Estrategias disruptivas de ciberseguridad: abordando las amenazas informáticas emergentes en el ámbito empresarial, educativo y gubernamental

Julián Estévez Herrera

Asesor

Joan Sebastián Bustos Miranda

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2025

Resumen

En la denominada “Era Digital”, la omnipresencia de la tecnología ha dado paso a una multiplicación de amenazas cibernéticas, desafiando la seguridad de los datos e infraestructuras digitales. Este estudio aborda el problema crítico de la ciberseguridad, destacando la evolución constante de las amenazas y la expansión del Internet de las Cosas. La presente monografía busca abordar de manera integral estos desafíos, proponiendo estrategias de ciberseguridad que anticipen y respondan eficientemente a las amenazas emergentes, investigando los problemas de seguridad cibernética asociados con la tecnología actual, analizando las implicaciones de la interconexión global de dispositivos y servicios, se proponen soluciones para fortalecer la protección de datos y sistemas en la Era Digital. Los objetivos específicos incluyeron explorar a fondo las amenazas cibernéticas más recientes, analizar desafíos relacionados con la adopción masiva de servicios en la nube y evaluar críticamente las soluciones de ciberseguridad actuales. Se pretende comprender la naturaleza cambiante de las vulnerabilidades y proponer mejoras basadas en experiencias y mejores prácticas, contribuyendo a un entorno digital más seguro y resistente frente a amenazas cibernéticas actuales y futuras.

Palabras clave: Ciberseguridad, Era Digital, Amenazas Cibernéticas, Internet de las Cosas (IoT), Servicios en la Nube.

Abstract

In the so-called “Digital Era”, the omnipresence of technology has led to a proliferation of cyber threats, challenging the security of data and digital infrastructures. This study addresses the critical issue of cybersecurity, highlighting the ongoing evolution of threats and the expansion of the Internet of Things. This monograph seeks to comprehensively address these challenges by proposing cybersecurity strategies that anticipate and efficiently respond to emerging threats. By investigating cybersecurity issues associated with current technology, analyzing the implications of the global interconnection of devices and services, solutions are proposed to enhance data and system protection in the Digital Era. Specific objectives include thoroughly exploring the latest cyber threats, analyzing challenges related to the widespread adoption of cloud services, and critically evaluating current cybersecurity solutions. The aim is to understand the changing nature of vulnerabilities and propose improvements based on experiences and best practices, contributing to a safer and more resilient digital environment against current and future cyber threats.

Keywords: Cybersecurity, Digital Era, Cyber Threats, Internet of Things (IoT), Cloud Services.

Contenido

Lista de Tablas

Lista de Figuras

Introducción

En la era digital actual, la ciberseguridad se ha convertido en un componente importante para la protección de la información y la infraestructura tecnológica. Las amenazas cibernéticas evolucionan constantemente, obligando a desarrollar y aplicar técnicas de seguridad innovadoras y avanzadas. Este estudio se centra en tres aspectos críticos de la ciberseguridad: analizar las técnicas recientes, correlacionar estrategias avanzadas de protección y evaluar la eficacia de las soluciones de protección de datos.

Inicialmente, se analizarán las técnicas de ciberseguridad más recientes para comprender la naturaleza cambiante de las vulnerabilidades en la tecnología actual. El avance de tecnologías como el aprendizaje automático y la criptografía cuántica ha permitido desarrollar métodos de defensa más robustos, aunque también ha creado nuevas áreas de riesgo. Este análisis proporcionará una visión integral de cómo estas técnicas se están aplicando y adaptando para enfrentar las amenazas emergentes.

En segundo lugar, se correlacionarán las estrategias avanzadas de protección cibernética con el objetivo de anticipar y responder eficazmente a las amenazas informáticas. La implementación de sistemas de monitoreo continuo, la inteligencia artificial y los protocolos de respuesta rápida son esenciales para minimizar el impacto de los ataques cibernéticos. Estas estrategias no solo deben ser efectivas en la detección y respuesta, sino también en la anticipación de posibles amenazas.

Finalmente, se evaluará la eficacia de las soluciones de protección de datos en entornos digitales para mitigar los riesgos de pérdida o robo de información confidencial. La gestión de Identidades y Accesos (GIA) y las auditorías de seguridad son fundamentales para asegurar que la información sensible se mantenga protegida frente a actores malintencionados.

Este trabajo tiene como propósito ofrecer una visión detallada y actualizada de las técnicas y estrategias de ciberseguridad, proporcionando una comprensión profunda de cómo se están abordando las vulnerabilidades en el entorno tecnológico actual. A través de un análisis exhaustivo, se busca contribuir al desarrollo de prácticas más efectivas y resilientes en la protección cibernética.

Planteamiento del Problema

En la Era Digital, el uso generalizado de tecnologías de la información y comunicación (TIC) ha cambiado profundamente cómo interactuamos con el mundo. La expansión de dispositivos conectados a Internet, conocidos como el Internet de las Cosas (IoT), ha permitido automatizar procesos y aumentar la eficiencia en diversos sectores. Sin embargo, esta creciente interconexión también ha ampliado la exposición a amenazas cibernéticas, creando nuevos desafíos en términos de ciberseguridad.

A medida que las tecnologías de protección avanzan, las amenazas también evolucionan, utilizando métodos más sofisticados y adaptables que superan las defensas tradicionales. Los ciberdelincuentes están aprovechando herramientas avanzadas como el aprendizaje automático y la inteligencia artificial para detectar vulnerabilidades y atacar con mayor precisión. Esto se complica por la falta de conocimiento y conciencia en muchos usuarios, quienes no siempre cuentan con los recursos o la información necesarios para implementar medidas de seguridad efectivas.

No enfrentar adecuadamente estas amenazas puede tener consecuencias graves. Las violaciones de seguridad pueden resultar en pérdida de datos confidenciales, robo de información o compromiso de dispositivos conectados, afectando tanto la privacidad como la economía de las personas y organizaciones. La interconexión de sistemas críticos aumenta la gravedad de los posibles ataques, ya que el daño no se limita al ámbito digital, sino que puede extenderse a la vida real.

A pesar de la creciente preocupación por la seguridad cibernética, todavía existe una brecha en el desarrollo de estrategias disruptivas que sean efectivas frente a estas amenazas emergentes. Las soluciones tradicionales, diseñadas principalmente para proteger a grandes

corporaciones, no siempre son adecuadas para entornos más pequeños o específicos. Esto subraya la necesidad urgente de desarrollar estrategias innovadoras, capaces de adaptarse a la rapidez con la que evolucionan las ciberamenazas.

El problema central que esta investigación aborda es la insuficiencia de las estrategias actuales de ciberseguridad para responder de manera efectiva a las amenazas emergentes. Se requiere la implementación de nuevas soluciones disruptivas que fortalezcan la protección digital y reduzcan los riesgos asociados a la pérdida de información confidencial y el acceso no autorizado a dispositivos.

Objetivos

Objetivo General

Proponer estrategias disruptivas de ciberseguridad que permitan una respuesta eficiente ante las amenazas informáticas emergentes, garantizando la protección integral de los activos digitales.

Objetivos Específicos

Analizar técnicas de ciberseguridad recientes, con el fin de comprender la naturaleza cambiante de las vulnerabilidades en la tecnología actual

Correlacionar estrategias avanzadas de protección cibernética para anticipar y responder eficazmente a amenazas informáticas

Evaluar la eficacia de soluciones de protección de datos en entornos digitales para mitigar riesgos de pérdida o robo de información confidencial.

Justificación

El avance constante de las tecnologías conectadas y la evolución de las amenazas cibernéticas exigen el desarrollo de estrategias de ciberseguridad disruptivas que puedan adaptarse a estos nuevos escenarios. La presente investigación busca cerrar el vacío en el conocimiento actual, ofreciendo soluciones innovadoras que respondan a las necesidades de seguridad en un mundo cada vez más digital. Además, esta investigación pretende servir como una guía para implementar mejores prácticas en ciberseguridad, contribuyendo al fortalecimiento de una cultura de protección digital eficiente y proactiva.

Marco Conceptual

Vivimos en un mundo completamente conectado, donde la tecnología forma parte de nuestra rutina diaria. Desde dispositivos inteligentes que controlan la temperatura de nuestras casas hasta los teléfonos que llevamos a todas partes, estamos inmersos en un entorno digital que conocemos como el Internet de las Cosas (IoT). Aunque este ecosistema nos facilita muchas tareas, también trae consigo desafíos de seguridad.

La ciberseguridad se encarga de protegernos en este escenario digital. Es el conjunto de prácticas y tecnologías diseñadas para resguardar sistemas, redes y datos de accesos no autorizados o ataques. Sin embargo, los ciberdelincuentes están constantemente mejorando sus métodos, utilizando herramientas avanzadas como la inteligencia artificial para detectar y explotar vulnerabilidades en los sistemas.

Las amenazas cibernéticas son acciones malintencionadas que buscan comprometer la seguridad digital, desde ataques de phishing hasta la propagación de malware. Estas amenazas aprovechan vulnerabilidades, que son puntos débiles en los sistemas o procesos, ya sea por errores en el software o fallos humanos. Cuando estas amenazas logran materializarse, hablamos de incidentes de seguridad, como el robo de datos o la interrupción de servicios esenciales.

En este contexto, proteger los datos se vuelve una prioridad. Esto abarca desde medidas básicas, como el uso de contraseñas seguras, hasta soluciones avanzadas como la criptografía, que garantiza que solo personas autorizadas puedan acceder a información confidencial. Además, la Autenticación Multifactor (MFA) añade una capa extra de seguridad al exigir más de una prueba para verificar la identidad de un usuario.

El IoT ha transformado nuestras vidas al conectar dispositivos cotidianos a internet, pero también introduce riesgos de seguridad únicos que requieren atención. Por su parte, la

computación en la nube ofrece grandes beneficios en términos de almacenamiento y accesibilidad, pero también implica nuevos retos para garantizar que los datos almacenados estén protegidos contra accesos no autorizados.

La inteligencia artificial se ha convertido en un aliado crucial en ciberseguridad. Gracias a su capacidad para analizar grandes volúmenes de datos en tiempo real, puede identificar patrones sospechosos y responder rápidamente a amenazas potenciales. Al mismo tiempo, la ciberseguridad cuántica emerge como una solución revolucionaria, aprovechando principios de la mecánica cuántica para crear sistemas de protección prácticamente inviolables.

La evolución de la ciberseguridad ha sido constante, desde las primeras medidas destinadas a proteger hardware local hasta los enfoques actuales que abarcan redes globales y entornos complejos como la nube y el IoT. Paralelamente, se han desarrollado leyes y regulaciones para garantizar un manejo seguro de la información. En Colombia, la Ley 1581 de 2012 establece directrices claras para la protección de datos personales, obligando a las organizaciones a implementar medidas que resguarden la privacidad de los usuarios.

Además, normas internacionales como la ISO/IEC 27001 ofrecen marcos para que las organizaciones gestionen su seguridad de manera estructurada y eficiente, promoviendo la adopción de buenas prácticas. Estas regulaciones son esenciales en un contexto donde los incidentes de seguridad no solo generan pérdidas económicas significativas, sino que también afectan la reputación de las organizaciones y exponen a las personas a riesgos adicionales.

Por todo esto, las estrategias disruptivas han ganado relevancia. No basta con mantener las medidas tradicionales; es necesario innovar y diseñar soluciones que puedan anticiparse a las amenazas emergentes. La combinación de diferentes tecnologías y enfoques, como la inteligencia artificial y la criptografía, permite fortalecer la defensa contra ataques cibernéticos,

mientras que la evaluación constante de estas soluciones garantiza su eficacia en distintos escenarios.

Marco Metodológico

Se realizaron búsquedas exhaustivas en bases de datos científicas especializadas, tales como Scopus, IEEE Xplore, Google Scholar, Scielo y ScienceDirect. La selección de los estudios se realizó bajo criterios específicos que garantizaran la pertinencia y calidad de los mismos. En primer lugar, se incluyeron estudios que cumplieran con los siguientes criterios:

Enfoque en técnicas recientes de ciberseguridad, protección cibernética, soluciones de protección de datos y amenazas emergentes en entornos informáticos.

Artículos y estudios publicados en los últimos años, que hayan sido revisados por pares y que cuenten con rigor científico.

Una vez recopilados, los artículos fueron filtrados por su relevancia en relación con el tema de interés. Se priorizaron aquellos estudios que analizaran en profundidad las técnicas de ciberseguridad, correlacionaran estrategias avanzadas de protección cibernética y abordaran la mitigación de riesgos asociados a la pérdida o robo de información confidencial.

Durante el proceso de selección, se consideraron combinaciones de palabras clave tanto en inglés como en español. Esto permitió ampliar el espectro de la búsqueda, asegurando que no se excluyeran estudios relevantes por limitaciones lingüísticas. Los términos clave fueron traducidos entre ambos idiomas respetando la sintaxis propia de cada uno. La palabra "ciberseguridad" fue central en la búsqueda, ya que permitió unificar las temáticas tratadas en los distintos estudios analizados.

Finalmente, se revisaron un total de 36 artículos científicos que proporcionaron los fundamentos teóricos y prácticos necesarios para la construcción de los capítulos de esta investigación.

Analizar Técnicas de Ciberseguridad Recientes, con el fin de Comprender la Naturaleza Cambiante de las Vulnerabilidades en la Tecnología Actual

Según el autor Arreola-García, 2019, la ciberseguridad tiene como objetivo principal proteger dos aspectos esenciales en los sistemas digitales: la información y la infraestructura, pero también busca asegurar la seguridad de quienes los utilizan. En otras palabras, se trata de proteger los recursos informáticos valiosos de cada persona, evitar el espionaje industrial y asegurar que la información estratégica que se usa para decisiones importantes, como la seguridad nacional, esté siempre a salvo. Además, la ciberseguridad se enfoca en proteger la infraestructura que sostiene toda esa información.

La tendencia creciente hacia el trabajo remoto ha traído consigo nuevos desafíos para la ciberseguridad. A medida que más empleados trabajan desde casa, la protección de datos y sistemas se ha convertido en una prioridad. Para mitigar los riesgos asociados con el acceso remoto, es fundamental implementar medidas de seguridad robustas. El uso de redes privadas virtuales (VPN) es una de las principales herramientas en este contexto. Las VPNs cifran las conexiones a Internet, protegiendo los datos transmitidos a través de redes públicas. Esto permite que los empleados accedan de forma segura a los recursos corporativos, simulando que están dentro de la red de la empresa. Además, es importante que las empresas utilicen VPNs de calidad, con protocolos de cifrado fuertes y actualizados, para hacer frente a amenazas emergentes.

Una medida importante es la autenticación multifactor (MFA), que agrega una capa extra de seguridad en el acceso a sistemas corporativos. La MFA requiere que los usuarios presenten dos o más pruebas de identidad, como contraseñas y códigos enviados a dispositivos adicionales. Esto reduce la probabilidad de ataques de phishing y accesos no autorizados, ya que incluso si un

atacante obtiene una contraseña, no podrá acceder al sistema sin el segundo factor de autenticación. Además de estas herramientas, las empresas deben establecer políticas de seguridad claras que definan el uso de dispositivos personales, el manejo de contraseñas y las restricciones para acceder a información sensible. Es fundamental que los empleados reciban formación continua sobre buenas prácticas de seguridad, para estar preparados ante las amenazas más comunes, como el phishing o el malware.

Con respecto a la seguridad de los dispositivos, se deben aplicar políticas de protección que incluyan el uso de software antivirus actualizado, la encriptación de discos y el uso de contraseñas robustas. Las empresas también pueden implementar soluciones de gestión de dispositivos móviles (MDM) para garantizar que los dispositivos estén protegidos y configurados de acuerdo con los estándares de seguridad corporativos. Estos enfoques, junto con la educación constante de los empleados, son fundamentales para mantener la seguridad en un entorno de trabajo remoto.

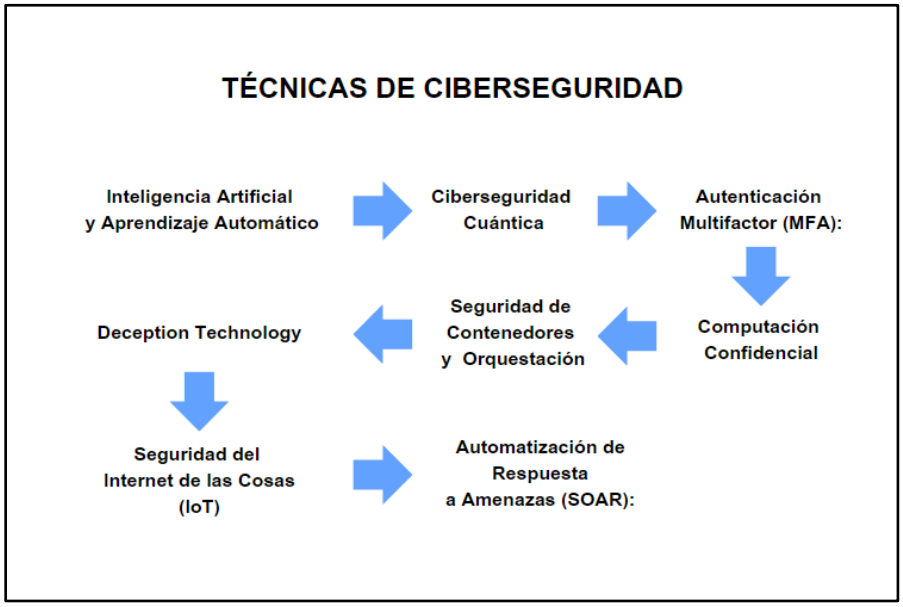
En cuanto al impacto de la computación cuántica en la ciberseguridad, esta tecnología representa tanto una amenaza como una oportunidad. Los ordenadores cuánticos tienen la capacidad de resolver problemas matemáticos complejos a una velocidad mucho mayor que los sistemas tradicionales, lo que podría hacer obsoletos muchos de los métodos de cifrado actuales.

La seguridad en el trabajo remoto requiere una combinación de herramientas tecnológicas como VPNs, MFA y políticas de seguridad bien estructuradas.

A continuación, la figura 1 desarrolla un conjunto de tecnologías avanzadas que refuerzan la seguridad digital, enfocándose en la automatización, la autenticación y la protección de entornos complejos, con el fin de prevenir y responder de manera efectiva ante posibles amenazas cibernéticas.

Figura 1

Esquema de las Técnicas de Ciberseguridad



Nota. Proceso secuencial de tecnologías avanzadas que refuerzan la seguridad digital, enfocándose en la automatización, la autenticación y la protección de entornos complejos, con el fin de prevenir y responder de manera efectiva ante posibles amenazas cibernéticas. *Fuente.* Autoría Propia

Inteligencia Artificial y Aprendizaje Automático

Para Rouhiainen (2018) la inteligencia artificial (IA) infiere la capacidad de las máquinas para llevar a cabo tareas que usualmente requieren inteligencia humana. Esto implica el uso de algoritmos, el aprendizaje a partir de datos y la toma de decisiones, todo sin necesidad de descanso y con la habilidad de procesar grandes volúmenes de información de manera eficiente.

La IA permite que las máquinas realicen trabajos que antes solo podían hacer los humanos, mejorando muchos aspectos de la vida cotidiana. No obstante, también es importante estar conscientes de los posibles riesgos y desventajas del rápido avance de la IA y estar preparados para gestionarlos adecuadamente.

Por otro lado, Nikolskaia y Naumov (2021) afirman que la inteligencia artificial (IA) es una tecnología con dos caras: puede ser utilizada tanto para llevar a cabo ataques maliciosos como para proteger contra riesgos de ciberseguridad. No obstante, su uso como herramienta de defensa está limitado por las regulaciones gubernamentales y de la Unión Europea. La adopción de técnicas de aprendizaje automático y profundo amplía el espectro de amenazas, creando nuevas vulnerabilidades y alterando las características habituales de los ataques. Además, la falta de transparencia y control sobre los sistemas de IA presenta desafíos importantes para evaluar su comportamiento en situaciones específicas, lo que resalta la necesidad de supervisión y auditoría humana en estos procesos.

Ciberseguridad Cuántica

Frente a este tema Yadav et al. (2023), explican que, en los sistemas de ciberseguridad potenciados por aprendizaje profundo y tecnología cuántica, la distribución de claves cuánticas (QKD) es esencial para asegurar las comunicaciones. Esta técnica utiliza principios de la física cuántica para crear claves de cifrado que, en teoría, son inviolables. La QKD se basa en el entrelazamiento cuántico, generando estados cuánticos entrelazados entre un emisor y un receptor, por ejemplo, si un emisor, un receptor y un espía intenta interceptar la clave, estos estados cuánticos detectarán su presencia. Ana y Carlos pueden verificar la seguridad de su intercambio midiendo ciertas propiedades cuánticas. La detección de espías en QKD se fundamenta en que cualquier interferencia con un estado cuántico causa una ruptura en su coherencia, lo cual es detectable. Ana y Carlos pueden identificar cualquier interferencia gracias

al estado cuántico representado por la secuencia "ACEACEAC" que aparece si un espía (Emma) está presente. La QKD es importante para la ciberseguridad mejorada cuánticamente porque asegura la privacidad de los datos transmitidos y proporciona una protección que los métodos tradicionales de criptografía no pueden ofrecer, siendo vital para proteger los canales de comunicación contra ataques cuánticos.

Autenticación Multifactor

Internet es una red pública con gran posibilidad de ataques, realizados para hacerse con el control de las redes conectadas. Los ataques en forma de repetición, descifrado de contraseñas por fuerza bruta y ataques de phishing amenazan con romper las implementaciones de autenticación de cualquier aplicación web expuesta a Internet. Las vulnerabilidades de robo de identidad en línea y secuestro de cuentas en las configuraciones de autenticación deben conectarse para lograr el cumplimiento de seguridad relacionado con la configuración de autenticación. La implementación del paradigma de autenticación multifactor multicapa, al seguir el enfoque de bloqueo múltiple, impide que los atacantes rompan fácilmente la configuración de autenticación.

En este sentido Chaudhari et al. (2011), destaca que los esquemas de autenticación basados en este enfoque ofrecen menos comodidad al usuario, pero proporcionan una seguridad superior, lo cual es vital para redes con baja confianza, como Internet. Se utilizan múltiples capas con diversos factores de autenticación, permitiendo el acceso a cada capa solo tras una autenticación exitosa en la capa anterior. En la última capa, además del usuario y la contraseña habituales, se incorporan factores adicionales de autenticación al esquema.

Computación Confidencial

Zhao et al. (2022) explican que según el Confidential Computing Consorcian (CC), este sistema protege los datos y el código en un entorno de ejecución confiable (TEE) basado en

hardware. Para mantener la integridad, CC divide la memoria física y asegura que solo las entidades autorizadas accedan a áreas de memoria específicas. En cuanto a la confidencialidad, CC utiliza motores de cifrado de memoria mejorados por hardware para evitar que los atacantes accedan al contenido de la memoria. Sin embargo, en la nube, para reducir costos y la dependencia del hardware, los proveedores como Amazon recurren a la virtualización para un aislamiento estricto, lo que requiere que los clientes confíen en el hipervisor privilegiado. Un aspecto importante de CC es la certificación remota, que proporciona evidencia verificable sobre la autenticidad del hardware subyacente y el estado de ejecución actual. Con esta certificación, los clientes de la nube pueden asegurarse de que su código sensible a la seguridad se esté ejecutando en un TEE genuino.

La seguridad en la computación en la nube es un tema clave dentro de la ciberseguridad, ya que aunque este entorno ofrece flexibilidad y escalabilidad, también plantea desafíos particulares. Uno de los principales problemas es la correcta configuración de los sistemas. Errores como otorgar permisos excesivos o almacenar datos sin cifrar son responsables de muchos incidentes de seguridad en la nube. Además, el hecho de que los recursos sean compartidos por múltiples usuarios puede incrementar el riesgo de violaciones si no se aplican medidas de aislamiento adecuadas.

Otro reto significativo es la dependencia de los proveedores de servicios en la nube. Los clientes confían en que estos aplicarán medidas de seguridad sólidas, pero en muchas ocasiones no tienen visibilidad sobre sus procesos internos. Esto hace evidente la importancia de establecer acuerdos claros y realizar auditorías periódicas para garantizar que los datos estén protegidos según los estándares requeridos.

Entre las prácticas más recomendadas para mejorar la seguridad en la nube se encuentra el cifrado de datos, tanto durante su transmisión como en almacenamiento. Este paso asegura que, incluso si la información es interceptada, no pueda ser usada sin las claves de descifrado. Asimismo, el uso de autenticación multifactor (MFA) es esencial para dificultar accesos no autorizados.

Otra medida clave es la segmentación de redes dentro de los entornos en la nube, que permite limitar el alcance de un ataque en caso de que ocurra una intrusión. También es fundamental establecer controles de acceso estrictos para asegurar que solo usuarios y sistemas autorizados puedan interactuar con información sensible.

Por último, resulta indispensable contar con sistemas de monitoreo constante y herramientas capaces de detectar amenazas en tiempo real. Soluciones basadas en inteligencia artificial son especialmente útiles para identificar comportamientos anómalos y enviar alertas antes de que un problema de seguridad se agrave. Además, disponer de un plan bien estructurado para responder a incidentes ayuda a mitigar las posibles consecuencias negativas.

Seguridad de Contenedores y Orquestación

De acuerdo con lo conceptuado por Naydenov y Ruseva (2023), se detalla que la orquestación de contenedores es un proceso automatizado que gestiona las cargas de trabajo, servicios y aplicaciones en contenedores. Este proceso abarca diversas operaciones, como aprovisionamiento, despliegue, mantenimiento y gestión del ciclo de vida de los contenedores. Además, la orquestación se encarga de integrar y organizar aplicaciones y servicios, así como de tareas como configuración, programación, asignación de recursos, garantía de disponibilidad, gestión de redes (como enrutamiento de tráfico y seguridad entre contenedores) y monitoreo.

Por su parte Khan (2017) destaca la importancia de los contenedores en la flexibilidad de las aplicaciones. Con el avance de las aplicaciones en la nube desde formas simples hasta

virtualizadas y la llegada de tecnologías como los contenedores y la computación sin servidor, se han logrado mejoras significativas en eficiencia, lo que ha abierto las puertas a una amplia gama de nuevas aplicaciones. Los contenedores se han utilizado para una variedad de propósitos, incluyendo la ejecución de servicios a largo plazo, procesamiento de lotes a gran escala, control de planos, Internet de las cosas y cargas de trabajo de inteligencia artificial.

Bajo este mismo paradigma, el surgimiento de los microservicios se explica como una solución al desafío de crear aplicaciones grandes capaces de escalar, actualizarse gradualmente y mantenerse operativas en entornos propensos a fallos. En este enfoque, una aplicación basada en microservicios se compone de múltiples unidades pequeñas, casi independientes, que se comunican mediante mensajes o eventos. Estas unidades, conocidas como microservicios, suelen ser empaquetadas en contenedores para su despliegue y gestión eficientes.

Deception Tecnology

Señalado por Park y Kim (2019), las estrategias comunes para llevar a cabo el ciberengaño involucran la suplantación de identidad y el establecimiento de una red trampa. La suplantación de identidad implica falsificar información para ganar acceso a sistemas o aproximarse a los defensores, mientras que la red trampa consiste en tender un señuelo para atraer a otros y esperar su acercamiento.

De acuerdo con Estrada (2020), un ciberengaño es un tipo de delito que utiliza Internet como su principal medio para llevarse a cabo. Estos ciberengaños han escalado a un problema crítico tanto para empresas como para particulares. Ejemplos de estos delitos incluyen mensajes que engañan a las personas para que realicen donaciones falsas, el uso de software malicioso para robar información, o la venta fraudulenta de productos que nunca llegan a entregarse.

La crisis ocasionada por el coronavirus y las medidas de confinamiento llevaron a muchas personas a realizar más compras y gestiones bancarias en línea, lo que no pasó

desapercibido para los delincuentes, quienes han enfocado su actividad en este entorno. Un ejemplo notable es el ataque informático conocido como "Ataque de doble factor (2FA)" reportado en 2020, que se disfraza en aplicaciones comunes como calculadoras o linternas, instalando código malicioso en dispositivos móviles. Este ataque monitorea aplicaciones, especialmente bancarias, capturando usuarios, contraseñas y códigos de seguridad, evadiendo la autenticación de doble factor que los bancos proveen. Para protegerse, se recomienda no instalar aplicaciones fuera de tiendas oficiales como Play Store o App Store y siempre revisar los comentarios de las apps. Estos ciberengaños no son nuevos; un ejemplo temprano fueron las estafas por correo electrónico, conocidas como "estafas nigerianas", en las que se pedían datos bancarios bajo el pretexto de recibir una herencia de un supuesto familiar fallecido.

Seguridad del Internet de las Cosas

En concordancia con Rodríguez y Geovanny (2015), se resalta que el Internet de las Cosas representa una evolución del Internet inicial, que estaba más centrado en las personas. Su potencial radica en la capacidad de integrar datos con personas, procesos y objetos. Mediante sensores, redes avanzadas de comunicación y análisis de datos a gran escala, se están desarrollando aplicaciones que prometen simplificar la vida cotidiana, mejorar los servicios de salud y educación, impulsar la innovación en ciudades, edificios y redes eléctricas inteligentes, fortalecer la seguridad de la información y aumentar la eficiencia tanto en empresas como en las administraciones públicas.

Por otro lado, según Ignacio et al. (2018), uno de los principales desafíos del Internet de las cosas (IoT) radica en las limitaciones humanas de tiempo, atención y precisión para capturar datos del mundo real. Esta limitación conlleva a problemas comunes al implementar dispositivos IoT. Uno de estos problemas es la abrumadora cantidad de datos que estos dispositivos pueden recopilar, almacenar y generar por sí mismos. Esta capacidad de los dispositivos IoT genera

preocupación en las empresas, ya que no están cómodas con la idea de que estos dispositivos puedan manejar una cantidad tan masiva de información.

Así que, el Internet de las Cosas (IoT) representa una evolución significativa en la forma en que interactuamos con el mundo, ofreciendo promesas de mejoras sustanciales en diversos aspectos de la vida cotidiana y en sectores como la salud, la educación y la infraestructura urbana. Sin embargo, junto con los beneficios potenciales, surgen desafíos importantes relacionados con la gestión y seguridad de la gran cantidad de datos generados por los dispositivos IoT. Abordar estas preocupaciones será importante para aprovechar plenamente el potencial transformador del IoT sin comprometer la privacidad y la seguridad de las personas y las organizaciones.

Automatización de Respuesta a Amenazas

Según Delgado (2017), los fallos típicos en la seguridad de Tecnología de la Información (TI) resaltan la falta de priorización de la seguridad, una respuesta inadecuada a las amenazas, sistemas de seguridad mal integrados, falta de formación para empleados, y reglas y procedimientos ineficientes, además de las amenazas internas. Estos problemas pueden aumentar los riesgos de seguridad y dificultar la respuesta a amenazas cibernéticas. La automatización de la respuesta a amenazas, como parte de una estrategia integral de ciberseguridad, puede solucionar varios de estos problemas al mejorar la eficiencia y la eficacia de la respuesta ante incidentes. Por ejemplo, la orquestación de seguridad puede acelerar la respuesta a incidentes, mientras que la automatización de procesos puede facilitar la implementación de medidas correctivas de forma rápida y consistente. Además, la integración de herramientas de seguridad puede proporcionar una visión más completa de las amenazas, permitiendo una respuesta más coordinada y eficiente. Sin embargo, la automatización no es una solución completa y debe complementarse con otros enfoques, como la capacitación de empleados y la revisión de

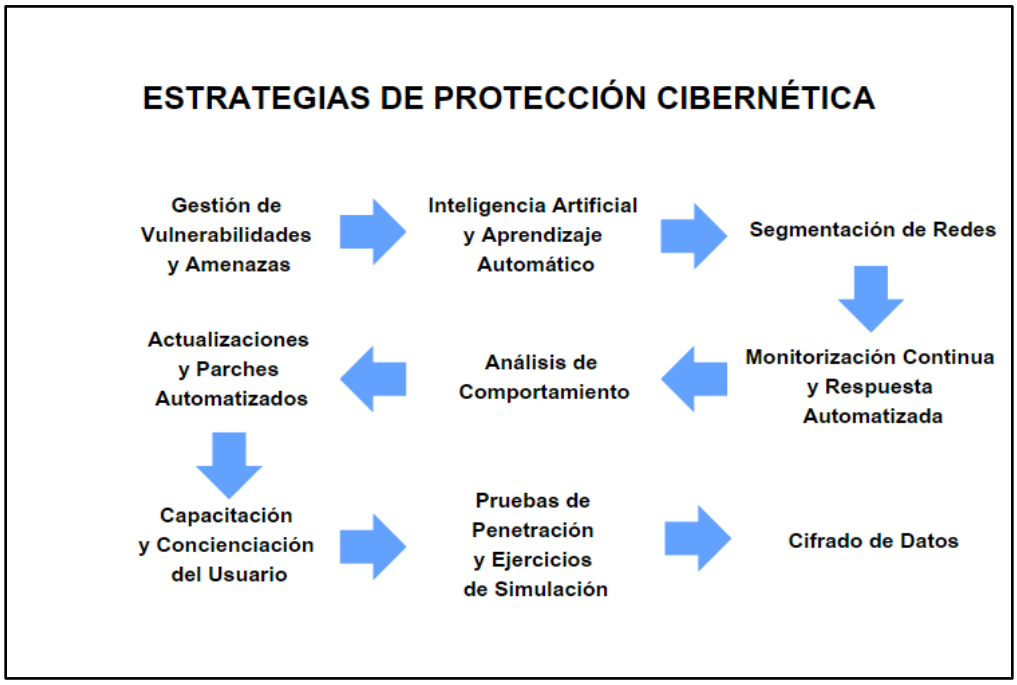
políticas y procedimientos, para abordar de manera efectiva los errores comunes en seguridad de TI y proteger adecuadamente los activos de la organización contra las amenazas cibernéticas.

Correlacionar Estrategias Avanzadas de Protección Cibernética para Anticipar y Responder Eficazmente a Amenazas Informáticas

A continuación, la figura 2 destaca varias estrategias para la protección cibernética, centradas en la prevención, detección y respuesta a amenazas. Incluye el uso de tecnologías avanzadas, la segmentación de redes, la monitorización y la capacitación de usuarios para fortalecer la seguridad digital y mitigar riesgos de manera efectiva.

Figura 2

Esquema de las estrategias de protección cibernética



Nota. Estrategias clave para la protección cibernética, centradas en la prevención, detección y respuesta a amenazas. Incluye el uso de tecnologías avanzadas, la segmentación de redes, la monitorización y la capacitación de usuarios para fortalecer la seguridad digital y mitigar riesgos de manera efectiva. *Fuente.* Autoría Propia

Correlación de Vulnerabilidades y Estrategias para la Protección Cibernética

La correlación de vulnerabilidades permite identificar, analizar y relacionar diversas debilidades en los sistemas, permitiendo priorizar estrategias de ciberseguridad. Al conectar múltiples amenazas con enfoques como la inteligencia artificial, segmentación de redes y gestión automatizada de actualizaciones, se fortalece la protección integral contra ataques emergentes, mejorando la resiliencia y eficiencia de la infraestructura digital. A continuación, la tabla 1 presenta algunas vulnerabilidades a tener en cuenta:

Tabla 1

Correlación de vulnerabilidades y estrategias para la protección cibernética

Vulnerabilidades y Amenazas	Estrategia Relacionada
Incapacidad para detectar amenazas emergentes.	Inteligencia Artificial y Aprendizaje Automático: Implementar Inteligencia Artificial para la respuesta autónoma y rápida a incidentes, acelerando la detección y contención de amenazas.
Configuraciones incorrectas en dispositivos IoT.	Segmentación de Redes: Promover el uso de software legal y evitar fuentes no confiables para asegurar que los dispositivos reciban parches de seguridad necesarios y reduzcan el riesgo de malware.
Ataques de denegación de servicio (DDoS)-	
Incapacidad para detectar amenazas emergentes.	Monitorización Continua y Respuesta Automatizada: Implementar sistemas de monitorización que utilicen aprendizaje automático

Tiempo de respuesta lento ante incidentes de seguridad	para detectar patrones de amenazas en tiempo real y mejorar la respuesta ante incidentes. Automatizar las respuestas a incidentes para reaccionar más rápido a amenazas detectadas y evitar que se propaguen dentro de la red.
Amenazas internas mal gestionadas Conductas inseguras por parte de las personas	Análisis de Comportamiento: Evaluar cómo los factores humanos afectan la ciberseguridad y establecer medidas para prevenir amenazas internas mediante la comprensión de comportamientos y actitudes. Identificar patrones de comportamiento riesgoso entre empleados mediante el análisis de datos y fomentar una cultura de seguridad activa en toda la organización.
Falta de actualizaciones de software Uso de software pirata y desactualizado	Actualizaciones y Parches Automatizados: Implementar actualizaciones automáticas y educación sobre la importancia de mantener software y dispositivos actualizados para cerrar brechas de seguridad.
Conocimiento limitado sobre ciberseguridad Errores humanos que comprometen la seguridad	Capacitación y Concienciación del Usuario: Realizar programas de concienciación y capacitación para educar a los empleados sobre las mejores prácticas de ciberseguridad y el impacto de sus acciones. Mejorar la cultura de seguridad mediante la formación y concienciación, para que los empleados sean más conscientes de sus responsabilidades en la protección de los sistemas.

Fugas de datos por falta de pruebas	Pruebas de Penetración y Ejercicios de Simulación: Realizar simulaciones de ataque y pruebas de penetración para identificar vulnerabilidades en los sistemas antes de que puedan ser explotadas por personas malintencionadas.
Vulnerabilidades no descubiertas en sistemas críticos	Utilizar equipos de "Equipo Rojo" y "Equipo Azul" para simular ataques y evaluar la capacidad de respuesta y la robustez de los sistemas contra ataques simulados.
Acceso no autorizado a datos sensibles	Cifrado de Datos: Utilizar algoritmos de cifrado para proteger datos en tránsito y almacenamiento, asegurando que solo los usuarios autorizados puedan acceder a la información sensible.
Intercepción de datos en tránsito	Proteger la comunicación de datos sensibles mediante cifrado robusto, garantizando que los datos no puedan ser interceptados y leídos por terceros no autorizados.

Nota. Esta tabla muestra la relación entre las vulnerabilidades y amenazas respecto a estrategias de protección de estas. *Fuente.* Autoría propia

Gestión de Vulnerabilidades y Amenazas

El autor Ortega (2024) indica que la gestión de riesgos implica identificar, evaluar y responder a posibles peligros, comprendiendo tanto la probabilidad de ocurrencia como su impacto. Con esta comprensión, las organizaciones pueden definir su tolerancia al riesgo y priorizar sus actividades de ciberseguridad. Dependiendo del contexto empresarial, las organizaciones pueden manejar el riesgo mediante mitigación, transferencia, prevención o aceptación, adaptando su enfoque según el impacto en sus servicios esenciales.

En otra arista Díaz (2019), discurre que; en los últimos diez años, la inteligencia artificial (IA) ha avanzado de manera impresionante, integrándose en una amplia gama de áreas científicas

e industriales, desde la medicina y la logística hasta la agricultura y las telecomunicaciones. Su versatilidad es evidente en campos como la robótica y el Internet de las Cosas (IoT). Además, la seguridad es un tema importante, ya que los dispositivos IoT son susceptibles a ciberataques, como los de denegación de servicio distribuido (DDoS). Estos ataques se aprovechan de las debilidades en los protocolos TCP/IP y de dispositivos mal configurados, poniendo en riesgo tanto infraestructuras críticas como la privacidad y seguridad de los datos. Con el crecimiento acelerado del IoT, la necesidad de soluciones de seguridad sólidas y efectivas se vuelve cada vez más indispensable.

Adicionalmente, Ortega (2024) nos habla que también es muy importante proteger los activos contra amenazas y vulnerabilidades ya que es fundamental para la seguridad de las organizaciones. Las partes interesadas, responsables de estos activos, deben tener en cuenta las amenazas al evaluar los riesgos asociados.

La gestión de riesgos es un proceso continuo que abarca la identificación, evaluación y respuesta a las amenazas y vulnerabilidades. Las organizaciones necesitan comprender la probabilidad de que ocurran ciertos eventos y su posible impacto. Esta información les permite determinar su nivel aceptable de riesgo, o tolerancia al riesgo. Con este entendimiento, pueden priorizar las actividades de ciberseguridad y tomar decisiones informadas sobre los gastos necesarios. Los programas de gestión de riesgos facilitan la cuantificación y comunicación de los ajustes requeridos en los programas de ciberseguridad.

Para manejar las amenazas y vulnerabilidades, las organizaciones pueden adoptar diversas estrategias, como mitigar, transferir, prevenir o aceptar el riesgo, según el impacto potencial en los servicios críticos. El entorno empresarial influye significativamente en las decisiones sobre el riesgo; por ejemplo, una pequeña empresa puede ser más tolerante al riesgo

en comparación con una empresa grande. El análisis de riesgos informáticos consiste en identificar activos y sus vulnerabilidades, evaluar las amenazas y su probabilidad de ocurrencia, y determinar los controles adecuados para gestionar el riesgo mediante la aceptación, reducción, transferencia o evitación de este.

Inteligencia Artificial y Aprendizaje Automático

El aprendizaje automático es un método esencial para la inteligencia artificial, ya que su principal función es desarrollar un modelo capaz de aprender de datos históricos y experiencias previas para realizar tareas específicas. A diferencia de los sistemas expertos tradicionales, su ventaja radica en su habilidad para aprender de manera autónoma. Según (Wang & Zhang, 2023), si el modelo no logra entender completamente la información de los datos históricos, se enfrenta a un problema de desajuste. Por el contrario, si el modelo aprende demasiado de los datos, incluyendo el ruido o información irrelevante, se enfrenta a un problema de sobreajuste.

En el contexto del aprendizaje automático, "ruido" se refiere a datos irrelevantes o errores presentes en el conjunto de datos que no representan patrones verdaderos o útiles para el modelo. Estos datos pueden surgir por diversas razones, como errores de medición, variabilidad aleatoria, o incluso datos incorrectos. El ruido puede llevar al modelo a aprender información que no es realmente significativa para las tareas objetivo, lo que puede causar problemas de sobreajuste. En el sobreajuste, el modelo se ajusta demasiado a los datos de entrenamiento, incluyendo estos elementos irrelevantes, y como resultado, su desempeño en nuevos datos o datos de prueba se ve afectado negativamente.

Según Granados (2022), la inteligencia artificial se define como un conjunto de tecnologías diseñadas para imitar el comportamiento humano. Estas tecnologías permiten el desarrollo de sistemas artificiales capaces de realizar tareas o actividades profesionales de

manera similar a como lo harían las personas, es decir, máquinas que piensan y operan como seres humanos.

El aprendizaje automático es una técnica clave dentro de la inteligencia artificial (IA) que permite a las máquinas aprender de los datos y mejorar sin intervención humana directa. Al identificar patrones y realizar predicciones, el aprendizaje automático impulsa la capacidad de la IA para evolucionar y adaptarse a nuevas situaciones. Esta relación es fundamental, ya que el aprendizaje automático permite que los sistemas de IA no solo ejecuten tareas predefinidas, sino que también desarrollen comportamientos cada vez más complejos y autónomos, acercándose a la inteligencia humana.

Segmentación de Redes

En concordancia con Mario et al. (2023) la segmentación de redes es una técnica esencial en ciberseguridad que consiste en dividir una red grande en subredes más pequeñas, cada una con controles y reglas de acceso propios. Esto permite restringir la propagación de amenazas en caso de un ataque y aplicar medidas de seguridad específicas según las necesidades de cada segmento. Los principales beneficios son la mejora de la seguridad al contener las amenazas, el control detallado de accesos y la optimización del tráfico en la red. Además, ayuda a cumplir con normativas que exigen proteger datos sensibles y separar diferentes entornos de TI.

Para implementar la segmentación de redes, se deben seguir varias etapas: primero, evaluar los riesgos y los requisitos; luego, diseñar la red segmentada; después, configurar y probar los segmentos; y finalmente, monitorear y mantener la red continuamente. Entre las tecnologías utilizadas están las VLANs, las subredes y la microsegmentación mediante redes definidas por software (SDN). Es fundamental mantener una documentación clara, aplicar el principio de mínimos privilegios, realizar auditorías de seguridad regularmente y capacitar al

personal en estas prácticas. Si se lleva a cabo correctamente, la segmentación de redes mejora notablemente la seguridad y eficiencia de la infraestructura de TI.

Monitorización Continua y Respuesta Automatizada

Para mejorar las respuestas a amenazas de forma automatizada Vallejo (2023) expone que, el aprendizaje automático (Machine Learning) es una rama de la inteligencia artificial (IA) que permite que los sistemas mejoren y optimicen procesos de forma independiente, sin necesidad de recibir instrucciones específicas.

Este enfoque es particularmente efectivo en la ciberseguridad. Se utiliza para detectar y prevenir intrusiones, identificar patrones en grandes volúmenes de datos y mejorar la respuesta a amenazas. Además, el aprendizaje automático es importante para crear sistemas robustos que pueden adaptarse y mejorar continuamente. Esto ofrece una herramienta poderosa para mejorar la toma de decisiones y la seguridad en diversas áreas, desde la protección de datos personales hasta el análisis de amenazas.

Análisis de Comportamiento

Baltuttis et al. (2024) indican que el análisis del comportamiento en ciberseguridad se centra en cómo los factores humanos, como la personalidad, las actitudes y las motivaciones, afectan la seguridad informática en las organizaciones. Este enfoque no solo considera las características individuales, sino también cómo los empleados interactúan con la tecnología y entre ellos. La investigación destaca la importancia de entender las tendencias de comportamiento para predecir y prevenir posibles amenazas internas. Además, se examinan los impactos de la formación en seguridad, las políticas organizacionales y el liderazgo en la creación de una cultura de seguridad robusta. Al comprender y modificar estos factores humanos, las organizaciones pueden desarrollar estrategias más efectivas para proteger sus activos digitales y mejorar la resiliencia frente a ciberataques. También se enfatiza el uso de

encuestas y análisis de datos para evaluar continuamente la efectividad de las medidas de seguridad implementadas y adaptarlas según sea necesario.

Actualizaciones y Parches Automatizados

El autor Herrero (2019) destaca la vital importancia de mantener actualizados nuestros dispositivos para garantizar la ciberseguridad. Aunque en el ámbito empresarial este concepto es bien conocido, su implementación en hogares no es tan común. Según el autor, muchos dispositivos, como los routers, suelen tener firmware desactualizado con vulnerabilidades serias. Además, usar software pirata impide recibir parches de seguridad del fabricante, ya que estas versiones suelen ser obsoletas. Descargar software de fuentes no oficiales también incrementa el riesgo de malware, afectando tanto a las versiones pirateadas como a los programas que parecen originales, pero se obtienen de sitios no confiables. El autor menciona que muchos usuarios desconocen los peligros de usar software vulnerable, lo que provoca desinterés o rechazo hacia las actualizaciones automáticas.

Para solucionar estos problemas, el autor sugiere varias medidas: primero, instalar software legal de fuentes oficiales; segundo, habilitar y aceptar las actualizaciones automáticas en todos los dispositivos, como Windows, iOS y Android. También recomienda revisar regularmente las actualizaciones de seguridad para dispositivos que no se actualizan automáticamente, como televisores y routers, consultando las páginas de soporte de los fabricantes. Finalmente, el autor resalta la necesidad de educar a los usuarios sobre los riesgos de usar software desactualizado y la importancia de mantenerlo al día, promoviendo así una cultura de ciberseguridad más sólida y consciente.

Capacitación y Concienciación del Usuario

Según los autores Nieles et al. (2017), la concienciación es clave para motivar a las personas a preocuparse por la seguridad y recordarles las prácticas importantes. Explicar las

consecuencias de una falla de seguridad para la organización, su misión, sus clientes y empleados ayuda a que la gente se tome este tema en serio. Los programas de concienciación sobre seguridad logran dos cosas principales: primero, establecen una base para la capacitación cambiando las actitudes dentro de la organización para que se valore la importancia de la seguridad y se comprendan las consecuencias negativas de no mantenerla; segundo, recuerdan a los usuarios los procedimientos que deben seguir.

La concienciación puede adaptarse a diferentes públicos. Por ejemplo, para los funcionarios administrativos, es importante destacar su papel en la configuración de las actitudes organizacionales hacia la seguridad. Para otros grupos, como los programadores de sistemas o los analistas de información, la concienciación debe enfocarse en la importancia de la seguridad en relación con su trabajo específico. En el entorno actual de sistemas, casi todos en una organización tienen acceso a los recursos del sistema y, por lo tanto, tienen el potencial de causar daños.

Pruebas de Penetración y Ejercicios de Simulación

De acuerdo con Almeida et al. (s.f.) resaltan la importancia de los ejercicios de simulación en ciberseguridad para combatir los ataques criminales y diversas amenazas en el ciberespacio. La protección contra adversarios estatales, criminales y terroristas, así como la prevención de vulnerabilidades en los sistemas, son aspectos clave de la ciberseguridad para garantizar la integridad, disponibilidad y confidencialidad de la información. Frente a la constante evolución de las amenazas cibernéticas, se han desarrollado estrategias como los famosos ejercicios entre el llamado “Equipo Rojo” contra “Equipo Azul” en ciberseguridad, los cuales simulan ataques y pruebas de defensa para fortalecer la preparación y la seguridad en línea.

Estos ejercicios involucran a los equipos Rojo y Azul: El Equipo Rojo actúa como atacante y el Equipo Azul como defensor. Emplean diversas técnicas y herramientas, como el "Hackeo Ético" y la ingeniería social, para identificar vulnerabilidades y proteger los sistemas de ataques simulados. La colaboración entre ambos equipos, junto con la capacitación de los usuarios y el cumplimiento de las normativas de seguridad informática, son esenciales para evitar la filtración de datos sensibles y reducir los riesgos en el ciberespacio.

Cifrado de Datos

De acuerdo con Gómez (2013) se resalta el proceso del cifrado de datos, que convierte información legible en algo ilegible, llamado criptograma, mediante un algoritmo. Esta información ilegible se puede enviar con menor riesgo de ser entendida por personas no autorizadas. Para volver a entenderla, el destinatario necesita descifrarla usando la clave del cifrado.

Según el autor Burgos (2021), la tecnología que está transformando la seguridad y el cifrado de datos es la Cadena de Bloques o BlockChain (BC). Esta tecnología ofrece una encriptación de datos más eficaz en comparación con otros algoritmos de seguridad. BlockChain se basa en una base de datos descentralizada, distribuida en múltiples computadores, conocidos como nodos, que están interconectados mediante un algoritmo matemático. La red de BlockChain está protegida criptográficamente y organizada en bloques, lo que permite que los datos sean transmitidos y validados por cada nodo, garantizando así la seguridad de la información.

Efectividad y Aplicabilidad de las Técnicas y Estrategias de Ciberseguridad

Las herramientas de ciberseguridad, como los firewalls, la autenticación multifactor y el cifrado, son bastante efectivas en distintos entornos, especialmente en organizaciones grandes o en el sector público, donde proteger la información es muy importante. Su efectividad depende

de varios factores, como la capacitación constante de los usuarios, la rapidez con la que emergen nuevas amenazas y la magnitud de la infraestructura a proteger. En entornos más pequeños o personales, aunque las soluciones básicas como contraseñas fuertes y antivirus son necesarias, muchas veces la falta de conciencia sobre la seguridad digital disminuye su efectividad. Por lo tanto, las estrategias deben adaptarse y actualizarse continuamente para hacer frente a las diversas amenazas.

A pesar de lo útiles que son estas herramientas, surgen preocupaciones éticas cuando se habla de su implementación. El uso de datos personales y la vigilancia para prevenir ciberataques pueden poner en riesgo la privacidad de las personas. Es fundamental encontrar un equilibrio entre proteger los sistemas y respetar los derechos de las personas. Las organizaciones deben ser transparentes y responsables con el uso de estos datos para asegurarse de que no invadan la privacidad de los usuarios sin su consentimiento.

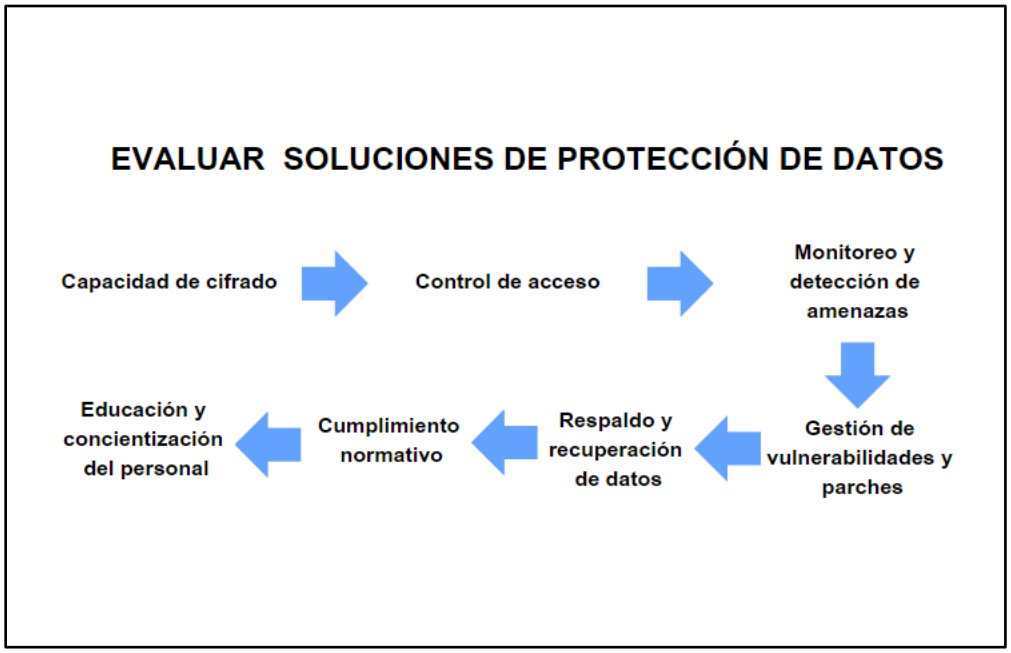
Desde el punto de vista legal, es importante que las estrategias de ciberseguridad se ajusten a las leyes de protección de datos, para evitar posibles problemas legales. Además, las organizaciones deben ser claras con los usuarios sobre cómo manejan sus datos personales, asegurándose de que cumplen con los derechos de privacidad de las personas y mantienen la confianza del público en las herramientas de seguridad que utilizan.

Evaluar la Eficacia de Soluciones de Protección de Datos en Entornos Digitales para Mitigar Riesgos de Pérdida o Robo de Información Confidencial.

La figura 3 muestra los elementos clave en la evaluación de soluciones para proteger los datos, destacando la importancia del cifrado, el control de acceso, la detección de amenazas y la gestión de vulnerabilidades. Además, resalta la educación continua del personal y la recuperación de datos para garantizar la seguridad y el cumplimiento normativo en entornos digitales.

Figura 3

Esquema para evaluar soluciones de protección de datos



Nota. Elementos clave en la evaluación de soluciones para proteger los datos, destacando la importancia del cifrado, el control de acceso, la detección de amenazas y la gestión de vulnerabilidades. *Fuente.* Autoría Propia

Capacidad de Cifrado

En concordancia con Gómez (2013) se destaca la relevancia del cifrado de datos en la protección de la información transmitida a través de redes, especialmente en situaciones donde las transacciones bancarias, compras en línea y comunicaciones por correo electrónico pueden ser interceptadas por terceros. El cifrado, también llamado encriptación, se presenta como un elemento esencial para garantizar la seguridad de las comunicaciones y salvaguardar la privacidad de las entidades o individuos que se comunican.

El proceso de cifrado de datos consiste en transformar un mensaje claro en un texto cifrado utilizando un algoritmo y una llave, lo que evita que otros puedan entender el contenido del mensaje. Luego, el destinatario del mensaje utiliza el mismo algoritmo y llave para revertir el texto cifrado al mensaje original. Esta técnica resulta importante para mantener la confidencialidad e integridad de la información en entornos donde la seguridad de las redes es de suma importancia.

Control de Acceso

El autor Romaniz (2008) expone que los controles de acceso representan elementos fundamentales en la seguridad de las aplicaciones, interactuando con los sistemas de autenticación y gestión de sesiones. Su propósito primordial consiste en evaluar si se autoriza la ejecución de una acción requerida sobre determinados recursos. La falta de robustez en estos controles posibilita que actores malintencionados comprometan la totalidad de la aplicación, accediendo a funciones administrativas y a datos sensibles de otros usuarios. A pesar de la existencia de sólidos mecanismos de autenticación y gestión de sesiones, diversas aplicaciones adolecen de una implementación inadecuada de controles de acceso, lo que las expone a vulnerabilidades. Por otro lado, los autores Vela et al. (2007) hablan sobre las definiciones de

Modelos de Control de Acceso para tener en cuenta al momento de evaluar la protección de los datos

DAC – Control de Acceso Discrecional

El Control de Acceso Discrecional (DAC) es un modelo de seguridad en el que el propietario de un recurso decide quién puede acceder a él y qué permisos tienen. Este sistema controla tanto a los usuarios, grupos o procesos (sujetos) como a los recursos (objetos) mediante reglas de autorización que el propietario puede cambiar y asignar. DAC ofrece flexibilidad, permitiendo a los usuarios autorizados copiar datos y conceder permisos a otros. Sin embargo, este modelo tiene riesgos de seguridad, ya que la información puede compartirse accidentalmente con usuarios no autorizados. Aunque es flexible, DAC no asegura completamente principios de seguridad como el "privilegio mínimo" o la "separación de deberes", siendo más apropiado en entornos donde es más importante compartir información que protegerla estrictamente.

MAC – Control de Acceso Obligatorio

El Control de Acceso Obligatorio (MAC) es un modelo de seguridad que organiza y etiqueta usuarios y recursos según niveles de seguridad predeterminados. Este sistema multinivel establece reglas estrictas, como "no leer hacia arriba" y "no escribir hacia abajo", para evitar que la información pase de niveles altos de seguridad a niveles más bajos, protegiendo así la confidencialidad e integridad de los datos. A diferencia del DAC, donde el dueño del recurso decide las reglas de acceso, en MAC, es el administrador del sistema quien establece y controla estas reglas. Aunque MAC ofrece una protección de datos más sólida, puede ser menos flexible y complicado de aplicar en ambientes colaborativos.

BAC – Control de Acceso Basado en Roles

El Control de Acceso Basado en Roles (RBAC) es un modelo de seguridad que otorga permisos a roles en lugar de asignarlos directamente a usuarios, lo que facilita la gestión del acceso en organizaciones grandes y complejas. Los roles representan diferentes funciones o responsabilidades dentro de la organización y están vinculados a conjuntos específicos de permisos.

Los usuarios adquieren los permisos necesarios según los roles que desempeñan. RBAC permite estructurar jerarquías de roles y establecer restricciones tanto estáticas como dinámicas para evitar conflictos de interés y gestionar el acceso en distintos contextos. Aunque este modelo es útil para asegurar la seguridad en el ámbito empresarial, puede ser menos flexible en entornos cambiantes y colaborativos, y puede resultar complicado de administrar cuando se necesita un control detallado sobre usuarios individuales y recursos específicos.

TBAC – Control de Acceso Basado en Tareas

El Control de Acceso Basado en Tareas (TBAC) es un modelo de seguridad que se enfoca en gestionar el acceso en entornos donde se utilizan workflows, añadiendo información contextual sobre actividades o tareas al control de acceso tradicional. En TBAC, el acceso se controla mediante "etapas de autorización", que determinan qué permisos están disponibles según el progreso de las tareas. Este sistema dinámico permite ajustar los permisos en tiempo real, ofreciendo un control detallado y flexible basado en el estado actual de las tareas y los workflows. No obstante, TBAC puede presentar desafíos en entornos colaborativos complejos, ya que se centra en la información contextual de las tareas y puede no contar con mecanismos avanzados para la gestión y delegación de privilegios.

Monitoreo y Detección de Amenazas

Según Aimaretto y Dujovne (2023), el aprendizaje automático (ML) y la detección de amenazas internas son esenciales para identificar acciones maliciosas por parte del personal autorizado en una organización. Las amenazas internas son particularmente difíciles de detectar debido a su escasa huella digital, y este desafío se agrava con la expansión del Internet de las Cosas (IoT), que aumenta la superficie de ataque.

Para abordar estas amenazas, se han creado soluciones de detección basadas en ML. Estas soluciones buscan mejorar la identificación de amenazas internas al enfocarse en la confiabilidad y el rendimiento del modelo. El concepto de "Trustworthy Learning" resalta la importancia de procedimientos éticos y confiables en la recopilación y análisis de datos, lo cual facilita la aceptación de estas soluciones. El estudio propone un método que asegura la privacidad y explicación de los modelos de ML y fomenta la colaboración entre diferentes propietarios de datos para mejorar el rendimiento del modelo. Los resultados muestran que esta solución es más efectiva que los modelos entrenados con datos individuales, subrayando la eficacia de la colaboración y el respeto a los principios éticos en el aprendizaje automático.

Gestión de Vulnerabilidades y Parches

Para Syed (2020) la importancia de la gestión de vulnerabilidades en ciberseguridad, describiéndola como el proceso de detectar, evaluar y solucionar vulnerabilidades en sistemas. Este proceso implica recopilar información de diversas fuentes, como el Centro de Coordinación del Equipo de Respuesta a Emergencias Informáticas (CERT/CC), redes sociales, blogs y wikis. Para organizar y analizar esta información, se emplean ontologías, que son representaciones estructuradas y formales del conocimiento en un área específica, como la ciberseguridad. Estas ontologías modelan las relaciones entre conceptos y datos, facilitando la organización, comunicación y análisis de información sobre vulnerabilidades. Al integrar estos datos, las

ontologías permiten evaluar la gravedad de las vulnerabilidades y emitir alertas, contribuyendo así a proteger a los usuarios y prevenir ataques cibernéticos.

Respaldo y Recuperación de Datos

Los autores Wilson et al. (2017) destacan la importancia de respaldar los datos en una empresa debido al aumento significativo de la información manejada. Señala que los backups tienen tres propósitos principales: recuperación de desastres, restauraciones operacionales y almacenamiento a largo plazo. La recuperación de desastres implica recuperar la información después de eventos catastróficos como incendios o inundaciones, generalmente en un lugar alternativo con infraestructura similar. Por otro lado, el respaldo operacional consiste en copias de seguridad de la información en momentos específicos para recuperar los datos si hay corrupción durante la operación normal de una aplicación o servidor, que es la causa más común de pérdida de datos en una organización.

Entonces lo que el autor nos indica es que el respaldo de datos y la recuperación de datos son importantes porque la integridad de la información en caso de desastres naturales, fallos del sistema, ataques cibernéticos u otros eventos que puedan causar la pérdida o corrupción de datos. Al realizar copias de seguridad periódicas, se asegura que la información crítica esté protegida y disponible para su restauración en caso de necesidad. Esto permite minimizar el tiempo de inactividad, mantener la productividad y preservar la confianza de las personas al garantizar que sus datos estén seguros y accesibles en todo momento.

Cumplimiento Normativo

El cumplimiento normativo en ciberseguridad se refiere al conjunto de medidas y prácticas que una organización debe seguir para cumplir con las leyes, regulaciones y estándares relacionados con la protección de la información y la seguridad de los datos. El objetivo principal del cumplimiento normativo es garantizar la confidencialidad, integridad y

disponibilidad de la información, así como también mitigar los riesgos relacionados con la seguridad cibernética.

Según lo expuesto por el autor Pulido (2022), la ciberseguridad busca proteger tanto los datos como la integridad de las personas y las empresas. Para lograr este objetivo, se apoya en un amplio marco normativo, importante para el éxito empresarial. Un ejemplo destacado es la normatividad de la Organización Internacional de Normalización (ISO), específicamente la norma ISO/IEC 27001:2013, que ha sido adoptada en Colombia a través de las Normas Técnicas Colombianas (NTC). Esta norma proporciona numerosos beneficios, entre ellos la reducción de riesgos de seguridad digital, la protección de la confidencialidad de la información, la disminución de amenazas en el ámbito de las tecnologías de la información (TI), la mejora de la competitividad en el mercado, el incremento de la confianza de socios y clientes, el cumplimiento de requisitos internacionales, la detección sistemática de vulnerabilidades, la reducción de costos y el control efectivo de riesgos en TI. ISO/IEC 27001:2013: Esta norma internacional de gestión de seguridad de la información proporciona un marco para proteger los activos de información. Sus beneficios incluyen la reducción de vulnerabilidades, garantía de confidencialidad, minimización de riesgos, obtención de una ventaja competitiva y aumento de la confianza de socios y clientes.

CONPES 3995: En Colombia, el Consejo Nacional de Política Económica y Social emitió una política para fortalecer la seguridad digital y aumentar la confianza en el manejo de la información digital. Las empresas deben cumplir con estas normativas para evitar sanciones que podrían afectar su éxito. (Ramírez et al., 2022).

Educación y Concientización del Personal: Técnica de Concientización en Ciberseguridad

Canfranc (2019) compara la ciberseguridad con la salud, destacando que debe ser monitoreada y cuidada constantemente, no solo con intervenciones ocasionales. Se considera un proceso continuo, que implica varias fases clave.

En primer lugar, la prevención es importante y requiere una formación continua para estar al tanto de las nuevas amenazas y cómo evitarlas. Esto incluye controlar quién accede a los recursos, asignar permisos según los roles, implementar medidas técnicas y legales para prevenir fugas de información, y establecer políticas de seguridad de red que deben ser regularmente auditadas.

La detección es otra fase esencial, que puede ocurrir en tiempo real o después de un ataque. Esto se logra mediante la monitorización constante de los sistemas para identificar y limitar rápidamente cualquier intento de descubrir las vulnerabilidades en la infraestructura informática.

Finalmente, la respuesta entra en juego cuando un ataque ha tenido éxito. Esta etapa incluye la recuperación de los sistemas afectados, restaurándolos a su estado previo, y la implementación de nuevas medidas de seguridad para prevenir futuros incidentes. Además, se enfatiza la inteligencia, que consiste en compartir información sobre los ataques con otras organizaciones para mejorar la respuesta colectiva al cibercrimen.

Barroso (2021), la implementación de ataques de phishing simulados es una estrategia clave para fortalecer la ciberseguridad en las organizaciones. Estos simulacros permiten entrenar a los empleados en la detección y reporte de correos electrónicos sospechosos, ayudándolos a reconocer intentos de phishing en un entorno seguro y controlado. Además, esta práctica ofrece retroalimentación inmediata, lo que facilita el aprendizaje continuo. Para llevarla a cabo, se recomienda utilizar plataformas que envíen correos electrónicos falsos y monitoreen las

respuestas de los empleados, evaluando así su nivel de preparación y mejorando sus habilidades preventivas.

El Phishing

Es importante destacar que, el phishing es un tipo de fraude donde se envían correos electrónicos falsos que simulan ser de servicios legítimos para engañar a los destinatarios y obtener información privada, como datos de tarjetas de crédito o credenciales de acceso. Este engaño, también llamado suplantación de identidad de una marca o "brand spoofing," se distribuye frecuentemente a través de correos no solicitados (spam) y es ilegal en muchos países. El phishing se basa en técnicas de ingeniería social para explotar la confianza que los usuarios tienen en grandes empresas, creando sitios web que parecen auténticos y familiares para convencer a las víctimas de que revelen su información personal. (según el autor).

En concordancia con Atlam y Oluwatimilehin (2023) el phishing es una forma de estafa en la que los atacantes envían correos electrónicos falsos que parecen ser de fuentes confiables para engañar a los usuarios y robar información sensible o instalar malware. Una variante más personalizada es el spear phishing, que se dirige a individuos específicos con mensajes adaptados a sus características. Además, el compromiso de correo electrónico empresarial (BEC) es una forma avanzada de spear phishing. En BEC, los atacantes acceden a cuentas de correo legítimas de proveedores para solicitar información confidencial o dinero. Este método ha evolucionado desde los fraudes simples por correo electrónico hasta técnicas sofisticadas en la actualidad, según el autor.

El autor Ortega (2024) menciona que, para protegernos de las amenazas cibernéticas, es importante implementar medidas de seguridad que no solo busquen prevenir infecciones, sino también minimizar los daños en caso de ser víctimas de un ataque. Estas acciones son fundamentales para reducir el impacto potencial de cualquier incidente de seguridad.

Estudio de Caso

Estrategias de Protección Cibernética en Colombia

En este capítulo, se presentará un análisis detallado de los incidentes de ciberseguridad reportados en Colombia entre noviembre y diciembre de 2022, con el fin de proporcionar una comprensión amplia de las amenazas cibernéticas enfrentadas por diversas entidades del país y las estrategias implementadas para su mitigación. El estudio se centra en un caso general que describe el panorama de los ataques, seguido de dos casos específicos que involucran a Empresas Públicas de Medellín (EPM) y Colsanitas (Keralty), entidades que sufrieron ataques significativos durante este período.

En la sección del Caso General, se describen los tipos más comunes de ciberataques reportados y las técnicas empleadas por los atacantes, destacando la suplantación de sitios web y dominios de correo electrónico como las estrategias más frecuentes. Posteriormente, se abordarán los Casos Específicos, donde se detallarán las respuestas y soluciones implementadas en incidentes críticos que afectaron a EPM y Colsanitas. En estos casos, se profundizará en las medidas tomadas por las instituciones afectadas en colaboración con el Equipo de Respuesta a Emergencias Cibernéticas de Colombia, en adelante – COLCERT – por sus siglas en inglés y el grupo especializado en ciberseguridad del Ministerio TIC, para mitigar los daños y recuperar sus operaciones.

Este enfoque permitirá comprender tanto el contexto general de los ciberataques reportados en Colombia durante este período como las particularidades de cada caso específico, mostrando las respuestas implementadas, las vulnerabilidades identificadas y la efectividad de las estrategias de protección utilizadas. Además, se evaluarán cuantitativamente los incidentes y se analizará la eficacia de las estrategias de protección de datos implementadas, identificando áreas de mejora para futuras situaciones.

En virtud de lo anterior, en el presente estudio de caso, se analizarán los incidentes de ciberseguridad reportados en Colombia entre noviembre y diciembre de 2022, en los que el Ministerio TIC, a través COLCERT, documentó 6 reportes de ciberataques. Las estrategias implementadas se centrarán en el análisis de técnicas de ciberseguridad recientes, la correlación de estrategias de protección cibernética, y la evaluación de soluciones de protección de datos (MinTIC, 2022).

Descripción del Caso

Entre el 1 de noviembre y el 16 de diciembre de 2022, se recibieron 36 reportes de incidentes de ciberseguridad en Colombia, siendo la suplantación de sitios web y de dominios de correo las técnicas de ataque más frecuentes. A continuación, se presenta una caracterización de los tipos de ataques reportados en el estudio de caso (MinTIC, 2022).

Tabla 2

Caracterización de los ataques cibernéticos

Tipo de Ataque	Cantidad de Reportes	Posibles Técnicas o Estrategias Implementadas
Suplantación de sitios web	19	Evaluación de soluciones de protección de datos como certificados SSL o autenticación multifactor (MFA).
Suplantación de dominios de correo	8	Uso de políticas de seguridad de correo para mitigar suplantación.

Nota. Esta tabla muestra el tipo de ataque y el número de reportes generados en el estudio de caso. *Fuente.* MinTIC,2022.

Tabla 3

Resumen de los ataques cibernéticos

Entidades Afectadas	Cantidad de Reportes
Entidades públicas de orden nacional	18
Entidades públicas de orden territorial	5
Empresas y organizaciones privadas	18

Nota. Esta tabla muestra las entidades afectadas por ataque cibernéticos y el número de reportes generados en el estudio de caso. *Fuente.* MinTIC,2022.

Análisis de Casos Específicos: EPM

El 13 de diciembre de 2022, Empresas Públicas de Medellín (EPM) sufrió un incidente de ciberseguridad. COLCERT contactó inmediatamente con los equipos de TI y ciberseguridad de EPM, activando protocolos de respuesta.

Tabla 4

Caracterización caso EPM

Incidente	Fecha	Afectación	Posibles Soluciones Implementadas	Respuesta
EPM	13 de diciembre	Sistemas internos	Evaluación de soluciones de protección de datos y	Contacto inmediato con COLCERT, activación de

	monitoreo continuo.	protocolos de recuperación y análisis posterior.
	Estrategias de protección cibernética mediante respaldo de datos y análisis de vulnerabilidades post-incidente.	Incidente reportado a la Superintendencia de Industria y Comercio y la Policía Nacional.

Nota. En esta tabla se observan los activos afectados, las soluciones implementadas y como se atendió la necesidad. *Fuente.* MinTIC,2022.

Análisis de Casos Específicos: Colsanitas (Keralty)

Este incidente afectó a Colsanitas y al grupo Keralty. Para este caso COLCERT, coordinó con el Ministerio de Salud y la Superintendencia de Salud para apoyar la contención del ataque y la recuperación de la operación.

Tabla 5

Caracterización caso Colsanitas (Keralty)

Incidente	Fecha	Afectación	Posibles Soluciones Implementadas	Respuesta
Colsanitas	Diciembre 2022	Sistemas médicos	Estrategias de protección cibernética centradas en la eliminación de la amenaza y recuperación rápida de los sistemas críticos.	COLCERT apoyó el proceso de contención, eliminación de la amenaza y recuperación de la operación. Coordinación con Ministerio de Salud y la Superintendencia de Salud.

Nota. En esta tabla se observan los activos afectados, las soluciones implementadas y como se atendió la necesidad. *Fuente.* MinTIC,2022.

Identificación de Vulnerabilidades

En los casos de EPM y Colsanitas, las vulnerabilidades identificadas estaban relacionadas con compromisos en los sistemas de TI. Aunque no se especificaron públicamente, se asume que

las áreas afectadas incluían la infraestructura crítica, lo que indica la necesidad de análisis preventivos y evaluaciones regulares de vulnerabilidades.

Tabla 6

Caracterización caso EPM

Entidad	Medidas Preventivas y Estrategias de Protección Implementadas
EPM	Estrategias de protección cibernética mediante la activación de protocolos de recuperación post-incidente y análisis de riesgos futuros.
Colsanitas	Evaluación de soluciones de protección de datos y monitoreo constante del tráfico para identificar anomalías.

Nota. En esta tabla se identifican las entidades impactadas en el estudio de caso, sus medidas preventivas y estrategias de protección implementadas. *Fuente.* MinTIC,2022.

Evaluación Cuantitativa

A continuación, se presenta un análisis cuantitativo de los incidentes reportados, destacando los tipos de ataques y las entidades afectadas:

Tabla 7

Análisis cuantitativo del ataque

Métrica	Cantidad
Total de incidentes reportados	36
Suplantación de sitios web	19
Suplantación de dominios de correo	8

Entidades públicas afectadas	23
Empresas privadas afectadas	18

Nota. En esta tabla se muestra el número de incidentes reportados por cada métrica. *Fuente.* MinTIC,2022.

Evaluación de la Eficacia de las Estrategias

Las estrategias de respuesta rápida implementadas por COLCERT permitieron contener y recuperar los sistemas afectados. Sin embargo, la falta de medidas preventivas robustas y de una evaluación cuantitativa de los daños y recuperación sugiere la necesidad de mejoras en la identificación de vulnerabilidades y en la evaluación de la eficacia de las estrategias.

Tabla 8

Valoración de las Estrategias

Indicador de Evaluación	Resultados
Tiempo de respuesta	Inmediato
Restablecimiento de la operación	Sí
Prevención de futuros incidentes	No especificado
Evaluación de soluciones de protección de datos	No cuantificada

Nota. En esta tabla se valoran las estrategias por indicador de evaluación y sus resultados. *Fuente.* MinTIC,2022.

Resultados

En esta investigación, examinó la relevancia de distintas estrategias y enfoques para la protección de datos y la ciberseguridad. Los resultados muestran que aplicar controles y prácticas efectivas puede mejorar significativamente la seguridad de la información en el mundo digital. A continuación, se detallan los hallazgos más importantes.

El control de acceso es vital para mantener la seguridad de nuestras aplicaciones y sistemas de información. Si no se implementa correctamente, existe el riesgo de que personas no autorizadas accedan a datos sensibles, lo que puede comprometer la seguridad de la organización. Así que es importante evaluar qué modelos de control de acceso son más efectivos. Existen varias opciones a considerar:

Control de Acceso Discrecional (DAC): Este modelo permite a los propietarios decidir quién puede acceder a sus recursos y qué permisos tienen. Aunque es flexible, puede ser arriesgado, ya que los permisos pueden compartirse por accidente, lo que podría causar problemas de seguridad.

Control de Acceso Obligatorio (MAC): Este enfoque utiliza reglas establecidas por el administrador y niveles de seguridad para restringir el acceso. Ofrece una mayor protección que el DAC, pero puede ser menos adaptable en entornos donde la colaboración es importante.

Control de Acceso Basado en Roles (RBAC): Este modelo asigna permisos según los roles dentro de la organización, lo que facilita la gestión del acceso, especialmente en estructuras grandes. Sin embargo, puede volverse complicado de manejar en entornos dinámicos.

Control de Acceso Basado en Tareas (TBAC): Este enfoque se centra en el acceso según el progreso de las tareas, ofreciendo un control más detallado en entornos con flujos de trabajo específicos. Sin embargo, puede ser un desafío en situaciones colaborativas complejas.

Al analizar estos modelos, las organizaciones pueden elegir el que mejor se ajuste a sus necesidades, fortaleciendo así su seguridad y protegiendo sus recursos más valiosos.

En el ámbito de la ciberseguridad, el monitoreo y la detección de amenazas es muy importante para reconocer acciones maliciosas. En este contexto, el aprendizaje automático (ML) se ha vuelto una herramienta fundamental. Gracias a las soluciones basadas en ML, las organizaciones pueden detectar amenazas de manera más rápida y precisa, lo que también mejora la confiabilidad y el rendimiento de los sistemas. Además, para que estas herramientas realmente funcionen, es esencial que haya una colaboración constante entre los equipos de seguridad y que se respeten principios éticos en el desarrollo y uso del aprendizaje automático. Esto garantiza que las tecnologías implementadas sean efectivas. Al enfocarse en estos aspectos, las organizaciones pueden mejorar su capacidad para identificar y reaccionar ante amenazas, fortaleciendo así su seguridad en general.

En el ámbito de la ciberseguridad, gestionar las vulnerabilidades es importante para proteger los sistemas de información. Este proceso implica detectar, evaluar y solucionar vulnerabilidades, utilizando información de diferentes fuentes para obtener una visión completa de la seguridad. Las ontologías juegan un papel importante al ayudar a organizar y analizar estos datos, lo que permite a las organizaciones entender mejor la gravedad de cada vulnerabilidad y emitir alertas cuando sea necesario. Al hacerlo, pueden priorizar acciones correctivas y mejorar su capacidad para enfrentar amenazas, fortaleciendo así su seguridad general.

El respaldo y la recuperación de datos son importantes para asegurar que las operaciones de una organización continúen sin interrupciones. Hacer copias de seguridad regularmente garantiza que la información crítica esté a salvo y pueda recuperarse en caso de pérdida o daño.

Esto no solo ayuda a reducir el tiempo de inactividad, sino que también contribuye a mantener la productividad y la confianza en la seguridad de los datos.

Por otro lado, la educación constante del personal es esencial para protegerse contra las amenazas cibernéticas. Estrategias como las simulaciones de phishing permiten a los empleados aprender a reconocer y reportar correos sospechosos, lo que ayuda a minimizar el riesgo de ataques.

Seguir normativas como la ISO/IEC 27001:2013 proporciona un marco que refuerza la protección de la información y aumenta la confianza con socios y clientes. En Colombia, políticas como la CONPES 3995 también subrayan la importancia de cumplir con estas regulaciones para fortalecer la seguridad digital en las organizaciones.

Discusión y Limitaciones

En este trabajo se analizaron algunas estrategias innovadoras de ciberseguridad para enfrentar las amenazas informáticas que están surgiendo. Encontrando que no existe una solución que funcione para todo. Por ejemplo, los diferentes modelos de control de acceso (como DAC, MAC, RBAC y TBAC) tienen sus ventajas y desventajas, dependiendo de dónde y cómo se utilicen. Aunque el RBAC parece ser más útil para organizaciones grandes porque usa roles, se puede complicar en situaciones donde el entorno cambia mucho o hay que colaborar bastante. De allí la importancia que los sistemas de seguridad sean flexibles y adaptables.

Otro hallazgo relevante, fue sobre el uso del aprendizaje automático para detectar amenazas. Esta tecnología ha sido bastante efectiva para identificar patrones peligrosos, pero su éxito depende mucho de la calidad de los datos que se usen para entrenarla.

Un problema que puede ocurrir es que, si los modelos no se entrenan bien, pueden cometer errores, como marcar algo seguro como una amenaza o dejar pasar una amenaza real. También el presente trabajo estableció que la gestión de vulnerabilidades es algo clave, pero no es fácil. Es necesario ser proactivo, pero uno de los problemas principales es cómo decidir qué vulnerabilidades son más urgentes, ya que hay demasiados datos que revisar. Las ontologías, que ayudan a organizar y analizar estos datos, pueden ser útiles, pero no son fáciles de implementar, especialmente si no se cuenta con muchos recursos.

Una de las principales limitaciones encontradas fue la falta de datos en tiempo real o de incidentes recientes que pudieran haber enriquecido el análisis. Además, como las amenazas cibernéticas cambian rápidamente, es probable que algunas de las soluciones que mencioné queden obsoletas pronto. Por eso, creo que es fundamental revisar y actualizar constantemente las estrategias de ciberseguridad.

Conclusiones

El estudio de las técnicas recientes en ciberseguridad muestra un panorama en constante cambio, donde las vulnerabilidades tecnológicas evolucionan rápidamente. A medida que los ataques cibernéticos se vuelven más sofisticados, es esencial adoptar enfoques innovadores, como la inteligencia artificial y la ciberseguridad cuántica, que no solo protegen información y sistemas, sino que también se adaptan a esta complejidad que avanza día a día. Sin embargo, con estas soluciones surgen nuevos desafíos, como la seguridad en el Internet de las Cosas y la gestión de la inteligencia artificial, lo que nos muestra la necesidad de una vigilancia continua y una preparación constante. En este mismo sentido la ciberseguridad es fundamental para mantener la confianza en un mundo digital cada vez más interconectado, lo que implica combinar tecnología avanzada con prácticas sólidas de gestión de riesgos y formación constante.

Las estrategias disruptivas de ciberseguridad analizadas demuestran que las soluciones tradicionales no son suficientes para enfrentar las amenazas emergentes. Innovaciones como el aprendizaje automático y la colaboración entre equipos de seguridad son cruciales para mejorar la capacidad de las organizaciones de anticiparse y reaccionar rápidamente, lo que garantiza la protección integral de los activos digitales.

En este mismo orden de ideas, el análisis de las técnicas recientes de ciberseguridad ha revelado que las amenazas evolucionan a un ritmo acelerado, lo que hace necesario un enfoque adaptativo en la gestión de vulnerabilidades. Tecnologías como el aprendizaje automático, que permiten una detección más precisa de amenazas, son clave para abordar las vulnerabilidades dinámicas en el entorno digital.

Correlacionar estrategias avanzadas de protección cibernética es fundamental para anticipar y responder de manera eficaz a las amenazas emergentes. Entre las principales

estrategias disruptivas se encuentran el uso de inteligencia artificial y aprendizaje automático, que permiten detectar y responder rápidamente a incidentes, así como la segmentación de redes, que minimiza el impacto de ataques al aislar distintas partes de la red. Además, la monitorización continua y la automatización de respuestas garantizan que las amenazas se identifiquen y se puedan detener en tiempo real, mejorando la protección de la infraestructura digital.

También es importante la capacitación y concienciación del usuario, ya que muchos riesgos cibernéticos surgen de errores humanos o desconocimiento. Estrategias como la actualización y parcheo automatizado de software, el análisis del comportamiento de los empleados y las pruebas de penetración ayudan a crear una defensa más fuerte contra ataques cibernéticos. Cuando se implementan estas medidas se forma una barrera efectiva que mejora la capacidad de una organización para resistir y mitigar las amenazas cibernéticas.

En este sentido, las estrategias avanzadas de protección, como los controles de acceso basados en tareas (TBAC) y roles (RBAC), junto con el monitoreo constante y la detección automatizada de amenazas, han demostrado ser efectivas para anticipar y mitigar ataques informáticos. El éxito de estas estrategias depende de su correcta implementación y la adaptación a entornos colaborativos.

De igual manera, la evaluación de la eficacia de soluciones de protección de datos en entornos digitales permite identificar como podemos responder a riesgos asociados a la pérdida o robo de información confidencial. Elementos como el cifrado, los controles de acceso, el monitoreo y detección de amenazas, y la gestión de vulnerabilidades son esenciales para garantizar la integridad, confidencialidad y disponibilidad de los datos. Además, el respaldo y recuperación de información, junto con el cumplimiento normativo y la educación continua del personal, complementan un enfoque integral de protección.

Este análisis no solo asegura la implementación de medidas técnicas, sino que también promueve una cultura de ciberseguridad sólida y adaptable a los riesgos emergentes y comprometida con la protección de los activos digitales en un entorno cada vez más interconectado.

La ciberseguridad está en constante evolución, y las técnicas actuales deben adaptarse rápidamente a las nuevas amenazas y vulnerabilidades que surgen. Tecnologías como la inteligencia artificial y la ciberseguridad cuántica juegan un papel clave en la protección de sistemas y datos, pero también presentan desafíos, como asegurar el Internet de las Cosas (IoT) y gestionar la inteligencia artificial de manera adecuada. Es esencial estar al día con innovaciones como el aprendizaje automático y la automatización de respuestas, que permiten detectar y reaccionar ante ataques de forma más eficiente. Las estrategias tradicionales ya no son suficientes, y la vigilancia constante es clave para mantenerse protegido.

En los sectores empresarial, educativo y gubernamental, es fundamental tener un enfoque integral que combine tecnología avanzada con una fuerte cultura de ciberseguridad. La capacitación continua es vital para prevenir riesgos causados por errores humanos, mientras que las medidas como el cifrado de datos, la segmentación de redes y los controles de acceso ayudan a proteger la información. Además, fomentar la colaboración entre equipos de seguridad, tanto dentro como fuera de la organización, fortalece la capacidad de respuesta ante incidentes. Estas prácticas son esenciales para mejorar la defensa en sectores interconectados y asegurar la protección frente a amenazas cada vez más complejas.

Mirando hacia el futuro, las tendencias en ciberseguridad están apuntando hacia el uso de tecnologías avanzadas como la computación cuántica y las redes neuronales, que mejorarán la precisión y rapidez en la detección de amenazas. Sin embargo, será necesario encontrar un

equilibrio entre la protección de datos y la privacidad de los usuarios. Con el aumento del monitoreo y las tecnologías de vigilancia, las organizaciones deberán ser transparentes y responsables en cómo implementan estas herramientas, asegurando que se protejan tanto los sistemas como los derechos de los usuarios.

El futuro de la ciberseguridad estará marcado por la integración de nuevas tecnologías que puedan afrontar los desafíos emergentes de un mundo digital cada vez más complejo y conectado. Si bien estas innovaciones ofrecen grandes promesas, también traerán consigo nuevos desafíos que exigirán una vigilancia constante y una adaptación rápida de las estrategias de defensa.

Referencias Bibliográficas

Aimaretto, L., Dujovne, D. (2023). Enhancing end-to-end determinism and reliability in 6TiSCH networks with disjoint leaf-based MPLS-like tunnels. Internet of Things (Netherlands), 24. https://doi.org/10.1016/j.iot.2023.100988

Almeida, P., Josué, J., Vera, M., Johana, J., Vera, G., Jacinto, M., Rendon, Z., Dolores, A. (s.f.). Análisis de ejercicios de Ataque y Defensa en Ciberseguridad. https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/sigloxxi/XI/CIDEIT/S3/CIDEIT-S3-010.pdf

Angel, I., Odriozola, M., Larrart, R., Leguizamon, R., Proietti, M., Seijas, L., Georgopulos, A. (2018). Seguridad en Internet de las Cosas. https://grupogemis.com.ar/wp-content/uploads/2018/11/SyO_M_SeguridadEnIoT.pdf

Arreola, A. (2019). Ciberseguridad. https://www.google.com.co/books/edition/Ciberseguridad/ZqHDDwAAQBAJ?hl=es&gbpv=0&kptab=getbook

Atlam, H., Oluwatimilehin, O. (2023). Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. Electronics (Switzerland), 12(1). MDPI. https://doi.org/10.3390/electronics12010042

Avenía, C. (2017). Fundamentos de seguridad informática. https://digitk.areandina.edu.co/handle/areandina/1367

Baltuttis, D., Teubner, T., Adam, M. (2024). A typology of cybersecurity behavior among knowledge workers. Computers and Security, 140. https://doi.org/10.1016/j.cose.2024.103741

Barroso, V. (2021). Análisis y Simulación de un Ataque de Phishing. https://upcommons.upc.edu/handle/2117/355777

Blasco, P. (2019). Guía práctica de ciberseguridad en el hogar. https://rua.ua.es/dspace/handle/10045/93293

Burgos V. (2021). Cifrado de datos usando Cadena de Bloques (BlockChain) como tecnología de convergencia para dispositivos móviles asociados con IoT (Internet of Things), en la capa de aplicación del modelo de capas IoT. https://repositorio.utn.edu.ec/handle/123456789/11459

Canfranc, P. (2019). Ciberseguridad Protegiendo la información vulnerable. https://www.google.com.co/books/edition/Ciberseguridad/_LuGDwAAQBAJ?hl=es&gbpv=0

Cuzme R, Fabian G. (2015). INTERNET DE LAS COSAS TESIS Y CONSIDERACIONES DE SEGURIDAD. https://repositorio.puce.edu.ec/items/76adc1dd-9f40-4c2e-985a-220b6ee9aa36

Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006&lang=es

Fernando, C., Vallejo, M. (2023). Inteligencia Artificial y el Aprendizaje Automático en la Ciberseguridad. https://repository.unipiloto.edu.co/handle/20.500.12277/13395

Gómez Rivadeneira, m. b. (2013). cifrado de datos transmitidos a través de redes inalámbricas. https://repositorio.puce.edu.ec/items/0fe6d142-5db3-4dc7-add8-e7d8b89f3da7

Granados, J. (2022). Análisis de la inteligencia artificial en las relaciones laborales. CES Derecho, 13(1), 111–132. https://doi.org/10.21615/cesder.6395

Iñiguez, H. (2020). Seguridad Informática y Protección de Datos Personales ¿Qué tan protegido estás en internet? https://www.google.com.co/books/edition/SEGURIDAD_INFORM%C3%81TICA_Y_PROTECCI%C3%93N_DE/4ewEEAAAQBAJ?hl=es&gbpv=0

Khan, A. (2017). Key Characteristics of a Container Orchestration Platform to Enable a Modern Application. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/8125559

Mario, A., Peñaloza, A., Adolfo, P., Mendoza, S. (2023). Ciberseguridad: Tipos de ataques y vulnerabilidades en IoT para el hogar. https://bonga.unisimon.edu.co/items/b61ae2b2-1dc6-467b-9a28-f2ef2799855f

Naydenov, N., Ruseva, S. (2023). Cloud Container Orchestration Architectures, Models and Methods: A Systematic Mapping Study. 2023 22nd International Symposium INFOTEH-JAHORINA, INFOTEH 2023. https://doi.org/10.1109/INFOTEH57020.2023.10094059

Nieles, M., Dempsey, K., Pillitteri, V. (2017). An introduction to information security. https://doi.org/10.6028/NIST.SP.800-12r1

Nikolskaia, K., Naumov, V. B. (2021). The Relationship between Cybersecurity and Artificial Intelligence. Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021, 94–97. https://doi.org/10.1109/ITQMIS53292.2021.9642782

Ortega, J. (2024). CIBERSEGURIDAD Manual práctico. https://www.google.com.co/books/edition/_/oWT7EAAAQBAJ?hl=es&gbpv=1

Ortega, J. (2024). Ciberseguridad: Manual práctico. https://books.google.com.co/books?hl=es&lr=&id=oWT7EAAAQBAJ&oi=fnd&pg=PA1&dq=ciberseguridad:+Monitorizaci%C3%B3n+Continua&ots=Bb6lSGOyGb&sig=3TL

bj6-ThKif7Ff6MEkXqkKvJk4&redir_esc=y#v=onepage&q=ciberseguridad%3A%20Monitorizaci%C3%B3n%20Continua&f=false

Park, C., Kim, Y. (2019). PlatCon-19: 2019 International Conference on Platform Technology and Service: proceedings: 28-30 January, 2019, Jeju, Korea. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/8669410/authors#authors

Pulido, T. (2022). La Ciberseguridad es Clave en el Éxito Empresarial. https://repository.unimilitar.edu.co/handle/10654/44244

Ramírez, M., Arango, A., Blum, C., Carrasquilla, A., Cabello, M., Trujillo, H., Ruíz, F., Cabrera, B., Restrepo, J., González, V., Lozano, M., Malagón, J., Abudinen, K., Orozco, A., Barrero, E., Torres, M., Rodríguez, L., Gómez, D. (2022). Política Nacional De Confianza y Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Rivadeneira, M. (2013). Cifrado de Datos Transmitidos a Través de Redes Inalámbricas. https://repositorio.puce.edu.ec/items/0fe6d142-5db3-4dc7-add8-e7d8b89f3da7

Rodríguez, C., Geovanny, F. (2015). Internet de las Cosas Tesis y Consideraciones de Seguridad. https://repositorio.puce.edu.ec/items/76adc1dd-9f40-4c2e-985a-220b6ee9aa36

Romaniz, S. C. (2008). Seguridad de aplicaciones web: vulnerabilidades en los controles de acceso. https://sedici.unlp.edu.ar/handle/10915/21581

Rouhiainen, L. (2018). Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro. Alienta.

Swati, S., Rawat, A. (2011). 2011 International Conference on Emerging Trends in Networks and Computer Communications. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/5958480

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information and Management, 57(6). https://doi.org/10.1016/j.im.2020.103334

Vela, L., Pascual, V., Granollers, T., Paderewski, P. (2020). Revisión del Modelo de Privacidad Adaptativa para Evaluar Aplicaciones de Redes Sociales. Internet of Things (Netherlands), 1–12.

Yadav, D. C., Bhagwat, R., & Saha, A. (2023). Quantum Computing Enhancements in Deep Learning Models for Cybersecurity. International Conference on Recent Advances in Science and Engineering Technology, ICRASET 2023. https://doi.org/10.1109/ICRASET59632.2023.10420030

Zhao, X., Li, M., Feng, E., & Xia, Y. (2022). Towards A Secure Joint Cloud with Confidential Computing. Proceedings - 2022 IEEE 13th International Conference on Joint Cloud Computing, JCC 2022, 79–88. https://doi.org/10.1109/JCC56315.2022.00019