Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v16i31.2516

Artículos científicos

Ciberseguridad: Métodos de Defensa Ante Ataques de Infiltraciones

Cybersecurity: Defense Methods Against Infiltration Attacks

Cibersegurança: Métodos de Defesa Contra Ataques de Infiltração

Juan Manuel Bernal Ontiveros
Tecnológico Nacional de México, Instituto Tecnológico de Ciudad Juárez, México
Juan.bo@cdjuarez.tecnm.mx
https://orcid.org/0000-0002-3819-5750

Marisela Palacios Reyes*
Tecnológico Nacional de México, Instituto Tecnológico de Ciudad Juárez, México
marisela.pr@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-2830-5829

Francisco Zorrilla Briones
Tecnológico Nacional de México, Instituto Tecnológico de Ciudad Juárez, México
francisco.zb@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-0553-9841

Noé Ramón Rosales Morales
Tecnológico Nacional de México, Instituto Tecnológico de Ciudad Juárez, México
noe.rm@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-4526-3448

Susan Alexandra Cervantes Cardenas
Tecnológico Nacional de México, Instituto Tecnológico de Ciudad Juárez, México
L21111089@cdjuarez.tecnm.mx
https://orcid.org/0009-0008-6125-3657

* Autor de Correspondencia

Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

Resumen

Este estudio aborda la ciberseguridad frente a intrusiones, considerando la creciente digitalización y los riesgos asociados con la protección de información sensible en las organizaciones. Se plantea determinar qué métodos de defensa resultan más efectivos y cómo pueden adaptarse las organizaciones a tácticas emergentes de los ciberdelincuentes. Los objetivos incluyen identificar amenazas, evaluar las defensas actuales y proponer estrategias de mitigación para fortalecer la seguridad. La metodología contempla un estudio de caso en una organización, en el cual se evalúan vulnerabilidades mediante pruebas de penetración (penetration testing) y análisis de infraestructura.

Se espera como resultado una disminución en el tiempo de detección de amenazas y una respuesta más eficaz mediante la implementación de tecnologías avanzadas, como la autenticación multifactorial y la segmentación de redes. La interpretación de estos hallazgos destaca la relevancia de una ciberseguridad robusta y adaptativa, capaz no solo de prevenir sino también de mitigar ataques. Las conclusiones indican que las amenazas cibernéticas evolucionan rápidamente, lo que hace imprescindible la adopción de defensas proactivas y el fortalecimiento de una cultura organizacional orientada a la seguridad. En consecuencia, este estudio resalta que una estrategia de ciberseguridad sólida es esencial para reducir los impactos financieros y salvaguardar los activos críticos de las empresas.

Palabras clave: ataque cibernético, vulnerabilidad, intrusión, ciberseguridad, protección de datos.

Abstract

This study addresses cybersecurity in the face of intrusion attacks, considering the increasing digitalization and the risks associated with protecting sensitive information within organizations. It aims to determine the most effective defense methods and explore how organizations can adapt to emerging tactics employed by cybercriminals. The objectives include identifying threats, evaluating current defense mechanisms, and proposing mitigation strategies to enhance security. The methodology involves a case study within an organization to identify vulnerabilities through penetration testing and infrastructure analysis.

The expected results include shorter threat detection times and a more effective response enabled by advanced technologies such as multifactor authentication and network segmentation. These findings highlight the need for robust and adaptive cybersecurity that

not only prevents but also mitigates attacks. The conclusions emphasize that cyber threats evolve rapidly, necessitating the implementation of proactive defense mechanisms and fostering a strong cybersecurity culture within organizations. Ultimately, this study underscores that a resilient cybersecurity strategy is crucial to minimizing financial losses and safeguarding critical corporate assets.

Keywords: cyber attack, vulnerability, intrusion, cybersecurity, data protection.

Resumo

Este estudo aborda a segurança cibernética contra intrusões, considerando a crescente digitalização e os riscos associados à proteção de informações sensíveis nas organizações. O objetivo é determinar quais métodos de defesa são mais eficazes e como as organizações podem se adaptar às táticas emergentes de cibercriminosos. Os objetivos incluem identificar ameaças, avaliar as defesas atuais e propor estratégias de mitigação para fortalecer a segurança. A metodologia inclui um estudo de caso em uma organização, no qual as vulnerabilidades são avaliadas por meio de testes de penetração e análise de infraestrutura.
O resultado esperado é a redução do tempo de detecção de ameaças e uma resposta mais eficaz por meio da implementação de tecnologias avançadas, como autenticação multifator e segmentação de rede. A interpretação desses resultados destaca a importância de uma segurança cibernética robusta e adaptável, capaz não apenas de prevenir, mas também de mitigar ataques. As conclusões indicam que as ameaças cibernéticas estão evoluindo rapidamente, tornando essenciais a adoção de defesas proativas e o fortalecimento de uma cultura organizacional voltada para a segurança. Consequentemente, este estudo destaca que uma estratégia de segurança cibernética robusta é essencial para reduzir os impactos financeiros e proteger os ativos críticos do negócio.

Palavras-chave: ataque cibernético, vulnerabilidade, intrusão, segurança cibernética, proteção de dados.

Fecha Recepción: Octubre 2024 **Fecha Aceptación:** Julio 2025

Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

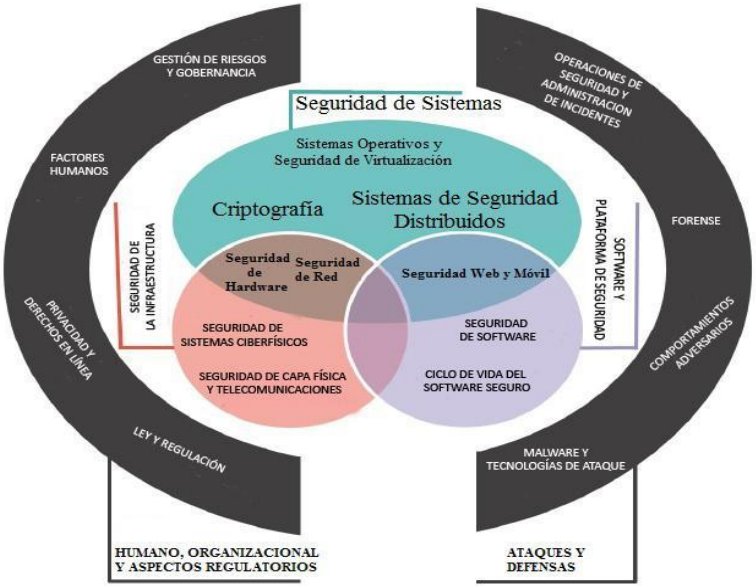
Introducción

En primer lugar debemos asimilar que es la Ciberseguridad, y se define como la salvaguarda de los sistemas de información, que abarca hardware, software y la infraestructura relacionada, igual que los datos y los servicios que ofrecen, contra accesos no autorizados, daños o usos inapropiados. Esto comprende tanto los daños provocados deliberadamente por el usuario del sistema como aquellos que ocurren de manera accidental debido a la falta de cumplimiento de los protocolos de seguridad. En el surgimiento de la combinación de las tecnologías móviles y basadas en la nube, se ha acentuado el manejo de seguridad en los datos. En este contexto, suele plantearse con frecuencia la interrogante sobre la importancia de centrarse en la seguridad, especialmente en organizaciones que han experimentado incidentes relacionados con la protección de sus activos de información.

En tiempo real, es la discusión frecuente hoy en día, debido a los ataques a las vulnerabilidades de las empresas, y esto introduce que se hable del concepto de seguridad, de una manera u otra. La seguridad ya no es solo un requisito de un administrador de TI (Tecnologías de la información) o administradores de seguridad en una organización. Ahora es el requisito de todas aquellos usuarios, sistemas o dispositivos interconectados con redes digitales de una forma u otra con cualquier tipo de datos según lo comenta (Giménez, 2011).

Otro concepto importante dentro del campo de la ciberseguridad es el *Ciberespacio*, y se entiende como un lugar en el que se llevan a cabo transacciones de negocios, comunicaciones humanas, se hace y se disfruta el arte, se forman y desarrollan relaciones, etc. En este lugar, el crimen cibernético, la amenaza y guerra cibernética pueden ocurrir, teniendo impactos reales y virtuales. En su conjunto, el CyBOK (The Cyber Security Body of Knowledge) delinea una amplia gama de temas que parecen estar dentro del amplio alcance de la seguridad cibernética, además puede servir como una definición extendida del tema, y se resume a continuación en la figura 1 (Rashid, Chivers, Danezis, Lupu, y Martin, 2019).

Figura 1. Las 19 áreas de conocimiento (KA) en el ámbito de CyBOK



Nota: Extraida del manual CyBOK. Fuente: Rashid, Chivers, Danezis, Lupu, y Martin, (2019)

En ciberseguridad, la protección fundamental se orienta hacia la protección en contra de los atacantes, proceso físico o aleatorio que intentarán realizar una infiltración no autorizada. Por lo tanto, el núcleo de cualquier consideración de seguridad es el modelado de estos atacantes: los motivos para el ataque, las amenazas que plantean y las capacidades que pueden utilizar para llevar a cabo infiltraciones no autorizadas. Cuando se consideran las amenazas en la seguridad cibernética a menudo se implementa una serie controles que pueden afectar a las personas, los procesos y la tecnología, debido a los ataques perpetrados por los ciberdelincuentes. Algunos de estos se centrarán en la prevención de malos resultados, mientras que otros se abordan mejor a través de la detección y reacción en base a las infiltraciones de los ataques. Las organizaciones, empresas comerciales y de TI necesitan diseñar estrategias para proteger los activos digitales cada vez más valiosos, cómo evaluar las amenazas y cómo cumplir con las expectativas reglamentarias de los clientes que son cada vez más estrictas.

Antecedentes

En la actualidad digital, la ciberseguridad se ha convertido en un componente esencial debido al aumento constante de los ataques cibernéticos que ponen en riesgo tanto a usuarios individuales como a organizaciones. Estas amenazas suelen implicar accesos no autorizados a redes, sistemas o datos confidenciales, lo cual puede derivar en consecuencias significativas, tales como el robo de información, la interrupción de operaciones esenciales o incluso el sabotaje de infraestructuras críticas (Keyed Systems LLC, s. f.)

Para contrarrestar estos ataques, los métodos de defensa en ciberseguridad han evolucionado, adoptando estrategias tanto proactivas como reactivas, por ejemplo entre las estrategias más comunes se encuentran los firewalls, los Sistemas de detección y prevención de intrusiones (IDS/IPS), el cifrado de datos y la Autenticación multifactorial (MFA) (Kissel, 2013).

A medida que las tácticas de los ciberatacantes se vuelven más avanzadas y automatizadas, las defensas también han evolucionado, impulsando el uso creciente de la inteligencia artificial y el análisis predictivo en ciberseguridad. Estas tecnologías permiten detectar patrones complejos y anticipar amenazas en tiempo real, habilitando respuestas proactivas frente a ataques sofisticados (Asad & Steltzer, 2025).

Además, resulta fundamental considerar la importancia de la concienciación y formación en ciberseguridad dentro de las organizaciones. Los empleados suelen representar el punto de mayor vulnerabilidad en la cadena de defensa si no se capacitan adecuadamente en la detección de amenazas y en la implementación de buenas prácticas de seguridad (Corallo et al., 2022). De esta forma, la combinación de herramientas tecnológicas avanzadas y una cultura de seguridad sólida dentro de las organizaciones es clave para prevenir infiltraciones no autorizadas.

Métodos de Defensa

1. Firewalls: Actúan como una barrera que monitorea y controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas. Los firewalls modernos combinan el filtrado de paquetes con la inspección profunda de contenido (Tori, 2008).
2. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Estas herramientas analizan patrones de tráfico para identificar comportamientos sospechosos o anomalías que podrían ser indicativos de un ataque (Kissel, 2013).

3. Cifrado de Datos: Garantiza que la información sensible se mantenga segura incluso si es interceptada por actores maliciosos, utilizando algoritmos criptográficos avanzados (Tori, 2008).
4. Autenticación Multifactorial (MFA): La autenticación de múltiples factores añade capas adicionales de seguridad, solicitando más de un método de verificación de identidad (Corallo et al., 2022).

Marco Teórico

Los ataques o infiltraciones no autorizadas constituyen incidentes de seguridad que, al ser inesperados, pueden comprometer información confidencial dentro de las operaciones de una organización. Estas situaciones provocan pérdidas, uso indebido de datos y vulneraciones en los sistemas, generalmente con el objetivo de obtener beneficios por parte del ciberdelincuente. Entre los tipos de ataques más comunes se encuentran la infección por malware o virus, el phishing y los ataques de denegación de servicio distribuido (DDoS), entre otros (Diogenes & Ozkaya, 2018).

A continuación, se describen las categorías en las que pueden clasificarse los ataques cibernéticos o incidentes de seguridad:

- Contenido abusivo: Ataques que muestran signos evidentes de spam (correo no deseado) y contienen información inapropiada o perjudicial para el usuario o la organización.
- Contenido malicioso: Se presentan problemas relacionados con software malicioso, como virus, troyanos, gusanos, spyware, bots e inyecciones de código en sistemas de gestión de bases de datos.
- Obtención de información: Se incluyen técnicas de escaneo de sistemas, uso de sniffers (husmeadores de red), ingeniería social y ataques de fuerza bruta, con el fin de recopilar datos confidenciales o vulnerar credenciales de acceso.
- Acceso/Intrusión: Ingresos no autorizados a cuentas privilegiadas o no privilegiadas, comprometiendo la integridad de aplicaciones mediante ataques como los de "día cero" (zero-day), que explotan vulnerabilidades desconocidas por el proveedor.
- Disponibilidad: Ataques que afectan la disponibilidad de servicios, como las denegaciones de servicio (DoS), ataques distribuidos (DDoS) y sabotajes a la infraestructura tecnológica.

- Seguridad/Confidencialidad de la información: Infiltraciones dirigidas a acceder o modificar información de forma no autorizada, comprometiendo la confidencialidad y la integridad de los datos.
- Fraude: Incidentes relacionados con el uso indebido de identidad digital, infracciones a los derechos de autor, phishing, robo de credenciales y suplantación de identidad.
- Vulnerabilidad: Explotación de debilidades técnicas en un sistema o aplicación, que permite al atacante acceder, manipular o comprometer los recursos de la organización (Sánchez, 2018).
- Ataque cibernético: Acciones ejecutadas en el ciberespacio con el propósito de comprometer o desarticular la seguridad de una organización, causando daño mediante accesos no autorizados, sabotajes o robo de información crítica.
- Área de ataque cibernético: Parte específica del sistema que es objeto del ataque. Puede incluir redes, protocolos, sistemas operativos, aplicaciones o cualquier otro componente tecnológico vulnerable.
- Exploit: Técnica o software diseñado para aprovechar una vulnerabilidad específica en un sistema, con el fin de ejecutar acciones maliciosas. En el contexto del hacking ético, un exploit es utilizado para probar la seguridad de un sistema, pero en escenarios maliciosos se emplea para obtener beneficios ilegítimos mediante la ejecución de comandos, scripts o fragmentos de código que alteran el comportamiento del sistema.

Métodos de Pruebas de Seguridad

Los ciberdelincuentes representan una amenaza constante, ya que buscan vulnerar los sistemas mediante nuevas técnicas de intrusión en organizaciones o empresas. Para contrarrestar estas amenazas, existen métodos de protección como las pruebas de penetración, las pruebas de concienciación para los usuarios y la evaluación del equipo de seguridad, que permiten a las organizaciones monitorear su infraestructura y detectar posibles vulnerabilidades, según lo explica (Scarfone & Mell, 2007).

Tipos de Pruebas de Seguridad

Evaluación de vulnerabilidades

Este tipo de prueba tiene como objetivo identificar las vulnerabilidades que pueden ser explotadas por actores maliciosos para comprometer sistemas, aplicaciones, redes o, en general, la infraestructura organizacional. A continuación, se enumeran los principales

componentes que deben ser evaluados durante la implementación de una prueba de vulnerabilidades:

- Aplicaciones web
- Versiones del sistema (en lugar de "compilación del sistema")
- Dispositivos de red
- Infraestructura de red
- Superficie de ataque por phishing
- Aplicaciones móviles

Pruebas de Conciencia de los Usuarios

Las pruebas de concienciación en seguridad (security awareness testing) tienen como objetivo evaluar el nivel de preparación del personal ante amenazas cibernéticas, como ataques de phishing o ingeniería social. Estas pruebas suelen consistir en simulaciones controladas que permiten observar las reacciones de los empleados frente a intentos de ataque, con el fin de identificar vulnerabilidades en el comportamiento humano dentro de la organización. Si bien los empleados son una parte fundamental de cualquier empresa, también pueden representar un eslabón débil en términos de seguridad. Los resultados obtenidos a partir de estas pruebas son útiles para ajustar los programas de capacitación y mejorar la cultura organizacional en materia de ciberseguridad, tanto en el ámbito digital como físico.

Evaluación del Equipo

Cuando un actor malicioso logra infiltrarse en la infraestructura de una organización, suele aprovechar la ausencia de controles de seguridad sólidos para explotar vulnerabilidades en sistemas, redes o aplicaciones. Estos agentes externos, al poseer un amplio conocimiento de herramientas y software especializados, pueden acceder a información confidencial, interrumpir servicios críticos o comprometer la continuidad operativa de la empresa.

Para identificar y prevenir estas amenazas, se implementan evaluaciones técnicas como la prueba de penetración (penetration testing). Esta prueba simula un ataque real, autorizado por la alta dirección, con el fin de detectar fallos de seguridad tanto internos como externos. El proceso abarca diferentes capas de la infraestructura, incluidas las aplicaciones, las redes, el comportamiento de los empleados y los aspectos físicos de seguridad.

Como parte del proceso, también se realiza una evaluación del equipo (asset assessment), que consiste en examinar los distintos componentes de la infraestructura

tecnológica, con el objetivo de identificar posibles vulnerabilidades o la presencia de exploits (Vañó-Chic, 2014). Los ámbitos evaluados incluyen:

- Físico: Se revisan vulnerabilidades en instalaciones como oficinas, centros de datos, almacenes u otros espacios físicos críticos.
- Tecnológico: Se inspecciona la infraestructura digital, incluidos dispositivos móviles, servidores, routers, switches y otros activos de red.
- Humano: Se evalúa la preparación del personal interno, contratistas o socios externos, especialmente aquellos con acceso privilegiado.
- Compilaciones de software: Se analiza cada nueva versión de software implementada en la organización, identificando fallos potenciales antes de su despliegue definitivo.

Tras la ejecución de estas pruebas, se elabora un informe técnico detallado que se presenta a la gerencia. Este documento permite tomar decisiones fundamentadas en materia de ciberseguridad, así como establecer acciones correctivas y preventivas con el acompañamiento de especialistas.

Los principales sistemas y componentes tecnológicos evaluados incluyen:

- Servidores
- Firewalls
- Directorio Activo
- Switches
- Routers
- Servidores de bases de datos
- Servidores de aplicaciones
- Estaciones de trabajo

Pruebas de Penetración

Las pruebas de penetración (*penetration testing*) constituyen una técnica utilizada por las organizaciones para identificar vulnerabilidades en sus sistemas e infraestructura tecnológica. Este procedimiento consiste en simular ataques reales, de forma controlada y autorizada por la administración, con el propósito de evaluar la seguridad de los componentes más expuestos o críticos. El objetivo principal es detectar fallos que podrían ser explotados por actores maliciosos, a fin de implementar medidas correctivas antes de que ocurran incidentes de seguridad (Montero, 2005).

Las pruebas de penetración (*penetration testing*) tienen como finalidad identificar vulnerabilidades en sistemas, redes o aplicaciones que podrían ser explotadas por actores no autorizados. Su propósito es subsanar dichas debilidades mediante acciones preventivas, antes de que puedan ser utilizadas para acceder de forma ilícita a información confidencial o comprometer la integridad del entorno digital de la organización.

La prueba de penetración, también conocida como *pentesting*, forma parte del enfoque de hacking ético y tiene como propósito evaluar la eficacia de los mecanismos de defensa implementados en un sistema o red. A través de un ataque simulado, se analiza si dichos mecanismos son capaces de prevenir accesos no autorizados u otras formas de intrusión. Una vez finalizada la simulación, se elabora un informe técnico detallado que documenta los hallazgos, las vulnerabilidades identificadas y una serie de recomendaciones orientadas a mejorar la postura de seguridad de la organización.

Planteamiento del problema

Una institución educativa de nivel medio superior, ubicada en la zona sur-oriente de la ciudad, tiene como propósito atender a la población circunvecina mediante sus servicios académicos. Posterior al incidente, se detectó que los servidores de su red fueron comprometidos por un ataque de infiltración, el cual permitió que un ciberintruso accediera a los sistemas internos.

Dicho intruso utilizó las vulnerabilidades existentes para realizar una carga no autorizada de archivos en el servidor web de la institución, específicamente bases de datos externas. Esta intrusión fue posible debido a la limitada seguridad informática implementada, así como a la presencia de puertos abiertos en el servidor, los cuales carecían de configuraciones de seguridad adecuadas y de un monitoreo constante.

Esta situación comprometió gravemente la integridad y confidencialidad de la información sensible almacenada en los sistemas institucionales, además de poner en riesgo la seguridad general de la red. El uso ilícito del servidor como espacio de almacenamiento externo puede generar consecuencias significativas, como el consumo indebido del ancho de banda, la degradación del rendimiento de los servicios educativos y la posible exposición de datos confidenciales de estudiantes y personal.

Adicionalmente, este incidente incrementa el riesgo de sanciones por incumplimiento de normativas de protección de datos, además de los costos operativos

asociados a la restauración del sistema, la implementación de medidas correctivas y la mejora de los mecanismos de seguridad digital.

Descripción del problema

La falta de implementación de medidas de ciberseguridad ha generado diversos problemas operativos, entre ellos, incumplimientos normativos que ponen en riesgo los registros académicos de los estudiantes y afectan negativamente el prestigio de la institución educativa. Esta situación ha provocado una disminución en la inscripción de nuevos estudiantes, así como en el reingreso de los alumnos que ya formaban parte de la institución.

Además, se evidencia una carencia de mecanismos adecuados de seguridad y monitoreo continuo, lo que compromete la infraestructura de red institucional. Entre las consecuencias de esta vulnerabilidad se encuentran el uso indebido del ancho de banda, que afecta directamente el rendimiento de los servicios educativos, y el riesgo de violaciones a la confidencialidad de datos sensibles de estudiantes y personal. A esto se suma la posibilidad de enfrentar sanciones por incumplimiento de normativas de protección de datos, así como costos adicionales derivados de la restauración de sistemas y la implementación de medidas correctivas para prevenir futuros incidentes.

Justificación

Dado que la información constituye un activo estratégico fundamental para cualquier organización, su protección debe asumirse como una prioridad. En este contexto, la ciberseguridad adquiere una relevancia crucial, al encargarse de preservar la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas informáticos (Pfleeger, Pfleeger y Margulies, 2015).

Por lo tanto, en México, las empresas, organizaciones e instituciones educativas de todos los niveles deben cumplir con el marco legal en materia de protección de datos personales, el cual incluye la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), así como la Norma Mexicana NMX-I-008-NYCE-2015, que establece directrices para la gestión de la seguridad de la información en las organizaciones. Estas normativas demandan que cualquier tratamiento de datos personales se realice bajo estrictas medidas de seguridad, tanto para evitar sanciones legales como para garantizar la confidencialidad de los datos.

En este sentido, es esencial proteger credenciales de acceso, configuraciones de sistema y demás componentes críticos que puedan dar lugar a filtraciones de información o poner en riesgo la reputación institucional. Para dar cumplimiento a dicho marco legal y prevenir la exposición de información sensible del personal docente, administrativo y estudiantil, resulta indispensable implementar un sistema de ciberseguridad robusto. Esto permitirá asegurar la continuidad operativa, mitigar riesgos asociados y fortalecer la resiliencia institucional frente a los desafíos del entorno digital actual.

Objetivo General

Fortalecer la infraestructura de ciberseguridad en la institución educativa mediante la identificación y corrección de vulnerabilidades en los servidores, la implementación de configuraciones de seguridad adecuadas, y el establecimiento de un sistema de monitoreo constante, con el fin de proteger la información sensible y garantizar la integridad y disponibilidad de los servicios educativos.

Objetivos Específicos

1. Realizar una auditoría de seguridad de los servidores y la red interna para identificar vulnerabilidades actuales, incluyendo puertos abiertos y configuraciones inadecuadas de los sistemas que puedan facilitar accesos no autorizados.
2. Desarrollar y aplicar políticas de seguridad para el cierre y control de puertos no necesarios en los servidores, con el fin de reducir la superficie de ataque y prevenir accesos indebidos.
3. Implementar mecanismos de autenticación y autorización más seguros que regulen el acceso a los servidores y servicios críticos, protegiendo los datos confidenciales de la institución, así como de los estudiantes y el personal.
4. Establecer un sistema de monitoreo y alerta en tiempo real que permita la detección inmediata de actividades inusuales o no autorizadas en los servidores, facilitando la respuesta oportuna ante intentos de infiltración.
5. Capacitar al personal de tecnologías de la información y a los usuarios internos en buenas prácticas de ciberseguridad, incluyendo el uso seguro de las redes y la importancia del monitoreo constante, con el objetivo de consolidar una cultura institucional de seguridad.

6. Documentar un plan de recuperación y respuesta ante incidentes de ciberseguridad que detalle los procedimientos para la contención, eliminación de amenazas y restauración de los servicios afectados, minimizando así el impacto ante futuros ataques.
7. Garantizar el cumplimiento de las normativas vigentes en materia de protección de datos mediante la revisión y mejora continua de las políticas de seguridad, fortaleciendo la confianza en la institución y disminuyendo el riesgo de sanciones regulatorias.

Metodología

Una metodología de seguridad consiste en seguir un conjunto estructurado de pasos destinados a identificar y analizar las amenazas potenciales que podrían comprometer la integridad, disponibilidad o confidencialidad de los activos de una organización. Este proceso incluye la evaluación de vulnerabilidades específicas, la estimación del nivel de riesgo asociado y el análisis de su posible impacto en las distintas áreas operativas. En la actualidad, existen diversos estándares, normativas y marcos metodológicos, tanto del ámbito público como privado, que contribuyen al diseño de una defensa robusta frente a incidentes de seguridad informática. Asimismo, la detección temprana de intrusiones y la implementación oportuna de medidas de contingencia permiten reducir la exposición de la organización frente a posibles ataques (Gómez González, 2012).

Principios de la Metodología de la Defensa

En este caso específico se implementaron los principios de metodología de la defensa, cuyo principal objetivo de protección es la "Organización en su Totalidad", en otras palabras, es considerar que lo que se requiere es un plan de defensa para la continuidad funcional de la organización y los objetivos de negocio (NCSA, 2017).

Por tanto, se describe lo anteriormente expresado de la siguiente manera:

1. Responsabilidad de la Dirección: La responsabilidad de proteger la información recae principalmente en la alta dirección de la organización. Una vez otorgada la autorización correspondiente y formalizado el contrato, se notificó a las partes interesadas el marco legal aplicable. Además, se estableció una planificación detallada y un alcance definido, en los que se precisaron los objetivos del proyecto, los límites de las pruebas y los tiempos

de respuesta esperados. Con la aprobación del proyecto, se dio inicio a la implementación de medidas orientadas al fortalecimiento de la ciberseguridad en la institución.

2. Defensa multicapa: La defensa cibernética es un proceso que integra tres componentes principales: personas, productos y procesos (las 3P). De acuerdo con Easttom (2018), es fundamental adoptar un enfoque de seguridad en múltiples capas para mitigar de manera eficaz las amenazas cibernéticas. Para ello, se requiere la combinación de herramientas tecnológicas con políticas de seguridad robustas y la capacitación continua del personal. Esta estrategia debe incluir la implementación de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), redes privadas virtuales (VPN) y prácticas de cifrado sólidas, con el fin de fortalecer las capacidades defensivas de la organización.
3. La defensa en profundidad o defensa multicapa: La defensa en profundidad, también conocida como defensa multicapa, es una estrategia de ciberseguridad que emplea múltiples capas de protección para mitigar riesgos y salvaguardar los activos críticos de una organización. Cada capa está diseñada para enfrentar distintos tipos de amenazas, generando redundancias que fortalecen la seguridad general. Para lograr una protección integral en la escuela preparatoria, se implementaron los siguientes puntos clave, destinados a garantizar un entorno seguro tanto para la infraestructura tecnológica como para los datos y usuarios:
    a. Seguridad física. Se establecieron controles de acceso mediante tarjetas inteligentes y lectores biométricos para restringir el ingreso a zonas críticas, como la sala de servidores. Estas áreas son monitoreadas constantemente por cámaras de vigilancia, mientras que los servidores y dispositivos clave están asegurados con cerraduras físicas robustas.
    b. Seguridad perimetral. En los límites de la red institucional se instalaron firewalls avanzados para filtrar el tráfico externo y prevenir accesos no autorizados. También se implementaron sistemas de detección y prevención de intrusos (IDS/IPS) que identifican y bloquean amenazas potenciales en tiempo real. Para garantizar conexiones remotas seguras de estudiantes y personal administrativo, se utiliza una red privada virtual (VPN).
    c. Seguridad de la red. La red interna fue segmentada en subredes y VLANs para separar las áreas administrativas de las estudiantiles, limitando así el movimiento lateral en caso de una intrusión. Se implementó monitoreo continuo del tráfico interno con el fin de detectar anomalías y prevenir actividades maliciosas.

d. Seguridad de los endpoints. Cada dispositivo conectado a la red cuenta con soluciones antimalware y antivirus actualizados. Se emplean sistemas de administración de dispositivos móviles (Mobile Device Management, MDM) y se aplican parches de seguridad de forma periódica, garantizando la protección frente a vulnerabilidades conocidas en los sistemas operativos.
e. Seguridad de las aplicaciones. Se adoptaron prácticas de programación segura, como la validación de entradas para prevenir ataques por inyección SQL y cross-site scripting (XSS). Asimismo, las aplicaciones críticas son sometidas a pruebas de vulnerabilidad y monitoreo continuo durante su operación.
f. Seguridad de los datos. Los datos sensibles son cifrados tanto en tránsito como en reposo, utilizando protocolos como TLS y AES. Se etiquetan según su nivel de confidencialidad y se aplican políticas de respaldo regular para asegurar su recuperación en caso de incidentes.
g. Gestión de identidades y accesos (IAM). Se implementó la autenticación multifactor (MFA) para acceder a sistemas críticos, junto con un modelo de privilegios mínimos que asegura que cada usuario solo pueda acceder a los recursos necesarios. Las cuentas con privilegios elevados son gestionadas mediante herramientas de Gestión de Accesos Privilegiados (PAM).
h. Concienciación y capacitación de usuarios. Se desarrollaron programas de capacitación periódica dirigidos a estudiantes, docentes y personal administrativo sobre prácticas seguras, incluyendo la detección de intentos de phishing. También se han realizado simulacros para evaluar y mejorar la respuesta ante posibles ataques.

Metodología de Defensa de la Estructura

Dado que las empresas u organizaciones operan en entornos dinámicos, la evolución tecnológica, la situación particular de cada empresa y los sectores en los que participan influyen directamente en la manera en que deben protegerse en el ciberespacio. La metodología propuesta exige que las organizaciones realicen evaluaciones periódicas de riesgos. Este análisis constituye la base para desarrollar un plan de trabajo a largo plazo, orientado a reducir vulnerabilidades mediante la implementación de los controles necesarios (NCSA, 2017).

El Proceso de Defensa Cíclico

La metodología de defensa propuesta se desarrolla de forma cíclica y se compone de tres etapas principales:

- Planificación y evaluación: consiste en rastrear los objetivos de defensa, realizar una evaluación de riesgos, inspeccionar los controles existentes y diseñar un plan de trabajo para cerrar las brechas detectadas.
- Ejecución del plan de trabajo: implica el desarrollo de procesos organizacionales, la integración de herramientas, así como la incorporación de la ciberdefensa dentro de la estructura organizativa.
- Actualización continua de las defensas: se debe responder al dinamismo del ciberespacio manteniendo actualizados tanto los procesos como las tecnologías de la organización. Esto incluye la instalación de nuevos equipos y redes, la adquisición de software avanzado, la incorporación de elementos como el Internet de las Cosas (IoT), la oferta de nuevos servicios como la computación en la nube, entre otros. Dado que las amenazas y métodos de ataque evolucionan constantemente, las herramientas de defensa deben adaptarse de forma continua.

Como complemento, se incluye una lista de cotejo ("checklist") con las etapas descritas para facilitar la implementación del ciclo con una periodicidad semestral, aunque esta puede ajustarse según las necesidades.

Tipos de Pruebas de penetración (penetration testing) realizados

Es relevante señalar las categorías en las que se clasifican las pruebas de penetración, también conocidas como pruebas de seguridad. Estas evaluaciones son realizadas por especialistas en pruebas de penetración, comúnmente denominados hackers éticos, quienes pueden aplicar uno o varios tipos de pruebas a los sistemas de las organizaciones. A continuación, se describen los principales tipos de pruebas:

- *Pruebas de Ingeniería Social:* este tipo de evaluación busca engañar a las personas para que revelen información confidencial sobre sí mismas o sobre la organización a la que pertenecen. Por esta razón, las personas pueden representar el eslabón más vulnerable dentro de un sistema de seguridad (Tori, 2008). Para su aplicación, se complementa con simulaciones y evaluaciones humanas, proporcionando una visión integral de la postura de seguridad de la institución. La combinación de pruebas técnicas (como las realizadas con herramientas como Nessus), las simulaciones de

ingeniería social y, especialmente, la capacitación del personal administrativo y docente, resulta fundamental para abordar tanto las vulnerabilidades técnicas como aquellas relacionadas con el factor humano.

- *Pruebas de Aplicaciones Web:* consisten en el uso de diversas herramientas de software para evaluar la seguridad del código de una aplicación web. Estas pruebas permiten identificar vulnerabilidades en el código y establecer mecanismos para mitigarlas, reduciendo así el riesgo de posibles ataques.
- *Pruebas de Penetración Física:* tienen como objetivo verificar que los dispositivos físicos de una organización solo sean accesibles por personal autorizado. Estas pruebas evalúan posibles vulnerabilidades en el acceso físico a los equipos y dispositivos críticos.
- *Pruebas de Firmware de Red:* se aplican a todos los puntos de entrada de una red, con el fin de analizar el tráfico de entrada y salida. Estas pruebas se pueden realizar tanto de manera local como remota para evaluar el comportamiento y la seguridad del firmware involucrado.
- *Pruebas del Lado del Cliente:* se enfocan en el software instalado en los equipos de los usuarios dentro de la organización, con el propósito de identificar vulnerabilidades en los componentes que interactúan con la infraestructura interna.
- *Pruebas de Red Inalámbrica:* consisten en escanear todos los puntos de acceso Wi-Fi dentro de una organización, con el fin de detectar posibles debilidades o configuraciones inseguras que puedan comprometer la red inalámbrica.

En la Tabla 1 se muestra el reporte del análisis de 14 puertos de los cuales solo 3 debiesen permanecer abiertos y bajo resguardo de un firewall, lo que significa que 11 puertos abiertos sin uso y que han sido utilizados para alguna infiltración.

Tabla 1. Puertos abiertos identificados mediante escaneo con Metasploit (db_nmap) al servidor 10.13.70.52.

Puerto	Estado	Servicio
135	Abierto	msrpc
139	Abierto	netbios-ssn
445	Abierto	microsoft-ds
623	Abierto	oob-ws-http
1025	Abierto	NFS-or-IIS
1026	Abierto	LSA-or-nterm
1027	Abierto	IIS
1028	Abierto	desconocido
1049	Abierto	td-postman
1055	Abierto	ansyslmd
4444	Abierto	krb524
16992	Abierto	amt-soap-http
23130	Abierto	desconocido
23131	Abierto	desconocido

Nota: Datos generados mediante escaneo con el comando db_nmap -sS -p- 10.13.70.52 dentro del Metasploit Framework versión 6. Fuente: Rapid7 (2023).

En la Tabla 2 se muestra el extracto correspondiente al informe técnico generado tras un escaneo de seguridad a las aplicaciones y servicios de red mediante la herramienta Nessus. Los identificadores CVE han sido utilizados con fines ilustrativos.

Tabla 2. Vulnerabilidades detectadas mediante escaneo Nessus al host 192.168.1.100.

Puerto	Servicio	Severidad	CVE	Vulnerabilidad	Recomendación
445	SMB	Crítica	CVE-2017-0144	EternalBlue	Aplicar parche MS17-010 y deshabilitar SMBv1 si no es necesario.
4444	Remote Shell	Alta	CVE-2024-XXXXX	Acceso no autorizado	Deshabilitar el servicio o aplicar autenticación robusta.
623	IPMI	Alta	CVE-2022-XXXXX	Credenciales predeterminadas IPMI	Cambiar credenciales por defecto y restringir acceso con firewall.
1025	NFS-or-IIS	Media	CVE-2023-XXXXX	Acceso NFS no autenticado	Configurar autenticación y filtrar el tráfico hacia el puerto.
Nota: Datos extraídos del escaneo realizado el 13 de julio de 2023 con la herramienta Nessus. Fuente: Tenable (2023).					

Análisis de Resultados

Un análisis de los métodos de defensa frente a intrusiones permite identificar diversas áreas de oportunidad para mejorar la seguridad informática en una organización. A continuación, se presenta un examen técnico basado en los resultados obtenidos tras la implementación de distintos mecanismos de protección ante los accesos no autorizados sufridos por la institución educativa.

Informe de Pruebas de Seguridad - Análisis de Vulnerabilidades

En el marco de una evaluación de seguridad, se llevó a cabo un escaneo exhaustivo sobre una serie de puertos críticos, con el propósito de identificar posibles vulnerabilidades que pudieran comprometer la integridad y seguridad de la infraestructura de TI. El análisis fue realizado mediante el uso de Nessus, herramienta ampliamente reconocida en la detección de vulnerabilidades, lo que permitió obtener un diagnóstico preciso sobre los riesgos potenciales presentes en los sistemas.

Los resultados del escaneo evidenciaron diversas vulnerabilidades, algunas de ellas con un impacto considerable en la seguridad, por lo que deben ser atendidas con carácter prioritario. A continuación, se presentan los hallazgos más relevantes, clasificados según su nivel de severidad, junto con las correspondientes recomendaciones de mitigación.

1. Puerto 445: SMB (CVE-2017-0144 EternalBlue)

Severidad: *Crítica*

El puerto 445, asociado al servicio SMB, presenta una vulnerabilidad conocida como EternalBlue. Esta vulnerabilidad permite la ejecución remota de código, lo que podría ser explotado por atacantes para obtener acceso no autorizado y propagar malware a través de la red, como ocurrió en el ataque de WannaCry.

Recomendación: Es imperativo aplicar el parche MS17-010 de Microsoft para mitigar esta vulnerabilidad. Además, se debe deshabilitar el uso de SMBv1 si no es necesario para las operaciones de la red, ya que este protocolo obsoleto es el principal vector de ataque.

2. Puerto 4444: Remote Shell (Acceso no autorizado).

   Severidad: Alta.

El puerto 4444, comúnmente utilizado para conexiones remotas, presenta una vulnerabilidad crítica que permite el acceso no autorizado. Esta condición sugiere que un atacante podría establecer una conexión con el sistema sin autenticación previa, lo que constituye una amenaza grave para la integridad y seguridad del entorno.

Recomendación: Se recomienda deshabilitar cualquier servicio no esencial que utilice este puerto y reforzar la autenticación en todos los servicios críticos. Si es necesario utilizar este puerto, se deben aplicar controles estrictos de acceso y monitoreo.

3. Puerto 623: IPMI (Credenciales predeterminadas activas)

Severidad: Alta

En el puerto 623, correspondiente al servicio IPMI (Intelligent Platform Management Interface), se identificó el uso de credenciales predeterminadas. Esto permite que cualquier usuario con acceso a la red obtenga privilegios de administrador sobre el hardware, representando un grave riesgo para la seguridad del sistema.

Recomendación: Se deben cambiar de inmediato las credenciales predeterminadas del servicio IPMI y restringir el acceso a este puerto mediante reglas de firewall, permitiendo solo conexiones desde direcciones IP de confianza.

4. Puerto 1025: NFS (Servicio de acceso no autenticado)

Severidad: Media

En el puerto 1025, asociado al servicio NFS (Network File System), se encontró una configuración insegura que permite acceso no autenticado a directorios compartidos. Este tipo de configuración expone a los sistemas a riesgos de divulgación de información sensible y a la manipulación de datos.

Recomendación: Se recomienda restringir el acceso al servicio NFS mediante el uso de **firewall** y configurar adecuadamente la autenticación para prevenir accesos no autorizados a recursos compartidos.

Los resultados obtenidos durante el escaneo evidencian que los sistemas actuales se encuentran expuestos a diversas vulnerabilidades críticas que requieren atención inmediata. La detección de la vulnerabilidad EternalBlue en el puerto 445, así como la presencia de credenciales predeterminadas en IPMI, constituyen riesgos de alta severidad que pueden ser explotados para llevar a cabo accesos no autorizados y comprometer la infraestructura tecnológica.

Con el objetivo de mitigar estos riesgos, se recomienda implementar las siguientes acciones:

1. Aplicación de parches de seguridad: Es imprescindible actualizar los sistemas afectados mediante la instalación de los parches correspondientes, en particular aquellos que corrigen la vulnerabilidad EternalBlue y eliminan el uso de credenciales predeterminadas en IPMI.
2. Desactivación de servicios innecesarios: Aquellos servicios o puertos que no resulten esenciales para la operación deben ser deshabilitados o restringidos, con el fin de reducir la superficie de exposición ante posibles ataques.
3. Fortalecimiento de las configuraciones de seguridad: Se debe garantizar una configuración segura de los servicios de red, implementando autenticación robusta y restringiendo el acceso a puertos sensibles únicamente a direcciones IP autorizadas.
4. Ejecución de auditorías periódicas: La realización continua de escaneos y revisiones de seguridad permite identificar nuevas vulnerabilidades y verificar la efectividad de las medidas correctivas aplicadas.

Las pruebas de seguridad efectuadas han permitido identificar áreas críticas que demandan atención prioritaria. La aplicación de las recomendaciones descritas contribuirá significativamente al fortalecimiento de la postura de seguridad institucional, reduciendo la posibilidad de explotación y elevando el nivel de protección de la infraestructura.

La implementación de métodos de defensa ante ataques generó mejoras importantes en la seguridad informática de la organización. Por un lado, la adopción de sistemas de detección y respuesta a intrusiones (IDS/IPS) permitió identificar las amenazas de manera más rápida, lo que redujo significativamente el tiempo de permanencia de los atacantes en el sistema. Además, el uso de firewalls avanzados y la segmentación de redes fortaleció el control sobre el tráfico, limitando tanto las infiltraciones como la propagación lateral de los ataques.

La gestión de vulnerabilidades, a través de actualizaciones periódicas y auditorías de seguridad, contribuyó a disminuir la exposición a fallos conocidos. Asimismo, se reforzó la autenticación mediante métodos como la autenticación multifactorial (MFA), lo cual dificultó el acceso no autorizado y protegió los recursos críticos de la organización.

También se logró una mayor protección de los datos gracias al cifrado tanto en tránsito como en reposo, lo que garantizó la confidencialidad de la información, incluso en caso de una posible intrusión. Finalmente, al fomentar una cultura de seguridad entre los empleados, se logró reducir el riesgo de errores humanos como hacer clic en enlaces de phishing, fortaleciendo así la postura general de ciberseguridad. Como resultado de esta nueva estrategia, se elaboró una lista de cotejo que servirá para realizar auditorías periódicas o cuando lo requiera el nuevo personal encargado del centro de cómputo.

Checklist de Revisión y Verificación de Seguridad

1. Seguridad Física

- [ ] ¿Existen controles de acceso mediante tarjetas, biometría o códigos de seguridad para áreas críticas?

- [ ] ¿Se cuenta con cámaras de vigilancia operativas y ubicadas estratégicamente?

- [ ] ¿Están los servidores y dispositivos críticos protegidos con cerraduras físicas?

- [ ] ¿Se dispone de guardias de seguridad capacitados en procedimientos de emergencia?

2. Seguridad Perimetral

- [ ] ¿Se han implementado firewalls para controlar el tráfico entrante y saliente?

- [ ] ¿Están instalados sistemas IDS/IPS para la detección y prevención de intrusos?

- [ ] ¿Se utiliza una VPN para accesos remotos de personal y estudiantes?

3. Seguridad de la Red

- [ ] ¿Está la red segmentada en subredes y VLANs para limitar el acceso interno?

- [ ] ¿Existe un sistema de monitoreo constante del tráfico interno de la red?

- [ ] ¿Se han configurado reglas de filtrado para tráfico interno sospechoso?

4. Seguridad de los Endpoints

- [ ] ¿Todos los dispositivos conectados cuentan con antimalware y antivirus actualizados?

- [ ] ¿Se realizan actualizaciones y parches de software regularmente?

- [ ] ¿Se utilizan herramientas de gestión de dispositivos móviles (MDM)?

5. Seguridad de Aplicaciones

- [ ] ¿Se realiza validación de entrada en todas las aplicaciones críticas?

- [ ] ¿Se aplican pruebas de seguridad (DevSecOps) en las aplicaciones durante el desarrollo?

- [ ] ¿Se monitorean y escanean las aplicaciones regularmente en busca de vulnerabilidades?

6. Seguridad de los Datos

- [ ] ¿Están los datos sensibles cifrados en tránsito (TLS/SSL) y en reposo (AES)?

- [ ] ¿Se han clasificado y etiquetado los datos según su nivel de sensibilidad?

- [ ] ¿Se cuenta con políticas de respaldo regular y pruebas de recuperación?

7. Gestión de Identidades y Accesos (IAM)

- [ ] ¿Está activa la autenticación multifactor (MFA) en todos los sistemas críticos?

- [ ] ¿Se aplica el principio de privilegios mínimos para los usuarios?

- [ ] ¿Se gestiona adecuadamente el acceso a cuentas privilegiadas (PAM)?

8. Concienciación y Capacitación de Usuarios

- [ ] ¿Se realizan capacitaciones periódicas sobre ciberseguridad para estudiantes y personal?

- [ ] ¿Se han implementado simulacros de phishing para evaluar la respuesta de los usuarios?

- [ ] ¿Existen políticas claras y difundidas sobre el uso de recursos tecnológicos?

Con esta lista de cotejo “checklist” es posible verificar de manera sistemática la implementación y cumplimiento de medidas de seguridad esenciales para proteger la infraestructura y datos de la institución educativa.

Limitaciones del Estudio

No obstante, este estudio presenta diversas limitaciones que deben considerarse. En primer lugar, la efectividad de los métodos propuestos depende en gran medida de su correcta implementación y de la capacitación de los usuarios. Si las tecnologías no se adoptan de forma adecuada, su impacto puede disminuir significativamente. Un ejemplo de ello es la autenticación multifactor, que en algunos casos puede ser percibida como un obstáculo operativo, lo cual podría limitar su adopción generalizada.

En segundo lugar, la dependencia de herramientas basadas en inteligencia artificial y aprendizaje automático también representa un desafío. Aunque estas tecnologías ofrecen grandes ventajas, pueden generar falsos positivos o no responder eficazmente ante amenazas emergentes, lo que deja a las organizaciones expuestas a ciertos riesgos.

Una tercera limitación se relaciona con la segmentación de redes. A pesar de ser una práctica recomendada en seguridad, su implementación en infraestructuras amplias puede resultar compleja y generar dificultades en la comunicación entre sistemas.

Finalmente, es fundamental señalar que ninguna solución de ciberseguridad elimina por completo el riesgo; más bien, contribuyen a reducirlo. Dado que las tácticas empleadas por los atacantes evolucionan constantemente, es indispensable adoptar un enfoque dinámico y adaptativo en la gestión de la seguridad informática.

Discusión

El ámbito educativo enfrenta múltiples desafíos en materia de ciberseguridad, siendo especialmente vulnerable a incidentes como el correo no deseado (spam), ataques de ingeniería social (phishing) y diversas formas de delitos informáticos, tanto por parte de individuos con conocimientos especializados como de personas sin formación técnica, motivadas por fines económicos o personales.

Las brechas de seguridad en las instituciones educativas son frecuentes debido a varios factores, entre los que destacan la falta de capacitación del personal encargado de los sistemas informáticos, la dependencia creciente de plataformas digitales, la limitada disponibilidad de recursos tecnológicos y financieros, así como la gestión de información sensible. Estos elementos en conjunto posicionan al sector educativo como un objetivo propenso a amenazas cibernéticas, requiriendo estrategias integrales de protección y concientización.

Este tipo de problemáticas, como la ocurrida en esta institución debido a las vulnerabilidades identificadas, podrían haber derivado en una amenaza informática de mayor gravedad, como un ataque de ransomware. Este tipo de ataque cibernético implica el uso de software malicioso que cifra los archivos y datos de la víctima, con el objetivo de exigir un rescate, comúnmente en criptomonedas, dificultando así el rastreo de los responsables. En este caso particular, se detectaron correos electrónicos en los que se solicitaba un pago a cambio de no comprometer los sistemas de almacenamiento del servidor.

Ante este tipo de riesgos, resulta fundamental la capacitación del personal responsable en el uso de herramientas adecuadas para la protección de la infraestructura informática. Entre estas herramientas se encuentran los firewalls, cuya aplicación práctica permite el análisis y control de los diferentes puertos de comunicación. En este contexto, el uso de soluciones de seguridad tanto de software como de hardware debe estar debidamente fundamentado en criterios técnicos y de eficacia comprobada. Por ejemplo, McAfee Firewall Enterprise es una herramienta reconocida por su capacidad para aplicar políticas de seguridad detalladas y por integrar análisis de amenazas en tiempo real, lo cual resulta esencial en entornos institucionales. Asimismo, dispositivos de seguridad perimetral como el D-Link DFL-2560 Office Firewall ofrecen filtrado de contenido, inspección profunda de paquetes y segmentación de red, lo que refuerza la defensa ante accesos no autorizados y ataques externos.

Los resultados obtenidos en este trabajo coinciden con estudios previos que enfatizan la importancia de implementar sistemas de detección y prevención de intrusiones (IDS/IPS), firewalls avanzados y segmentación de redes para proteger infraestructuras críticas de TI (Abrahams et al., 2024).

Los resultados obtenidos en este estudio evidencian patrones relevantes de vulnerabilidad en la infraestructura de ciberseguridad del sector educativo, especialmente en lo relacionado con la gestión de puertos de comunicación y la adopción de medidas preventivas. Estas conclusiones coinciden de manera significativa con lo reportado por McAfee en su *Informe de Amenazas Móviles* (Carroll, 2019), en el cual se señalaron vulnerabilidades similares en dispositivos del Internet de las Cosas (IoT) utilizados en entornos institucionales, lo que pone de manifiesto una problemática estructural persistente en este sector.

La explotación de puertos específicos como el 445, 4444, 623 y 1025 concuerda con los patrones de ataque documentados en el caso de EternalBlue (CVE-2017-0144). Este comportamiento confirma que las vulnerabilidades presentes en servicios básicos de red siguen representando vectores de ataque predominantes. Esta observación es consistente con investigaciones previas sobre el ataque WannaCry, el cual aprovechó debilidades similares en el protocolo SMB.

Un rasgo distintivo de este estudio es la identificación de la relación entre las limitaciones presupuestarias y la implementación de medidas de seguridad en instituciones educativas públicas. A diferencia de investigaciones previas centradas en aspectos técnicos

como el análisis del ataque de la botnet Mirai a DYN (Herrero, 2022), nuestros hallazgos destacan la relevancia de los factores socioeconómicos en la gestión de la ciberseguridad educativa. Asimismo, se evidencia una brecha considerable en la capacitación del personal técnico, en consonancia con estudios similares. No obstante, esta investigación aporta un enfoque propositivo al sugerir soluciones concretas, como la adopción de sistemas IDS/IPS y honeypots, viables dentro de las restricciones presupuestarias de las instituciones públicas.

Las limitaciones de nuestro estudio incluyen la focalización en un único caso institucional y la ausencia de un análisis longitudinal que permita evaluar la efectividad de las medidas correctivas implementadas. No obstante, nuestros hallazgos contribuyen significativamente al campo al proporcionar evidencia empírica sobre la necesidad de soluciones de ciberseguridad económicamente viables para el sector educativo público.

A diferencia de otros sectores, como el automotriz donde casos como el de Volkswagen han evidenciado la explotación de vulnerabilidades desde el interior de las organizaciones, el presente estudio identifica amenazas principalmente de origen externo en el ámbito educativo. Esta diferencia subraya la necesidad de adoptar un enfoque específico en la gestión de la ciberseguridad para las instituciones educativas, considerando tanto el riesgo de amenazas externas como las restricciones presupuestarias que caracterizan al sector (Hotten, 2015).

Los resultados obtenidos amplían el conocimiento existente sobre la ciberseguridad en el sector educativo al proporcionar evidencia empírica sobre la efectividad de soluciones *open source* caracterizadas por su accesibilidad, flexibilidad y bajo costo como una alternativa viable para instituciones con recursos limitados, un aspecto que ha sido poco abordado en la literatura previa sobre ciberseguridad educativa.

En comparación con otros estudios que se centran exclusivamente en ambientes empresariales, como el trabajo de Pfleeger & Pfleeger (2021), nuestro enfoque incluye una perspectiva educativa, abordando tanto los desafíos técnicos como la formación de futuros ingenieros especializados en ciberseguridad. Este elemento diferencial permite no solo proteger los activos de la institución, sino también generar un impacto a largo plazo en el desarrollo de competencias en el ámbito académico.

En cuanto al avance, este trabajo contribuye a cerrar una brecha en la literatura al proponer una metodología aplicable al ámbito educativo, que integra prácticas de defensa multicapa y procesos de capacitación continua. Esta propuesta no solo refuerza la

infraestructura tecnológica institucional, sino que también ofrece un modelo replicable para otros contextos educativos con desafío similares.

A pesar de los avances alcanzados, este estudio presenta ciertas limitaciones, como la dependencia de herramientas tecnológicas de alto costo y la necesidad de contar con un presupuesto adecuado para su implementación efectiva. No obstante, los resultados obtenidos, si bien alentadores, destacan la urgencia de mantener un enfoque dinámico y adaptable ante la evolución constante de las amenazas cibernéticas. En este sentido, la comparación con investigaciones anteriores enfatiza la relevancia de abordar la ciberseguridad desde una perspectiva integral, en la que converjan de manera coordinada la tecnología, los procesos y las personas, consolidando así un enfoque verdaderamente holístico y sostenible en el tiempo.

Sin embargo, muchas instituciones educativas, especialmente las públicas, enfrentan limitaciones presupuestales que dificultan la adquisición e implementación de estos sistemas, además de carecer de capacitación adecuada en herramientas y técnicas de ciberseguridad de código abierto.

Conclusiones

Los ataques mediante intrusiones ocurren con mayor frecuencia a medida que la tecnología y la web evolucionan, lo que conlleva también la sofisticación de las técnicas empleadas para vulnerar sistemas con fines ilícitos. En consecuencia, la ciberseguridad ha adquirido una importancia creciente en la protección de los activos informáticos de las instituciones educativas. Por ello, es fundamental implementar medidas que salvaguarden los sistemas y redes ante intentos de acceso no autorizado por parte de actores malintencionados que buscan obtener beneficios ilegítimos.

Este estudio no solo aborda la mitigación de riesgos cibernéticos en la institución educativa, sino que también sienta un precedente relevante a nivel institucional para la formación de futuros ingenieros en sistemas especializados en ciberseguridad. La implementación de métodos de defensa, tales como pruebas de penetración, análisis de vulnerabilidades y monitoreo constante de la infraestructura tecnológica, crea un entorno propicio para que los estudiantes desarrollen habilidades prácticas en un contexto real y aplicable.

Mediante estas prácticas, los futuros ingenieros podrán enfrentarse a escenarios reales que les permitirán desarrollar competencias esenciales en áreas clave, tales como la detección de intrusiones, el manejo adecuado de incidentes de seguridad y la configuración de sistemas de protección robustos. Asimismo, la incorporación de herramientas especializadas, como firewalls avanzados y sistemas IDS/IPS, junto con la aplicación de metodologías de defensa en profundidad, fortalecerá su capacidad para diseñar e implementar estrategias de ciberseguridad efectivas y adaptadas a las particularidades de diversas organizaciones.

De esta manera, la experiencia generada por este proyecto contribuirá no solo a la protección de los activos digitales de la institución, sino que también funcionará como una plataforma educativa fundamental para la formación de una nueva generación de especialistas, quienes asumirán el liderazgo en seguridad cibernética en un entorno cada vez más digitalizado. Así, el proyecto no solo fortalece la capacidad operativa institucional, sino que también impulsa el desarrollo académico y profesional necesario para enfrentar los desafíos futuros en el ámbito de la ciberseguridad.

Recomendaciones

Es fundamental implementar medidas preventivas para proteger la información y la infraestructura de una organización, con el objetivo de evitar accesos maliciosos, tales como el robo o la destrucción de datos y activos. La administración debe contar con un equipo especializado encargado de realizar auditorías periódicas a los dispositivos internos utilizados por los colaboradores, así como a los equipos de terceros que tengan acceso a los sistemas de la organización. Estas acciones contribuyen a fortalecer la seguridad y minimizar los riesgos asociados a posibles intrusiones no autorizadas.

El fomento y la capacitación del personal de la organización para adoptar prácticas tecnológicas y de seguridad que protejan el entorno frente a ataques de intrusión. Se deben establecer restricciones de acceso para los usuarios de la organización a redes, información, bases de datos y correos electrónicos, de manera que estos recursos sean utilizados únicamente en el ejercicio de sus funciones laborales. Asimismo, se deben regular los accesos a servicios alojados en la nube, garantizando que el nivel de acceso a la información se mantenga adecuado durante la realización de labores en modalidad de acceso remoto.

La implementación de una política de uso de software de ciberseguridad, como firewalls, antivirus y antimalware, debe ser cumplida por todos los empleados de una

organización. Asimismo, se recomienda establecer controles estrictos sobre el manejo y la protección de la información confidencial.

Se recomienda que se realicen respaldos de seguridad de los datos, tanto en la infraestructura virtual (en la nube) como en la documentación histórica. Además, es necesario asegurar el acceso mediante un sistema de autenticación robusto, que emplee herramientas específicas, como aplicaciones o tokens generadores de códigos únicos.

Referencias

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5*(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

Ariel y Fundación Telefónica (2016). *Ciberseguridad, la protección de la información en un mundo digital,* Editorial Ariel y Editorial Planeta.

Asad, F. & Steltzer, H. (2025). Artificial Intelligence in Cyber Defense: Predicting and Preventing Cyber Threats. 10.13140/RG.2.2.33128. https://www.researchgate.net/publication/388848352_Artificial_Intelligence_in_Cyber_Defense_Predicting_and_Preventing_Cyber_Threats

Carroll, E., Dunton, T., Fokker, J., Lancioni, G., Munson, Y., Roccia, T., Samani, R., Sarukkai, S., Sommer, D. & Woodward, C. (2019). Amenazas móviles McAfee. Capital Software. https://capitalsoftware.com.ni/informe-de-predicciones-de-amenazas-de-mcafee-labs-2019/

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, 103614. https://doi.org/10.1016/j.compind.2022.103614

Diogenes, Y. y Ozkaya, E. (2018), *Cybersecurity – Attack and Defense Strategies*, Packt Publishing Ltd. https:/www.tsoungui.fr/ebooks/CYBER-Security.pdf

Easttom, C. (2018). Network Defense and Countermeasures; Principles and practices. Pearson.

Giménez, V. (2011). *Hacking y Ciberdelito*. Universitat Politécnica de Valencia, https://riunet.upv.es/server/api/core/bitstreams/c744b4de-4c52-463c-9556-984ab6148ade/content

Gómez González, I. C. (2012). *Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL* (Trabajo de grado, Ingeniería en Telecomunicaciones). Universidad Militar Nueva Granada, Bogotá, Colombia. Recuperado de https://repository.umng.edu.co/server/api/core/bitstreams/fde2bafc-c534-4152-a089-e29af7a1cbbc/content

Hotten, R. (2015, December 10). *Volkswagen: The scandal explained*. BBC News. https://www.bbc.com/news/business-34324772

Herrero, M. (2022). Estudio, despliegue y modificación de la Botnet Mirai. [Tesis de pregrado, Universidad de Alcalá Escuela Politécnica Superior] Biblioteca Digital Universidad de Alcalá. https://ebuah.uah.es/dspace/handle/10017/54033

Keyed Systems LLC. (s. f.). *Understanding the Consequences of Cyber Attacks on Infrastructure*. https://keyedsystems.com/understanding-the-consequences-of-cyber-attacks-on-infrastructure/

Kiser, Q. (2021). Ciberseguridad: Una simple guía para principiantes sobre ciberseguridad, redes informáticas y cómo protegerse del hacking en forma de phishing, malware, ransomware e ingeniería social. Editorial Primasta.

Kissel, R. (2013). *Glossary of key information security terms* (NIST IR 7298r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r2

Montero, V. (2005). *Técnicas de Penetration Testing*, CYBSEC Security System, Buenos Aires Argentina, septiembre 2005.

National Cyber Security Authority (NCSA) (2017), **"**Cyber Defense Methodology For An Organization**",** NATIONAL CYBER SECURITY AUTHORITY, June 2017.

Rapid7. (2023). *Metasploit Framework (Version 6)* [Computer software]. https://www.metasploit.com

Rashid, A.,Chivers, H., Danezis, G., Lupu, E. y Martin, A. (2019), *The Cyber Security Body of Knowledge*, The National Cyber Security Centre. https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf.

Sánchez, G. (2018), Seguridad Cibernética: Hackeo Ético y Programación defensiva. Alfaomega Grupo Editor, S.A. de C.V.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Tenable. (2023). *Nessus Vulnerability Scanner (Versión de julio de 2023)* [Computer software]. https://www.tenable.com/products/nessus

Tori, C. S. (2008). *Hacking ético* [Manuscrito autoeditado]. Rosario, Argentina. Recuperado de WordPress: https://nebul4ck.wordpress.com/wp-content/uploads/2015/08/hacking-etico-carlos-tori.pdf?utm_source=chatgpt.com

Vañó-Chic, J. (2014). Exploits. Universitat Oberta de Catalunya. UOC.

Rol de Contribución	Autor (es)
Conceptualización	Juan Manuel Bernal Ontiveros
Metodología	Francisco Zorrilla Briones
Software	Noé Ramón Rosales Morales
Validación	Francisco Zorrilla Briones
Análisis Formal	Francisco Zorrilla Briones
Investigación	Marisela Palacios Reyes
Recursos	Noé Ramón Rosales Morales
Curación de datos	Marisela Palacios Reyes
Escritura - Preparación del borrador original	Marisela Palacios Reyes
Escritura - Revisión y edición	Juan Manuel Bernal Ontiveros
Visualización	Susan Alexandra Cervantes Cárdenas
Supervisión	Juan Manuel Bernal Ontiveros
Administración de Proyectos	Marisela Palacios Reyes
Adquisición de fondos	N/A