenciales para detectar actividades sospechosas. Para ello, se ha optado por la instalación de **Fail2Ban**, una herramienta que monitoriza los archivos de registro y automáticamente bloquea las direcciones IP que intentan acceder repetidamente al servidor de forma no autorizada. Esto actúa como una medida preventiva ante posibles ataques de fuerza bruta y ayuda a mitigar intentos de intrusión.

```
# Instalar Fail2Ban
sudo apt install fail2ban

# Iniciar y habilitar el servicio
sudo systemctl start fail2ban
sudo systemctl enable fail2ban
```

Ilustración 6. Instalación Fail2Ban

```
2018-04-08 00:17:02,248 fail2ban.actions[4152]: WARNING [ssh] Unban 221.0.194.22
2018-04-08 00:21:04,553 fail2ban.actions[4152]: WARNING [ssh] Ban 183.230.146.26
2018-04-08 00:25:54,921 fail2ban.actions[4152]: WARNING [ssh] Ban 103.207.37.199
2018-04-08 00:31:05,310 fail2ban.actions[4152]: WARNING [ssh] Unban 183.230.146.26
2018-04-08 00:35:55,669 fail2ban.actions[4152]: WARNING [ssh] Unban 103.207.37.199
2018-04-08 01:18:11,573 fail2ban.actions[4152]: WARNING [ssh] Ban 181.214.87.4
2018-04-08 01:24:12,016 fail2ban.actions[4152]: WARNING [ssh] Ban 103.89.91.28
2018-04-08 01:28:12,326 fail2ban.actions[4152]: WARNING [ssh] Unban 181.214.87.4
2018-04-08 01:34:12,764 fail2ban.actions[4152]: WARNING [ssh] Unban 103.89.91.28
2018-04-08 02:34:56,905 fail2ban.actions[4152]: WARNING [ssh] Ban 5.188.10.182
2018-04-08 02:44:57,618 fail2ban.actions[4152]: WARNING [ssh] Unban 5.188.10.182
2018-04-08 05:01:56,044 fail2ban.actions[4152]: WARNING [ssh] Ban 87.54.18.103
2018-04-08 05:11:56,761 fail2ban.actions[4152]: WARNING [ssh] Unban 87.54.18.103
```

Ilustración 7. Baneo de IPs

Direcciones IP Concedidas	Antes	Después
0.0.0.0/20	320	180
0.0.0.0/21	430	101
0.0.0.0/22	230	60
0.0.0.0/23	497	30
0.0.0.0/24	250	10

Tabla 5. Bloqueo de IPs Antes-Después

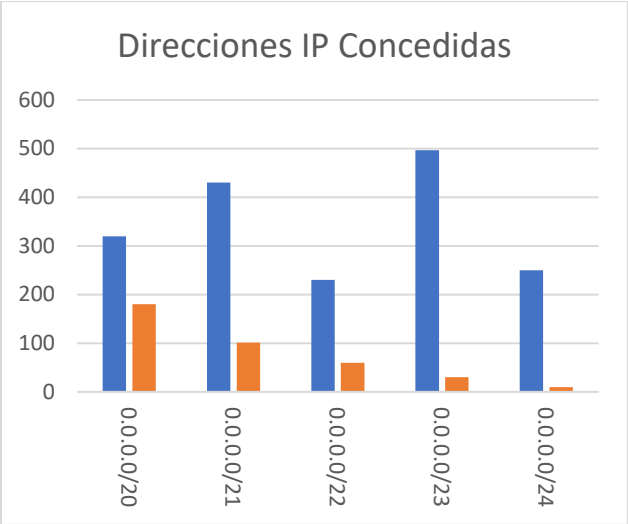


Ilustración 8. Direcciones IPs Concedidas

6) Monitoreo Constante

La monitorización en tiempo real del servidor es fundamental para identificar comportamientos anómalos o usos excesivos de recursos. Se han considerado herramientas como **htop** e **iftop** para este propósito. Además, se está evaluando la implementación de plataformas más avanzadas, como **Prometheus** en conjunto con **Grafana**, que ofrecen visualización detallada y alertas en tiempo real sobre el estado del servidor y el uso de recursos, facilitando una gestión proactiva.

E. Plan de acción y evaluación de riesgos.

Para mantener cualquier plataforma segura y en buen funcionamiento se necesita un plan que abarque desde el diagnóstico inicial hasta los ajustes necesarios en el camino. Este esquema de plan de acción no solo busca resolver los problemas de ahora, sino que también se anticipa a los cambios y retos que puedan surgir.

#	TIPO AMENAZA	AMENAZA	VULNERABILIDADES
1	HARDWARE	Avería de origen físico o lógico.	- Falta de mantenimiento - equipo obsoleto/ no reemplazado - falta de verificación de

			componentes del sistema. - Falta de ventilación data center. - Manipulación inadecuada durante el mantenimiento.
2	HARDWARE	Perdida de equipos	- Instalaciones física sin seguridades. - Falta de control de accesos.
3	HARDWARE	Corte del suministro eléctrico.	- Falta de equipo de respaldos de energía. - No contar instalación puesta tierra.
4	HARDWARE HARDWARE	El hardware puede estar sujeto a obsolescencia tecnológica	No existe soporte para el equipamiento
5	SOFTWARE	Fallo inicio de sistema operativo	Parches mal actualizados
6	SOFTWARE	Fallo inicio de sistema operativo	Errores en la configuración
7	SOFTWARE	Falta de sistemas de protección Antivirus	Activación de Malware
8	SOFTWARE	Fallo en el proceso de controles de cambio	Errores en la gestión de recursos.
9	SOFTWARE	Fallo en el proceso de controles de cambio	Errores en los sistemas de validación.
10	SOFTWARE	Fallo en el proceso de configuración de seguridades	Errores que permiten el acceso a directorios.
11	SOFTWARE	Fallo en el proceso de configuración de seguridades	Errores en la gestión y asignación de permisos.
12	SOFTWARE	Falta de sistemas de protección de Seguridad	Amenazas de ataques de denegación de servicio.
13	SOFTWARE	Proceso de Gestión de identidades, no controlado	Uso incorrecto o negligente de credenciales por parte de un usuario.
14	SOFTWARE	Proceso de Gestión de identidades, no controlado	Incorrecta asignación de privilegios o permisos de la administración.
15	HARDWARE	Fallos o ataques que vulneren el servidor de Base de datos	Información concentrada en un único servidor (Punto único de fallo)
16	ACCESOS	Perfiles de usuarios privilegiados, no controlados	Accesos no autorizados con usuarios privilegiados. Accesos Totales.
17	PERSONAL	Errores en la ejecución de procedimientos almacenados	Personal con poco conocimiento en la gestión de la Base de Datos
18	COMUNICACION	Servidor pierde conexión con el transaccional	Fallo de servicios de comunicaciones
19	HARDWARE	Servidor deja de funcionar inesperadamente	Degradación de los soportes de almacenamiento de información.

20	CONFIGURACION	Servidor deja de funcionar inesperadamente	Ausencia de monitoreo de estado de salud del Servidor
		Servidor deja de funcionar inesperadamente	Ausencia de monitoreo de estado de salud del Servidor
21	DATOS	No existen controles de exfiltración de información	Filtración de información sensible de la base de datos
22	DATOS	Ausencia de personal capacitado en la operación de la Base de datos	Alteración accidental de la información
23	DATOS	Ausencia de monitoreo de logs de accesos a la base de datos	Alteración intencional de la información
24	DATOS	Falta de aplicación de parches de seguridad	Exposición del Servidor a ataques cibernéticos
25	SERVICIOS	Contrato puede ser interrumpido por proveedor	Indisponibilidad de proveedor tecnológico para el mantenimiento de la base de datos

#	SEVERIDAD	Riesgo Residual	Plan de acción
1	**CRÍTICO**	MEDIO	- Mantener un cronograma de mantenimientos con técnicos especializados. - Monitoreo automático de notificación en caso de eventos. - Mantenimiento programados de sistema de ventilación.
2	**ALTO**	MEDIO	Se mantendría el mismo control. Se debe llevar un registro actualizado e informar las novedades.
3	**MEDIO**	BAJO	Contar con respaldos de energia, y llevar registro de eventos. Contar con manual operativo en caso de activar eventos inadecuados.
4	**ALTO**	MEDIO	Mantener un monitoreo de consumos de recursos. Actualizar equipos que se encuentran descontinuados. Coordinar, análizar equipos con proveedores para cambio y/o reemplazo.
5	**CRÍTICO**	CRÍTICO	Realizar la comprobación frecuencia de efectividad de respaldos.
6	**CRÍTICO**	ALTO	Intervención de personal capacitacido responsable.
7	**ALTO**	MEDIO	Mantener actualizado el software de Antivirus.
8	**MEDIO**	MEDIO	Mantener el monitoreo y realizar subcomites por lo menos 2 veces al año.
9	**ALTO**	MEDIO	Mantener los controles existentes
10	**ALTO**	ALTO	Se debe monitorear los accesos a procesos criticos.

11	**CRÍTICO**	CRÍTICO	Entregar cuentas de accesos limitados, y llevar registros de autorizaciones a los accesos críticos.
12	**MEDIO**	BAJO	Configuración de alertas y asignación del personal responsable para Monitoreo de servicio.
			Firmar acuerdos de cambios de información con los proveedores de servicios.
13	**ALTO**	ALTO	Solicitar reportes periodicos, y llevar un monitoreo de accesos.
14	**ALTO**	ALTO	Inscribirlo en un registro público, (Propiedad Intelectual)
15	**CRÍTICO**	CRÍTICO	Encriptar información sensible contra los ataques.
			Encriptar información sensible contra los ataques para la transportación.
16	**CRÍTICO**	CRÍTICO	Segregación de roles y perfiles. Habilitar logs de accesos en la base de datos.
			Segregación de roles y perfiles. Habilitar logs de accesos en la base de datos.
17	**CRÍTICO**	CRÍTICO	Asignar personal calificado para administración de base de datos.
			Habilitar logs de accesos en el motor de bdd.
18	**CRÍTICO**	ALTO	Cerrar puertos no utilizados. Utilizar herramienta segura de acceso remoto. Deshabilitar accesos remotos en los servidores.
			Contar con un proveedor de comunicaciones redundantes para balancear carga y segregar servicios. Contar con equipos redundantes de comunicaciones.
19	**CRÍTICO**	CRÍTICO	Monitoreo frecuente de la salud de disco duro y realizar actualizaciones de la herramienta.
			Aplicar la duplicación de disco RAID 5. Crea una copia exacta de los datos de las unidades
20	**CRÍTICO**	CRÍTICO	Monitoreo y revisión frecuentes de la salud de base (estimación informes mensuales). Supervisión de calidad de datos. Número mínimo de usuarios que debe tener acceso a la base de datos. Permisos limitados y los niveles mínimos necesarios para que puedan realizar su trabajo.
			Migración a Cloud
21	**CRÍTICO**	CRÍTICO	Habilitar logs de accesos en el motor de bdd.
			Encriptación de la información sensible.
22	**CRÍTICO**	CRÍTICO	Acceso a la red con un nivel mínimo de permisos necesarios.
23	**CRÍTICO**	CRÍTICO	Crear usuarios con privilegios limitados. Asignar permisos mínimos de accesos

			unicamente para la actividad correspondiente
			Activación de logs y permisos restringidos.
24	**CRÍTICO**	CRÍTICO	Ejecución de parches actualizados. Cambio o reemplazo a equipos actualizados.
			Encriptar textos planos en la transportación de información en varias capas.
25	**CRÍTICO**	CRÍTICO	Contar con personal bakcup del proveedor.
			Contar con cláusula que obligue al proveedor a operar al menos 60 días luego de notificar su salida.

Tabla 6. Plan de Acción

F. Evaluación de activos cuantificados

CONFIDENCIALIDAD		
Descripción	***Impacto***	***Valor***
La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible. Ej Divulgación de información sensible que afecta la reputación - Perdida de credibilidad - Demandas de los cliente	Critico	5
El riesgo puede ser aceptable momentáneamente sin embargo es importante considerarlo en planes de mitigación futuros. Ej. Información confidencial es compartida a sitios estratégicos, hay conocimiento del incidente de filtración	Alto	4
La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno, acceso no autorizado a información interna, exfiltración de políticas	Medio	3
El impacto se puede controlar con medidas rutinarias	Bajo	2
Acceso a información anonimizada No hay afectación reputacional		
El impacto existe pero es insignificante Acceso a información anonimizada No hay afectación reputacional	Muy Bajo	1

Tabla 7. Evaluación de activos Confidencialidad

INTEGRIDAD		
Descripción	***Impacto***	***Valor***
La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución, Ej. Pérdida, afectacion o destrucción del 100% de la Data, sin capacidad de restaurar respaldos, multas y sanciones de los entes de control, demandas judiciales	Critico	5
La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución Ej. Existe un 25% o más de la data afectada que no es recuperable y debe ser reescrita, alto número de comentarios en redes sociales	Alto	4
La destrucción o modificación de la información tiene un efecto leve para la institución Ej. Afectación de la data se puede recuperar con respaldos, pocos comentarios en redes sociales	Medio	3
El impacto se puede controlar con medidas rutinarias Afectación mínima de la información, recuperable en máximo 30 minutos	Bajo	2
El impacto existe pero es insignificante Afectación mínima de la información, recuperable en máximo 30 minutos	Muy Bajo	1

Tabla 8. Evaluación de activos Integridad

DISPONIBILIDAD		
Descripción	***Impacto***	***Valor***
La interrupción al acceso de la información o los sistemas tienen un efecto severo para el departamento Ej. Se paralizan las operaciones en un 100%,	Critico	5

interrupción de operaciones por más de (5) Días, intervención por parte de un ente de control u otro ente regulador, demandas judiciales de los clientes		
La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución. Ej. Se paraliza el 75% de las operaciones, interrupción de las operaciones, demandas judiciales, conocimiento en redes sociales, de la indisponibilidad de servicios	Alto	4
La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución. Ej. Se paraliza el 15% de servicios, se puede activar y recuperar el servicio en máximo 1 hora	Medio	3
El impacto se puede controlar con medidas rutinarias Infraestructura afectada es fácilmente reemplazable (menos de 30 minutos)	Bajo	2
El impacto existe pero es insignificante Infraestructura afectada es fácilmente reemplazable (menos de 30 minutos)	Muy Bajo	1

Tabla 9. Evaluación de activos Disponibilidad

CLASIFICACION SEGUN SU PRIVACIDAD		**VALOR**
RESTRINGIDA	Información que por su contenido sólo interesa a quienes va dirigida y cuya divulgación no autorizada podría ocasionar perjuicios a entidad.	3
USO INTERNO	Información dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma.	2
PUBLICO	Información que podría ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la institución sin que esto conlleve un impacto negativo de ninguna índole.	1

Tabla 10. Clasificación de Privacidad

VIII. ESTIMACION DE COSTO-BENEFICIO

En la revisión de seguridad del servidor, se detectaron varias vulnerabilidades, cada una con soluciones específicas para mitigar riesgos. Se fortalecieron las contraseñas exigiendo al menos 8 caracteres, inclusión de mayúsculas, números y caracteres especiales. Además, se instaló un antivirus para prevenir infecciones de malware, y se estableció un cronograma de actualizaciones semestrales para mantener el sistema operativo y software protegido contra posibles vulnerabilidades. También se aseguraron los accesos al servidor mediante autenticación basada en IP y credenciales seguras, y se implementaron bitácoras para registrar todas las actividades de acceso.

El análisis de puertos se realizó con Nmap, identificando los servicios activos en el servidor y resaltando posibles vulnerabilidades. Los resultados mostraron varios servicios críticos, como administración remota y transferencia de archivos, que deben estar actualizados y configurados de forma segura. Además, se decidió implementar un monitoreo continuo para identificar actividades sospechosas de manera oportuna y reforzar la seguridad en el sistema.

#	APLICACIÓN / SERVICIO	COSTO U.	COSTO ANUAL	VIGENCIA DEL CONTRATO	OBSERVACIÓN
1	FIREWALL	$1.000,00	$1.000,00	1 vez al año	Adquisición de licencias y soporte - seguridad perimetral.
2	ANTIVIRUS	$40,50	$450,00	1 vez al año	Adquisición de 10 licencias 1c/equipo

					- seguridad interna
3	SEGURIDAD EN REDES	$920,00	$11.040,00	Para 3 años	Adquisición de servicios de soporte, Configuraciones.
4	SEGURIDAD BDD	$27.200,00	$27.200,00	1 vez al año	Monitoreo y soporte y revisión de la salud de la bdd, monitoreo de almacenamiento -
COSTO SUBTOTAL ANUAL				$ 39.690,00	
COSTO TOTAL ANUAL + IMPUESTOS.				$ 45.643,50	

Tabla 11. Costos de Servicio

SERVICIOS CONSIDERADOS PARA ADQUIRIR					
#	**APLICACIÓN / SERVICIO**	**COSTO U.**	**COSTO ANUAL APROX.**	**VIGENCIA DEL CONTRATO**	**OBSERVACIÓN**
1	ETHICAL HACKING	$4.000,00	$4.000,00	1 vez al año	Test de penetración de redes externa, e interna, campañas de phishing.
2	AUDITOR INFORMÁTICO	$4.000,00	$4.000,00	Cada 2 año	Auditor Informática
3	PROGRAMA DE CAPACITACIÓN	$3.000,00	$3.000,00	1 vez al año	Capacitación OSI y sensibilización, campañas en seguridad
TOTAL, DE COSTOS CONSIDERADOS:				$11.000,00	
COSTO TOTAL + IMPUESTOS:				$12.320,00	

Tabla 12. Costos de Servicios para adquirir

RECURSOS FINANCIEROS CAPA DE SEGURIDAD	
PR	MES

	ENE	FEB	MAR	ABRI	MAYO	JUNIO	JULIO	AGOS	SEP	OCT	NOV	DIC
FIREWALL											$1.000,00	
ANTIVIRUS											$450,00	
SEGURIDAD	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00	$920,00
SEGURIDAD BDD											$27.200,00	
ETHICAL HACKIN					$4.000,00							
AUDITORIA						$4.000,00						
CAPACITACIÓN				$1500.00					$1.500,00			
SUBTOTAL	$920,00	$920,00	$920,00	$2.420,00	$4.920,00	$4.920,00	$920,00	$920,00	$4920,00	$920,00	$29.5700,0	$920,00
TOTAL, COSTO												$53.19<

Tabla 13. Recursos Financieros

Tarea	**Objetivo de aprendizaje**	**Duración**	**Fecha -Inicio**	**Fecha -Fin**	**Responsable**
Modulo 1	OE.1	30	18/10/2023	18/11/2023	P.O
Modulo 2	OE.2	35	19/11/2023	05/01/2024	J.M
Modulo 3	OE.3	65	06/01/2024	06/04/2024	P.O

Modulo 4	OE.4	65	06/04/2024	23/08/2024	P.O
Modulo 5	OE.5	45	23/08/2024	18/10/2024	J.M

Tabla 14. Fechas de Actividades

Responsable	**Horas**
(J.M) – Jonathan Marcelo Moran Velasco	120h
(P.O) – Pedro José Orellana Jaramillo	120h
Total de horas: 240h	
Fecha de Inicio: 18/10/2023 – Fecha de Fin: 18/10/2024	

Tabla 15. Responsables de Ejecución

IX. ESTIMACION DE NECESIDADES

En este punto, se pretende identificar las necesidades en relación con los temas de seguridad de la información. Este análisis se centra en adquirir el conocimiento general que poseen los empleados antes de la ejecución del plan de concienciación y formación.

Para evaluar el nivel de conocimiento previo a la implementación del plan, se utilizarán métodos como: encuesta y observación y difusión.

A. Formación del levantamiento de necesidades.

Se utiliza el método de la encuesta en donde se aplicará un cuestionario a través de Google Forms con preguntas que abarcan aspectos como conceptos básicos de seguridad, programa maligno, ingeniería social, correos y sitios web fraudulentos, gestión de contraseñas, políticas institucionales de seguridad y buenas prácticas de seguridad. El formulario se configurará con respuestas cerradas para medir el nivel de conocimiento de los usuarios que utilizan la plataforma. Es importante destacar que el programa se orienta hacia personas sin formación técnica en el campo de la tecnología de la información.

ENCUESTA DE NIVEL DE CONOCIMIENTO		
		Domino el tema
Pregunta 1	¿Conoce de qué se trata la seguridad de la información?	Conozco un poco
		No tengo ningún conocimiento del tema
		Domino el tema
Pregunta 2	¿Sabe lo que es un ataque informático?	Conozco un poco
		No tengo ningún conocimiento del tema
Pregunta 3	¿Conoce lo qué es un ciberdelincuente?	Conozco un poco
		No tengo ningún conocimiento del tema
		Domino el tema
Pregunta 4	¿Generalmente escanea un dispositivo USB con el antivirus antes de utilizarlo?	Siempre
		A veces
		Nunca
		Domino el tema
Pregunta 5	¿Conoce qué es el ransomware?	Conozco un poco
		No tengo ningún conocimiento del tema
Pregunta 6	¿Conoce de qué se trata un ataque de phishing?	Domino el tema
		Conozco un poco
		No tengo ningún conocimiento del tema
Pregunta 7	¿Podría reconocer una página web fraudulenta?	Si
		No
		No estoy seguro/a
Pregunta 8	¿Verifica el remitente de sus correos electrónicos, antes de abrir enlaces o descargar archivos adjuntos?	Siempre
		A veces
		Nunca
Pregunta 9	¿Bloquea o cierra sus sesiones cuando abandona momentáneamente su estación de trabajo?	Siempre
		A veces
		Nunca

Pregunta 10	¿Generalmente guarda las contraseñas en uno o varios de estos lugares? (notas, cuaderno, teléfono, archivos de texto, fotografías, navegador web)	Siempre
		A veces
		Nunca
Pregunta 11	¿Reutiliza la misma contraseña para sus aplicaciones? (cuentas institucionales, personales)	Para 2 aplicaciones
		Para 3 aplicaciones
		Para más de 3 aplicaciones
		Tengo una contraseña diferente para cada aplicación
Pregunta 12	¿La Cooperativa de Artesanos cuenta con políticas de seguridad de la informacion?	Si
		No
		Desconozco
Pregunta 13	¿En la Cooperativa de Artesanos existen directrices para el uso seguro de los equipos y manejo adecuado de la información?	Si
		No
		Desconozco
Pregunta 14	¿Conoce cómo establecer la privacidad de la información de sus redes sociales? (Ej. Facebook, Instagram, WhatsApp)	Se cómo hacerlo
		No sé cómo hacerlo
		Conozco un poco
Pregunta 15	¿Generalmente publica información personal en sus redes sociales? (cumpleaños, ciudad dónde vive, lugar de trabajo, profesión, teléfono, correo, gustos, intereses, etc.)	Siempre
		A veces
		Nunca
Pregunta 16	¿Ha recibido formación en temas de seguridad informática?	Si, de forma autónoma
		Si, en el trabajo
		No he recibido formación sobre este tema

Tabla 16. Encuesta de Seguridad

La nota máxima que se establece en esta encuesta es 48 puntos y la nota minina es 16 puntos.

B. Desarrollo de estrategias y planes.

El plan incluye tres programas distintos: la concienciación, entrenamiento y la formación, y cada una de ellas se describe detalladamente.

El propósito de esta etapa es orientar la atención de los participantes hacia la adquisición de conocimientos sobre las políticas de seguridad de la información. Se establecen las siguientes políticas para el programa de formación:

- Este programa integrará recursos de aprendizaje disponibles en la plataforma virtual, la cual estará activa todos los días del año para que cualquier persona que pueda acceder.
- La matriculación se realizará aproximadamente con 10 colaboradores mensuales, siendo esta planificación designada por el oficial de seguridad de la información.
- La duración del programa es de dos meses para cada estudiante, con previa notificación de la matriculación del curso por el oficial de seguridad de la información.
- El usuario y la clave de acceso al curso se enviarán por correo electrónico a la dirección institucional hasta el día de inicio del curso.
- Los estudiantes matriculados deberán realizar cuatro evaluaciones dentro del plazo establecido de dos meses para aprobar el curso.
- El estudiante podrá consultar su calificación en las evaluaciones de manera inmediata hasta el cierre del curso.

- El material estará disponible las 24 horas del día durante el periodo de matriculación.
- El estudiante es responsable de su propio autoaprendizaje, manteniendo la autonomía para cumplir con los objetivos del curso de autoestudio.
- Los foros de aprendizaje deben ser respondidos dentro de la semana de aprendizaje o para resolver inquietudes relacionadas con las evaluaciones.

C. Elección del material en función del personal.

Se genera contenido educativo destinado a la difusión del material de formación, diseñado para para abordar temas relacionados con el políticas, procesos y procedimientos. Este contenido estará disponible a través del aula virtual de la cooperativa.

D. Desarrollo del material.

La minuciosa descripción de los módulos en un programa de formación proporciona una comprensión detallada de las políticas internas de seguridad de la información, fundamentadas en los temas pertinentes de un reglamento actualizado en esta materia. Estos temas están diseñados para establecer una base sólida que será beneficiosa en las tareas diarias de los participantes. Se coloca los módulos que mantiene el material de formación.

MODULOS	DESCRIPCIÓN	TEMAS	RECURSOS
MÓDULO 1	Introducción a la Seguridad Informática	Conceptos generales de seguridad de la información	Guía Módulo 1.pdf Presentación Módulo 1.pdf
		Responsabilidad de los empleados	
		Pantallas despejadas y escritorios limpio	
		Uso de dispositivos	
		Usos de activos de la información	
		Respaldo de la información	
MÓDULO 2	Clasificación de información	Variable para la evaluación	Guía Módulo 2.pdf Presentación Módulo 2.pdf
		Etiquetado de la información	
		Directrices	
MÓDULO 3	Gestión de riesgos de seguridad de la información	Vulnerabilidades	Guía Módulo 3.pdf Presentación Módulo Videos de vulnerabilidades y amenazas 3.pdf
		Amenazas	
		Tratamiento de datos	
		Controles implementados	
MÓDULO 4	Control de accesos físicos y tecnológicos	Gestión de usuarios • Perfil de usuarios • Asignación y creación de usuarios • Mantenimiento de usuarios • Cierre y cancelación de usuarios	Guía Módulo 4.pdf Presentación Módulo 4.pdf
		Contraseña • Establecimiento de una contraseña • Uso de la contraseña	
		Funcionarios • funcionarios con privilegios • Protección de la contraseña	
		Medios de almacenamiento	
		Control de accesos a las conexiones remotas	
MÓDULO 5	Gestión de incidentes	Responsabilidad de colaborador en reportar	Guía Módulo 5.pdf Presentación Módulo 5.pdf
		Respuesta ante incidentes	
		Respuesta de eventos	
		Antes de la contratación	

MÓDULO 6	Seguridad de la información para recursos humanos	Durante la contratación Cese de la contratación	Guía Módulo 6.pdf Presentación Módulo 6.pdf
MÓDULO 7	Seguridad física	Áreas seguras Seguridad de los equipos	Guía Módulo 7.pdf Presentación Módulo 7.pdf
MÓDULO 8	Ciberseguridad	Firewall de acceso a internet Antivirus	Guía Módulo 8.pdf Presentación Módulo 8.pdf Videos sobre protecciones de ciberseguridad

Tabla 17. Módulos para Desarrollo

E. Material de Concienciación.

En este proceso de gestión, la plataforma seleccionada será Moodle, una herramienta que permite la creación de espacios interactivos para la participación de los usuarios a través de foros, evaluaciones y la carga de materiales de estudio acorde al perfil de participante y a los lineamientos establecidos en instructivo para este efecto.

Se centrará en la elaboración de contenido para campañas informativas utilizando los recursos internos de la cooperativa, con un enfoque específico en las temáticas mencionadas anteriormente. Estas campañas de concienciación se coordinarán con el departamento de marketing, ya que este se encargará de gestionar y publicar imágenes en las redes sociales. Se utilizan 2 medios de difusión de material de entrenamiento:

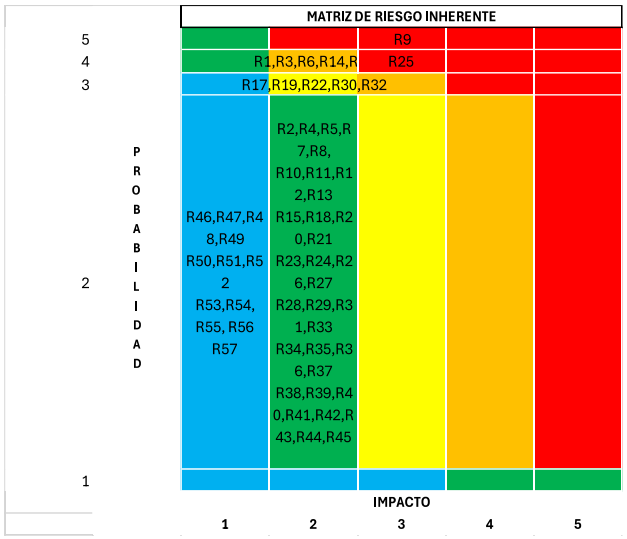
- **Publicidad en televisión:** Este método será utilizado para enviar material publicitario, que incluye pósteres y videos, dirigido a los socios/clientes que visitan las agencias.
- **Redes sociales:** Una herramienta de difusión del material a través de plataformas como Facebook e Instagram, WhatsApp, entre otras.

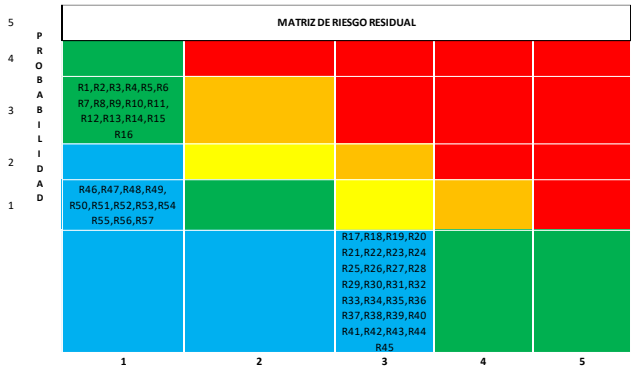
F. Concienciación.

En este contexto, se implementan campañas de concientización destinadas a los colaboradores. Estas iniciativas se llevan a cabo mensualmente con el propósito de aumentar la conciencia sobre prácticas incorrectas o mal ejecutadas. El objetivo principal es proporcionar material de relevancia e importancia al personal, brindando comprensión sobre temas críticos, especialmente para aquellos individuos que carecen de experiencia previa en este ámbito.

El enfoque consistirá en llegar a través de la difusión de posters, videos, etc., abordando temas relacionados con la protección de la información y la prevención de cualquier tipo de fraude.

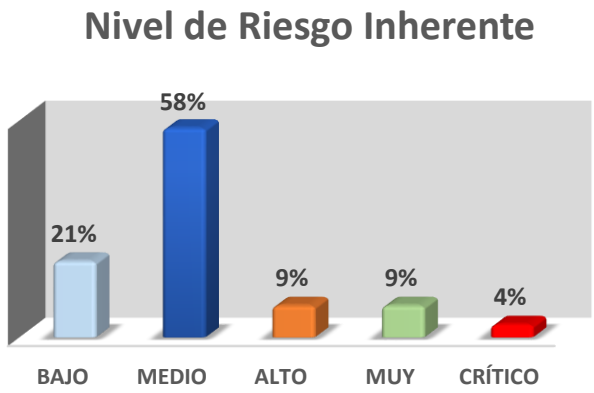
G. Matriz de Riesgos.





Limites	
>9	Critico
Entre 7 - 8	Muy alto
Entre 5 - 6	Alto
Entre 3 - 4	Medio
Entre 0 - 2	Bajo

Impacto		1	2	3	4	5
Probabilidad	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5



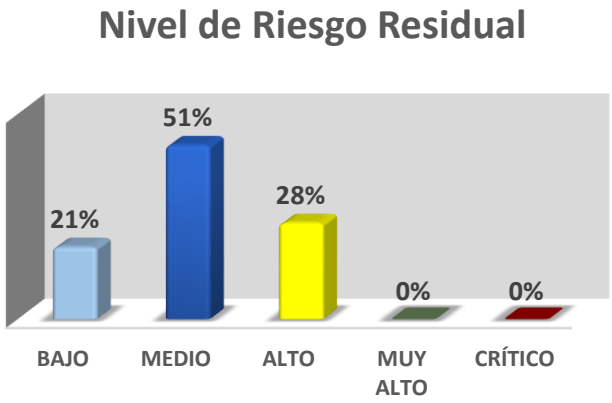


Ilustración 9. Niveles de Riesgo

X. CONCLUSIONES

Realizar auditorías de ciberseguridad en plataformas de Edutainment es súper importante para proteger tanto los datos de los usuarios como su privacidad. A lo largo de este análisis, hemos descubierto que, aunque la plataforma tiene buenas medidas de seguridad, siempre hay espacio para mejorar. Las auditorías nos han ayudado a identificar algunas áreas donde se podrían estar filtrando datos o donde hay riesgos que **podrían** ser explotados.

También hemos observado que la capacitación del personal y la educación de los usuarios son clave para mantener a raya los problemas de seguridad. Usar herramientas como Nmap y Metasploit nos permitió simular ataques y ver

cómo responderíamos ante una amenaza real. Y esto subraya la necesidad de estar siempre vigilantes y listos para adaptarnos a las nuevas amenazas que puedan surgir.

XI. RECOMENDACIONES

Para fortalecer la ciberseguridad en plataformas de Edutainment, es esencial implementar políticas de seguridad claras y comprensibles para todo el personal. La capacitación continua es fundamental: asegurarte de que todos estén actualizados sobre las mejores prácticas de seguridad puede marcar la diferencia en la protección de datos sensibles. Además, establecer un sistema de monitoreo constante y realizar auditorías regulares permitirá identificar vulnerabilidades antes de que sean explotadas. Las pruebas de penetración también son cruciales para evaluar la resistencia de la plataforma ante posibles ataques.

Por otro lado, mantener el software y hardware al día con los últimos parches de seguridad es vital para cerrar cualquier puerta que los atacantes puedan aprovechar. El cifrado de datos, tanto en reposo como en tránsito, garantizará que la información sensible de los usuarios permanezca protegida. Finalmente, contar con un plan de respuesta a incidentes bien definido y colaborar con expertos en ciberseguridad puede ayudar a manejar cualquier problema que surja, generando confianza en los usuarios y asegurando un entorno más seguro para todos.

XII. REFERENCIAS

[1] A. S. a. B. Johnson, The Importance of Cybersecurity in Educational Platforms, Journal of Cybersecurity Education, 2023.

[2] C. Williams, Best Practices for Securing Edutainment Applications, New York: International Conference on Cybersecurity, 2022.

[3] D. B. e. al., Cyber Threats in Online Learning Environments, Journal of Information Security, 2021.

[4] E. Garcia, Training and Awareness Programs for Cybersecurity, Cybersecurity Journal, 2022.

[5] F. Lee, The Role of Data Encryption in Protecting User Information, Journal of Data Protection, 2023.

[6] G. Patel, Incident Response Plans in Educational Technology, San Francisco: Proceedings of the Educational Technology Conference, 2023.

[7] H. Martinez, Monitoring and Auditing for Cybersecurity, Cybersecurity Review, 2024.

[8] J. B. a. K. Wilson, Cybersecurity Policies for Online Education, International Journal of Online Learning, 2022.

[9] L. Rodriguez, Penetration Testing in Educational Software, Journal of Information Assurance, 2021.

[10] M. Taylor, User Authentication in Edutainment Platforms, Journal of Cybersecurity Standards, 2023.

[11] N. Kim, Collaborative Approaches to Cybersecurity, Journal of Educational Technology, 2024.

[12] O. Davis, Emerging Cyber Threats in Digital Learning, Chicago: Proceedings of the Cybersecurity in Education Conference, 2022.

[13] P. White, Securing Online Learning Platforms: Challenges and Solutions, Cybersecurity Advances, 2023.

[14] Q. Thompson, Risk Assessment in Educational Environments, Journal of Risk Management, 2021.

[15] R. Hall, Data Privacy Regulations and Their Impact on Education, Journal of Privacy Law, 2024.

[16] S. Young, User Education as a Security Measure, International Journal of Cybersecurity Education, 2022.

[17] T. Green, Technological Innovations in Cyber Defense, Journal of Cyber Defense Strategies, 2023.

[18] U. Adams, Cloud Security in Educational Institutions, Cybersecurity Trends, 2021.

[19] V. King, The Future of Cybersecurity in Edutainment, Journal of Future Technologies, 2024.

[20] W. L. a. X. Chen, The Need for Cybersecurity Awareness in Schools, Boston: Proceedings of the Educational Technology Symposium, 2023.

[21] N. ISO, «Norma ISO 27001,» [En línea]. Available: https://www.normaiso27001.es/a5-politicas-de-seguridad-de-la-informacion.

[22] N. ISO, «Norma ISO 27001,» [En línea]. Available: https://www.normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion.

[23] N. ISO, «Norma ISO 27001,» [En línea]. Available: https://www.normaiso27001.es/a8-gestion-de-activos.

[24] N. ISO, «NORMA ISO 27001,» [En línea]. Available: https://www.normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion.

[25] P. I. Morales Paredes y P. Medina Chicaiza, «3Ciencias,» [En línea]. Available: https://3ciencias.com/articulos/articulo/ciberseguridad-plataformas-educativas-institucionales-educacion-superior-provincia-tungurahua-ecuador/?utm_source=chatgpt.com.

[26] Auditool, «Auditool,» [En línea]. Available: https://www.auditool.org/tecnologia-de-informacion/ciberseguridad/programa-de-auditoria-de-seguridad-en-redes-sociales-y-plataformas-digitales.

[27] J. Hernandez, «PreyProject,» [En línea]. Available: https://preyproject.com/es/blog/auditoria-de-ciberseguridad-claves-para-la-proteccion-digital-empresarial.

[28] A. V. J. Fernando, «PLAN DE CIBERSEGURIDAD PARA EDUCACIÓN BÁSICA ECUATORIANA CONTRA EL CIBERDELITO POR COVID-19,» *INNDEV - Innovation & Development Ciencias del Sur,* vol. II, nº 1.

[29] J. Oulefki, «PlanAlfa.es,» 12 Diciembre 2024. [En línea]. Available: https://planalfa.es/ciberseguridad-en-la-educacion-digital-desafios-del-aprendizaje-remoto/.

[30] P. Cueva, «SmartCo,» 30 Mayo 2024. [En línea]. Available: https://smartco.com.ec/articulos-2/la-importancia-de-la-ciberseguridad-en-la-educacion/.

[31] D. Herrera-Shigua, T. Mendoza-Solorzano, L. León-Navarrete y M. Zambrano-Antón, «Revista 593 Digital Publisher CEIT,» 2025. [En línea]. Available: https://www.593dp.com/index.php/593_Digital_Publisher/article/view/2952.

[32] M. d. T. y. d. l. S. d. l. Informacion, «Asociacion de Bancos Privados del Ecuador,» [En línea]. Available: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf.

[33] P. I. Morales-Paredes y P. Medina-Chicaiza, «CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR DE LA PROVINCIA DE TUNGURAHUA - ECUADOR,» vol. X, nº 2, 2021.

[34] «CadenaSer,» 15 Octubre 2024. [En línea]. Available: https://cadenaser.com/castillayleon/2024/10/15/la-cibercriminalidad-sube-un-151-en-valladolid-en-los-ultimos-cinco-anos-radio-valladolid/.

[35] P. Pillajo-García y D. Avila-Pesantez, «Escuela Superior Politécnica de Chimborazo,» 30 Diciembre 2022. [En línea]. Available: https://pdfs.semanticscholar.org/7109/e6f

b0cd71aef81496bd0cb33d91f2dc1f490.pdf.

[36] «Coorporacion Nacional de Finanzas Populares y Solidarias,» 21 Mayo 2021. [En línea]. Available: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf.

[37] «COSEDE,» 13 Noviembre 2023. [En línea]. Available: https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf.