UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN SEPTIEMBRE 2024 – MARZO 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

LA INTELIGENCIA ARTIFICIAL EN LA DETECCIÓN DE INTRUSOS EN INFRAESTRUCTURA DE TI

ESTUDIANTE:

ANTHONY ARON HERRERA FLORES

TUTOR:

ING. FERNANDEZ TORRES ANA DEL ROCÍO

AÑO 2024 - 2025

ÍNDICE

RESUMEN

La digitalización ha convertido a las infraestructuras de TI en blancos de ataques cibernéticos cada vez más sofisticados, evidenciando las limitaciones de los métodos tradicionales de detección de intrusos. En este contexto, la Inteligencia Artificial (IA) emerge como una herramienta clave para mejorar la identificación de amenazas, reducir falsos positivos y automatizar la respuesta ante incidentes.

Este estudio analiza el impacto de la IA en ciberseguridad, comparando algoritmos como Random Forest, Redes Neuronales y Support Vector Machines (SVM) en la detección de intrusos. Además, se identifican factores críticos para su implementación, como la calidad de los datos, costos y capacitación del personal.

Los hallazgos resaltan que la IA mejora significativamente la detección de amenazas y la adaptación a nuevos ataques. No obstante, su adopción enfrenta desafíos técnicos y económicos. Finalmente, se proponen estrategias para optimizar su integración en entornos empresariales, garantizando una protección más eficiente contra ciberataques.

Palabras clave: Ciberseguridad, Inteligencia Artificial, detección de intrusos, Machine Learning, infraestructuras de TI, algoritmos de clasificación, Redes Neuronales, ataques cibernéticos, automatización en seguridad informática.

SUMMARY

Digitalization has turned IT infrastructures into targets of increasingly sophisticated cyber attacks, highlighting the limitations of traditional intrusion detection methods. In this context, Artificial Intelligence (AI) emerges as a key tool to improve threat identification, reduce false positives and automate incident response.

This study analyzes the impact of AI in cybersecurity, comparing algorithms such as Random Forest, Neural Networks and Support Vector Machines (SVM) in intrusion detection. In addition, critical factors for its implementation are identified, such as data quality, costs and staff training.

The findings highlight that AI significantly improves threat detection and adaptation to new attacks. However, its adoption faces technical and economic challenges. Finally, strategies are proposed to optimize its integration into business environments, guaranteeing more efficient protection against cyber attacks.

Keywords: Cybersecurity, Artificial Intelligence, intrusion detection, Machine Learning, IT infrastructures, classification algorithms, Neural Networks, cyber attacks, automation in computer security.

PLANTEAMIENTO DEL PROBLEMA

Las infraestructuras de tecnología de información dentro un entorno altamente digitalizado, son extremadamente importantes para garantizar la continuidad en funcionamientos en sectores como la banca, la salud, la educación y el comercio. A pesar de ello esta creciente dependencia se transforma en el objetivo primordial del uso cada vez más avanzado de los ciberdelincuentes para socavar la seguridad. Bajo estas amenazas la intrusión en los sistemas de TI, es una de las más critica, esto se debe a que puede conducir a un acceso no autorizado, robo de información confidencial y operaciones.

Los métodos tradicionales de detección de intrusos han resultado inadecuados por la complejidad de las nuevas amenazas. La IA por su parte, se está posicionando como una alternativa interesante al permitir la detección de ataques de formas mucho más eficaces utilizando algoritmos complejos de (Machine Learning) a pesar de su utilidad, aún es necesario determinar qué puede afectar su rendimiento, como por ejemplo, la calidad de los datos, la infraestructura de tecnología disponible, los costos de implementación y la capacitación del personal.

La investigación de un estudio sobre la tecnología de seguridad corporativa en Guayaquil. (Sánchez Ramírez y Andaluz Granda, 2024) demuestra la importancia de la protección de datos, los sistemas y las redes comerciales. Aunque la Inteligencia Artificial (IA) no se mencionó específicamente en la detección de intrusos, este estudio destaca la necesidad de estrategias tecnológicas avanzadas para aumentar lo que sería la seguridad empresarial. Esto aumenta la necesidad de buscar nuevas soluciones como Inteligencia artificial que puede optimizar la identificación de amenazas y la reducción de la infraestructura tecnologicas para la información comercial.

En consecuencia, es supér importante realizar un análisis profundo para determinar el impacto de IA en la detección de intrusos, evaluando así, tanto a sus beneficios, limitaciones y áreas de mejora. Esto permitirá poder comprender su verdadero potencial y también permitirá definir estrategias que fortalezcan la seguridad en las infraestructuras de (TI) frente a las amenazas emergentes.

JUSTIFICACIÓN

Las infraestructuras de tecnología de información son claves para el funcionamiento de cualquier organización incluida las empresas. Pero hay un problema, los ataques cibernéticos han aumentado, esto obliga a buscar formas más avanzadas para para la detección y prevención de intrusos.

Aquí es donde entra la Inteligencia Artificial (IA). Su capacidad para analizar el tráfico de red, identificar patrones anómalos y respuestas en tiempo real la convierte en una herramienta poderosa para mejorar la seguridad informática. Sin embargo, su implementación no es tan sencilla, porque depende de varios factores, como la infraestructura tecnológica disponible, el presupuesto de cada empresa y, claro, la preparación de los expertos en ciberseguridad.

En Guayaquil un informe de una auditoría de seguridad informática, Según (Sánchez Ramírez y Andaluz Granda, 2024) se pone de manifiesto que varias empresas necesitan mejorar la protección de sus recursos informáticos. Sin embargo, todavía dependen de técnicas obsoletas que ya no son adecuadas frente a amenazas más complejas. Esto hace que sea fundamental evaluar cuán efectiva sería la IA para la detección de intrusiones y cuán práctica sería su implementación en el sector empresarial de la ciudad.

Este análisis es importante no solo para entender los beneficios y limitaciones de la IA en la ciberseguridad , sino también para diseñar estrategias que hagan su implementación más práctica y accesible. Con esta investigación, la idea es que las empresas de Guayaquil puedan proteger mejor su información sin que el proceso de adopción de nuevas tecnologías sea una carga imposible de asumir.

OBJETIVOS

OBJETIVO GENERAL

Analizar la contribución de la Inteligencia Artificial en la detección de intrusos en infraestructuras TI, considerando su aplicabilidad en entornos empresariales.

OBJETIVO ESPECÍFICOS

1. Identificar los principales beneficios de la Inteligencia Artificial en la detección de intrusos en infraestructuras TI y su impacto en la seguridad de organizaciones.

2. Determinar los factores que influyen en la efectividad de la Inteligencia Artificial en la detección de intrusos en infraestructuras de TI, considerando las necesidades de seguridad en entornos empresariales

3. Proponer algoritmos de (Machine Learning) para la detección de intrusos en infraestructuras de TI, evaluando su aplicabilidad y eficiencia en distintos escenarios de ciberseguridad empresarial.

LÍNEAS DE INVESTIGACIÓN

- Sistemas de información y comunicación, emprendimiento e innovación.

SUBLÍNEA DE INVESTIGACIÓN

- Redes y tecnologías inteligentes de software y hardware.

La linea investigativa esta conectada entre si con el estudio y su análisis sobre: La Inteligencia Artificial en la Detección de Intrusos en infraestructura de (TI) que a su vez también integra la tecnología de la información que es uno de los aspectos principales sobre el cual este estudio se enfoca. El estudio tiene como objetivo el uso de algoritmos de aprendizaje de máquina conocidos también como (Machine Learning) y redes neuronales en el incremento de la ciberseguridad en los sistemas de información y protección de activos digitales contra amenazas nuevas y emergentes.

La sublínea de investigación en este caso trata sobre el análisis de ciberataques mediante el uso de redes de computadoras, donde la sublínea enfocada en sistemas de detección de intrusiones y aprendizaje automático en el área de seguridad de redes tiene un contacto directo. La competencia que utiliza técnicas sofisticadas de infiltración en sistemas por lo general compromete datos y afecta la operativa de la organización. Con estos problemas, la inteligencia artificial es capaz de facilitar la mejor detección y prevención de intrusos utilizando algoritmos de aprendizaje automatizados que observan patrones, anomalías y responden de forma automatizada a incidentes en la seguridad.

MARCO CONCEPTUAL

¿Qué es la Inteligencia Artificial (IA)?:

Como señala (Telecomunicaciones UExternado, 2023), la Inteligencia Artificial (IA) es una área de informatica en el desarrollo de máquinas capaces de realizar tareas que requieren inteligencia humana, tales como aprender, razonar y resolver problemas, procesando grandes volúmenes de datos, identificando patrones y tomando decisiones sin intervención humana.

La evolución de la Inteligencia Artificial (IA):

Según, detalla (Fundación Bankinter, 2023), el avance de la Inteligencia Artificial (IA) es de caso muy significativo, desde un simple algoritmo hasta un modelo de aprendizaje automaticos de máquina y redes neuronales. Esta evolución ha permitido el uso de la IA en ciberseguridad, en el diagnóstico médico y también en la automatización de la industria.

Tipos de Inteligencias Artificiales:

Como señala, (BBC News Mundo, 2023). Las tecnología en IA se divide en categorías dependiendo del grado de ensamblaje de características humanas:

Inteligencia Artificial Débil (ANI):

La que es construida para realizar alguna tarea a un determinado nivel, por ejemplo, reconocimiento de voz o imagen.

Inteligencia Artificial General (AGI):

Que puede desempeñar todas las funciones cognitivas de la misma manera que un ser humano, pero a un nivel mucho más bajo.

Inteligencia Artificial Superior (ASI):

Que supera en todo a los seres humanos, a nivel por ejemplo en la creatividad, la escritura y la toma de decisiones.

Los Componentes principales de la Inteligencia Artificial (IA)

La Inteligencia Artificial, consta de componentes clave, los cuales hacen posible que las máquinas realicen tareas difíciles las mismas que normalmente necesitan de la participación humana. Entre los componentes resaltan el aprendizaje automático, las redes neuronales, procesamiento de lenguaje natural y algoritmos evolutivos. (Martín M, 2023)

Aprendizaje automático (machine learning)

También conocido como el aprendizaje asistido por máquinas, una herramienta clave para la Inteligencia Artificial. Es muy útil para cualquier sistema, ya que implica la posibilidad de los mismos de aprender algo de los datos, es decir, de hacer predicciones más o menos precisas y seguir mejorando sin ninguna codificación explícita.(García L, 2023)

Las redes neuronales artificiales

Se inspiraron en la estructura del cerebro humano y, en consecuencia, se emplean para procesar datos altamente complejos. En especial, redes de aprendizaje profundo han sido críticas para encontrar patrones avanzados y resolver problemas de clasificación compleja. (Pérez J, 2024)

El procesamiento de lenguaje natural (PLN)

Brinda la capacidad a las máquinas de interpretar y generar lenguaje humano. Aunque sus aplicaciones son muy amplias en muchos campos, en ciberseguridad cada vez es más habitual que los sistemas analicen mensajes en busca de amenazas, como phishing o simplemente comunicaciones maliciosas :. Phishing y amenazas sociales en la red. (Conzultek, 2023)

Finalmente, ***algoritmos evolutivos basados en conceptos de selección natural*** optimizan problemas complejos, adaptándose de forma dinámica a nuevas amenazas en el campo cibernético según WeLiveSecurity, (2023)

La importancia de Inteligencia Artificial en la ciberseguridad:

Según (Conzultek, 2023) señala que: El uso de la inteligencia artificial ha supuesto un cambio importante en la ciberseguridad, ya que ahora proporciona a los usuarios herramientas para detectar y responder a las ciberamenazas en tiempo real. La IA tiene la capacidad de trabajar con conjuntos de datos enormemente grandes y puede detectar patrones anormales e incluso ayudar con diferentes aspectos de la ciberseguridad que los métodos tradicionales no logran abordar.

La evolución de la inteligencia artificial en ciberseguridad:

Según (López, 2023) señala, que: El avance de la inteligencia artificial (IA) en ciberseguridad, ha llevado al desarrollo de sistemas autónomos los mismos que pueden responder de manera instantánea a un ataque esto ayuda a minimizar así el daño potencial y también ayuda fortaleciendo la flexibilidad de infraestructuras críticas.

Desafíos en la Implementación de IA para la Detección de Intrusos:

Según (Servnet, s.f.). La implementación de la inteligencia artificial en la automatización del seguimiento de intrusos cibernéticos a través de la IA, hay varios problemas que necesitan resolverse, como:

Sesgo de Datos (Información):

El sesgo de datos es uno de los problemas relacionados con los impactos negativos de los

conjuntos de datos sesgados en la detección de intrusos cibernéticos. Los datos sesgados cubren muchos términos que impactan la precisión de los modelos. Eso se debe a que los grupos de entrenamiento se seleccionan con mucho sesgo que no tiene en cuenta la miríada de amenazas posibles. La aplicación inadecuada de los conjuntos de datos lleva a la generación de modelos sesgados. Por lo tanto, el uso de Inteligencia Artificial en contextos críticos no solo resuelve los problemas pero también aporta nuevos.

Requerimientos de grandes volúmenes de información:

Para que los modelos funcionen de manera óptima, los algoritmos de Inteligencia Artificial necesitan conjuntos de datos muy voluminosos, lo cual supone retos bastante importantes en términos de captura, almacenamiento y procesos de manipulación de los datos. La gestión de esos datos no es solo costosa, sino que además hay que manejar complejas cuestiones éticas y también las legales, los datos en los deep learning datasets que se suelen utilizar para obtener información, tienen gran necesidad de datos, porque se tiene garantías en exceso, la privacidad del usuario final, lo que permite la posible exposición de información sensible.

Carencia de expertos cualificados:

Como hemos dicho, la falta de un ciberexperto con un alto nivel de competencia, sumado a la complejidad propia de las soluciones de seguridad de Inteligencia Artificial, puede traer como consecuencia decenas de años de atraso en la implementación de sistemas modernos apoyados en IA, mermando altamente su efectividad.

Incorporación en sistemas ya establecidos:

La sistematización de la Inteligencia Artificial en las ya existentes bases de datos en la seguridad pueden de igual manera, ser un procedimiento sencillo, el raspado de nuevos algoritmos de IA encima de sistemas ya existentes necesita un monitoreo de todo el sistema, lo que eleva la necesidad de cambios estructurales, actualización integral de los sistemas

Los costos de implementación de (IA):

La aplicación de Inteligencia Artificial en un área tan delicada como la ciberseguridad conlleva alza muy alta inversión relacionada no solo con el diseño de los modelos y el entrenamiento de los mismos, sino también con la infraestructura tecnológica que requieren para funcionar. Este hecho puede hacer que estas soluciones se tornen menos accesibles para ciertos tipos de organizaciones que no puedan hacer frente a la inversión necesaria.

Las ventajas de la inteligencia artificial en la detección de intrusos:

Mejora de la precisión y rapidez en la detección de amenazas:

La IA otorga la capacidad de identificar y responder a daños potenciales por medio de la intrusión, esto facilita el proceso al poder hacer una respuesta anticipada al daño que se pueda causar previamente.

Reducción de falsos positivos:

El análisis y comportamiento de la IA permite comprender la ciencia detrás de las alertas falsas y su reducción posterior. Esto permite responder un número mayor de amenazas reales y creíbles. (The Bridge, 2023)

Respuesta Automática a Incidentes:

La IA responde automáticamente a las amenazas, impidiendo que los intrusos puedan entrar y causar destrucción durante un ataque (Protecdata Colombia, 2022).

Capacidad de ajustes ante nuevas amenazas:

(Cámara de Comercio de Mallorca, s. f.) detalla que, la IA a través de algoritmos de aprendizaje profundo, es capaz de defender proactivamente contra ataques nuevos o avanzados que son desconocidos para las bases de datos tradicionales.

Conexión con sistemas de seguridad existentes

El uso de inteligencia artificial en ciberseguridad ya está viendo una mezcla de su adopción con medidas de seguridad existentes. Esto no solo aumenta la efectividad de las tácticas que se han adoptado, sino que también hace que su implementación sea sin esfuerzo. (IT Digital Security, 2023)

Aspecto	Ventajas	Desventajas
Precisión en detección	Detecta amenazas en etapas tempranas, reduciendo riesgos.	Puede generar falsos positivos o negativos si los datos de entrenamiento no son adecuados.
Reducción de falsos positivos	Permite que los equipos de seguridad se acerquen a amenazas reales.	En algunos casos, ciertos algoritmos pueden generar alertas erróneas, afectando la eficiencia.
Automatización de respuestas	Bloquee accesos no autorizados sin intervención humana.	Un error en el sistema podría bloquear a los usuarios legítimos.
Adaptabilidad a nuevas amenazas	Se ajusta de manera autónoma a nuevos ataques mediante aprendizaje profundo.	Requiere una gran cantidad de datos y entrenamiento constante para ser efectivo.
Integración con sistemas existentes	Compatible con diversas soluciones de ciberseguridad.	Puede requerir actualizaciones en la infraestructura, lo que incrementa los costos.
Costo de implementación	Puede reducir costos operativos a largo plazo.	Su implementación inicial es costosa y requiere inversión en hardware y software avanzado.
Dependencia del personal capacitado	Reducir la carga de trabajo de los analistas de seguridad.	Requiere expertos en IA y ciberseguridad para su correcta gestión y mantenimiento.

Tabla 1. Ventajas y Desventajas de la IA en la detección de Intrusos

Fuente: Anthony Herrera

Ciberseguridad en Infraestructuras TI:

La ciberseguridad aplicada a las infraestructuras TIC podemos entenderla como la estrategia de métodos, tecnologías, normativas que tienen la finalidad de proteger tanto a los sistemas informáticos como las redes de ordenadores y la información de accesos no autorizados, ataques maliciosos y daños imprevistos. Entendiendo la protección cibernética como un concepto que incluye no sólo las acciones preventivas sino también

las correctivas, que buscan reducir el riesgo y asegurar el correcto funcionamiento de la tecnología esencial para las organizaciones. (IBM, 2023)

Objetivos de la Ciberseguridad en Infraestructuras TI:

Según, (UMAD 2024) La ciberseguridad persigue objetivos específicos que es fundamental no perder de vista, objetivos como:

Proteger la información crítica y los activos digitales:

Una de las finalidades más importantes de la ciberseguridad consiste en proteger la información confidencial y privada de las personas y de las empresas. Todo ello entra dentro de la información pública, la información personal, la información financiera, la información comercial y otras clases de información sensible y de especial relevancia. En un mundo cada vez más digital, donde gran parte de la información está informatizada, es necesario garantizar el acceso seguro a la información informatizada. Para ello se utilizan métodos y prácticas como el cifrado de la información, la gestión de políticas de acceso y la gestión de la identidad del acceso y el uso del sistema asociativo (IAM).

Prevenir y reaccionar ante ciberataques:

Los incidentes cibernéticos constituyen una de las más peligrosas realidades en lo que concierne a la seguridad de los sistemas y redes informáticas, pues con el avance de la tecnología los ciberdelincuentes han diseñado otros métodos de ataque más sofisticados y devastadores. Por lo que debemos tener estrategias para prevenir y responder a los incidentes, los cuales los mas relevantes son los los virus, el malware, el ransomware, el phishing, por lo que para prevenir estos incidentes cibernéticos es necesario contar con medidas preventivas como la utilización de firewalls, sistemas de detección de intrusos (IDS) o programas de seguridad actualizados.

Asegurar la integridad y disponibilidad de los sistemas y redes:

La ciberseguridad centra su interés en certificar la integridad y la disponibilidad de los sistemas y las redes. Esto significa que se asegura que los sistemas y las redes sean

funcionales independientemente de los ataques y de las caídas, así como que el negocio se pueda ejecutar ante una crisis o un estado de emergencia. Para conseguir lo anterior, es necesario implementar funcionalidades de monitorización y detección de error, sistemas de disponibilidad continua o redundancia, así como asegurar que existan las políticas y los procedimientos que aseguren que los sistemas y las redes estén actualizados y libres de vulnerabilidades conocidas. Asimismo, la protección cibernética tiene como objetivo proteger la infraestructura de ataques que puedan perjudicar las operaciones del negocio provocando paradas de servicio, pérdidas de datos importantes, o el robo de propiedad intelectual; de este modo se convertirá en un elemento fundamental para asegurar la resiliencia empresarial y reducir el impacto negativo de forma económica y reputacional. (Fortra, 2023)

Los tipos de amenazas y ataques cibernético:

(Fortinet, 2023) indica que: Los 20 ataques cibernéticos más comunes son:

Malware:

El malware, también denominado como software dañino, constituyen software malicioso cuyo propósito es el de infectar, dañar o interrumpir los sistemas informáticos. Bajo esa etiqueta se encuentran, por ejemplo:

Virus: Virus que se replican al infectar ficheros.

Troyanos: Se presentan como aplicaciones legítimas.

Ransomware: Los cuales cifran información y exigirán rescate para restaurar su acceso.

El malware es el tipo de software que más preocupa, porque suele evadir los sistemas de detección y pueden adaptarse a nuevas amenazas.

Phishing:

El phishing consiste en una técnica de ingeniería social en la que los atacantes se hacen pasar por entidades legítimas para llevar a engaño a la víctima y conseguir de tal forma

que comparta información sensible y confidencial (contraseñas, datos bancarios, etc.). Normalmente, los mensajes de phishing contienen enlaces con el propósito de redirigir a los usuarios hacia otro sitio Web de apariencia falsa, tal como podría ser el sitio legítimo, que tiene la finalidad de capturar datos. Este método continúa siendo especialmente eficaz, y su efectividad se incrementa si se emplean técnicas de personalización.

Ransomware:

El ransomware está constituido por un tipo de malware que cifra los ficheros críticos que se encuentran en un sistema y que solicitará el pago para que el acceso a los datos pueda desbloquearse. Las organizaciones son uno de los objetivos habituales de este tipo de ataque, debido a la magnitud de la incapacidad que representa la pérdida de acceso a los datos que son esenciales para su continuidad. El ransomware se ha desarrollado para pasar de los ataques que llevaban objetivos individuales a objetivos de infraestructuras.

Ataques de Denegación de Servicio (DoS) y de Denegación de Servicio Distribuidos (DDoS):

Los ataques de Denegación de Servicio (DoS) son aquellos que intentan sobrecargar los recursos de un sistema o red, bloqueando así las peticiones de información legítimas. En cuanto a las Denegación Distribuida (DDoS), estos ataques buscan la utilización de múltiples dispositivos comprometidos en lo que se denomina "botnet", con el objetivo de enviar el mayor tráfico posible de manera simultánea y provocar así la paralización de sitios web o servicios durante horas o días, con las consecuencias económicas que ello lleva aparejado.

Man-in-the-Middle o (MitM):

En esta modalidad de ataque “Man-in-the-middle” o “MitM”, el perpetrador se hace parte de una conversación entre dos partes y se hace pasar por una de ellas, llevando a cabo una serie de acciones en sus nombres.

Cryptojacking:

El ataque de cryptojacking llega a la utilización de recursos informáticos no autorizados

de un tercero para la minería de criptomonedas utilizando, normalmente, scripts maliciosos y utilizando el navegador de la víctima o bien utilizar malware. No es un ataque destructivo, pero consume muchos recursos del sistema y ralentiza el rendimiento de la red.

SQL Injection:

Dentro de la categoría de ataques hay uno que se denomina “SQL injection”, que se fundamenta en el uso ilegítimo de comandos SQL en los formularios de entrada de las webs. Generalmente, los atacantes intentan acceder a, modificar o eliminar los datos de una base de datos con altos niveles de sensibilidad, algo que resulta bastante peligroso para cualquier organización que contenga información sensible.

Exploits de Día Cero (Zero-Day):

El ataque de Día Cero (Zero-Day) es aquel que utiliza una vulnerabilidad en software o hardware, para el cual el desarrollador no ha podido llegar a solucionar dicha vulnerabilidad. Su peligrosidad es alta, siendo considerado este tipo de ataque de los más peligrosos, ya que los sistemas de defensa no están diseñados para detectar o mitigar las características de estos ataques en sus inicios.

Ingeniería Social:

Se basa en proporcionar acceso a sistemas o que realicen acciones como contraseñas y la instalación de viejos programas, para realizar acciones que dañen la seguridad. Se trata de aprovechar a los usuarios desinformados sobre ciberseguridad.

Fuerza Bruta:

Los ataques de fuerza bruta son aquellos ataques que prueban una y otra vez una u otra combinación de contraseñas y/o claves para encontrar la auténtica. Aunque no son sofisticados, los ataques de fuerza bruta pueden ser muy eficientes bajo las condiciones apropiadas, si las contraseñas no son lo suficientemente fuertes.

Cross-Site Scripting (XSS):

Se trata de un ataque que consiste en intercalar scripts maliciosos en aplicaciones web. Una vez inyectados, los scripts maliciosos ejecutan su acción en el entorno del navegador del usuario; esto permite que los atacantes roben datos de sesión, lleven a cabo las acciones que deseen o incluyan al usuario en sitios maliciosos.

Cross-Site Request Forgery (CSRF):

Este ataque daña y obliga a un usuario autenticado a realizar acciones no deseadas en toda aplicación web, lo cual es particularmente complicado si el usuario es un administrador.

Password Spraying:

No se enmarca en ataques de 'brute force', están en la lógica de compartir claves con el target que tiene varias cuentas. Esta técnica ayuda a sortear el problema de cuentas que se bloquean por motivos de intentos de login fallidos en exceso.

Credential Stuffing:

Efectuando un ataque 'credential stuffing', el atacante utiliza una cuenta previamente hackeada y comienza a utilizar diferentes combinaciones de nombres de usuario y contraseñas recolectadas de otras violaciones. Razón por la cual este ataque es especialmente efectivo en el contexto de los que tienen acumulativo de usuario y contrasermo compartidos en diferentes servicios.

Eavesdropping:

Se refiere a la práctica de obtener información confidencial y de manera ilegal como correos o sabes.

Watering Hole:

Este es un ataque en el que se comprometen las páginas web frecuentadas por el grupo objetivo. El propósito es distribuir malware, lo que resultará en comprometer a algunos de los usuarios que acceden a ese sitio web.

Typosquatting:

Esto captura el trabajo de obtener nombres de dominio que son variaciones de sitios web populares con el propósito de engañar a los usuarios con errores tipográficos, tanto así que las personas que visitan estos sitios falsos pueden caer en la trampa de robar información.

Phishing dirigido:

A diferencia de la mayoría de las actividades de phishing, donde el objetivo suele ser amplio, en el spear phishing el enfoque está dirigido a personas específicas.

Vishing:

Es uno de los tipos de phishing que se realiza a través de conversaciones telefónicas para intentar engañar a la víctima para que revele sus datos privados, típicamente, los atacantes se hacen pasar por instituciones reputables con el fin de lograr su objetivo.

Tipo de Ataque	Descripción	Impacto Principal
Malware	**Software malicioso diseñado para infectar, dañar o interrumpir sistemas.**	**Pérdida de datos, daños en el sistema, acceso no autorizado.**
Virus	**Se replica infectando archivos legítimos.**	**Corrupción de archivos y sistemas.**
Troyanos	**Se disfrazan de software legítimo para obtener acceso al sistema.**	**Robo de información, instalación de más malware.**
Ransomware	**Cifra archivos y exige un pago para restaurar el acceso.**	**Pérdida de datos, extorsión económica.**
Phishing	**Suplantación de identidad para robar información confidencial.**	**Robo de credenciales, fraudes financieros.**
Spear Phishing	**Ataque dirigido a personas u organizaciones específicas.**	**Acceso a información altamente sensible.**
Vishing	**Engaño mediante llamadas telefónicas.**	**Robo de datos personales y bancarios.**
Ataques DoS/DDoS	**Sobrecarga de tráfico que bloquea el acceso a un sistema.**	**Interrupción de servicios, pérdidas económicas.**
Man-in-the-Middle (MitM)	**Intercepción y manipulación de comunicaciones.**	**Robo de credenciales y datos financieros.**
Cryptojacking	**Uso no autorizado de hardware para minar criptomonedas.**	**Consumo excesivo de recursos, ralentización del sistema.**
SQL Injection	**Inserción de código SQL malicioso en formularios web.**	**Robo, alteración o eliminación de datos en bases de datos.**
Zero-Day Exploit	**Aprovecha vulnerabilidades desconocidas en software.**	**Acceso y control total sobre sistemas vulnerables.**
Ingeniería Social	**Manipulación psicológica para obtener información sensible.**	**Acceso no autorizado a cuentas y sistemas.**
Fuerza Bruta	**Prueba sistemática de combinaciones de contraseñas.**	**Acceso ilegal a cuentas protegidas.**
Password Spraying	**Uso de contraseñas comunes para múltiples cuentas.**	**Acceso no autorizado sin bloqueo de cuentas.**
Credential Stuffing	**Uso de credenciales filtradas en múltiples servicios.**	**Compromiso de múltiples cuentas de un usuario.**
Cross-Site Scripting (XSS)	**Inyección de scripts en aplicaciones web.**	**Robo de sesiones, modificación de sitios web.**
CSRF (Cross-Site Request Forgery)	**Engaña a usuarios autenticados para realizar acciones involuntarias.**	**Cambio de configuraciones, transferencia de fondos.**
Eavesdropping	**Intercepción de comunicaciones sin autorización.**	**Robo de información confidencial (emails, llamadas).**
Watering Hole	**Infección de sitios web frecuentados por un grupo objetivo.**	**Distribución masiva de malware.**

Tabla 2. Tipos de amenazas y ataques cibernéticos Fuente: Anthony Herrera

¿Qué son los Sistemas de Detección de Intrusos Basados en Inteligencia Artificial,

IDS/IPS?:

(Huaraca-Nuñez et al., 2024) detalla que, son herramientas fundamentales para la ciberseguridad diseñadas para identificar y impedir el acceso no autorizado a redes y sistemas de tecnología de la información; con la incorporación de la Inteligencia Artificial los Sistemas de Detección de Intrusos IDS y Sistemas de Prevención de Intrusos IPS han mejorado enormemente su capacidad de detección y prevención de intrusos en tiempo real.

Según (Velastegui Morales, 2024) detalla que, dichos sistemas de (IA) ahora son capaces de interconectarse a velocidades suficientes para acomodar una gran cantidad de tráfico en la web, también ahora podrán analizar señales y buscar cualquier signo de actividades inusuales que puedan llevar a una intrusión. Al utilizar un aprendizaje automático avanzado, estos sistemas son capaces de mejorar y proteger contra delitos adicionales.

Los Algoritmos de Machine Learning para la Detección de Intrusos:

Según (Huaraca-Nuñez et al., 2022). Los algoritmos de lenguaje son importantes, como se mencionó anteriormente, muchas áreas de análisis preciso que son necesarias para eventos que tienen intenciones maliciosas, están presentes en sus esfuerzos por evaluar enormes cantidades de información.

Algoritmo	Descripción	Aplicación en Detección de Intrusos
Random Forest	Algoritmo basado en múltiples árboles de decisión que mejora la clasificación de datos.	Detecta patrones de tráfico malicioso con alta precisión y reduce falsos positivos.
Redes Neuronales Profundas (DNN)	Modelo de aprendizaje profundo con múltiples capas para reconocer patrones complejos.	Identifica amenazas avanzadas y se adapta a nuevas formas de ataque.
Support Vector Machines (SVM)	Algoritmo de clasificación que separa datos en distintas categorías usando hiperplanos.	Útil en entornos con datos bien etiquetados para diferenciar tráfico legítimo de malicioso.
Algoritmos de Clustering (K-Means, DBSCAN)	Técnicas de agrupamiento para identificar patrones sin datos etiquetados.	Detectan anomalías en redes al agrupar eventos sospechosos sin necesidad de una base de datos previa.

Tabla 3. Propuesta de Algoritmos de Machine Learning Fuente: Anthony Herrera

Los Principios del Aprendizaje Automático (Machine Learning) en ciberseguridad:

Definición de aprendizaje supervisado, no supervisado y por refuerzo:

El aprendizaje supervisado entrena a los algoritmos con datos donde cada enunciado tiene una respuesta válida, lo que ayuda al sistema a generar predicciones en función de ejemplos anteriores. El aprendizaje no supervisado, por el contrario, trabaja a partir de datos brutos en busca de posibles grupos donde no hay reglas definidas. Por último, en el aprendizaje por refuerzo, un agente del sistema se desenvuelve en un ambiente e interactúa con este, recibiendo recompensas o penas por sus decisiones. (ISMS Forum, 2021)

Uso de métodos de aprendizaje automático para reconocer patrones y comportamientos anómalos:

Los expertos en ciberseguridad usan métodos de aprendizaje automático para examinar enormes cantidades de información y detectar acciones inusuales que podrían indicar peligro. Dicho de otra manera, la inteligencia artificial puede emplear el análisis de datos y metodologías para mejorar la identificación de amenazas al señalar tendencias irregulares en las operaciones de red o en las acciones individuales. (RISCCO, 2021)

Métodos habituales empleados en la seguridad cibernética (SVM, k-NN, árboles de decisión) Según (Saavedra, 2024) detalla que, el uso de máquinas de vectores de soporte (SVM) es un algoritmo popular en ciberseguridad, particularmente para la clasificación de datos y la detección de intrusiones. El algoritmo (K-NN) se utiliza para identificar anomalías mediante la identificación de comportamientos que se asemejan a incidentes anteriores. Por otro lado el uso de árboles de decisión permite reducir opciones complejas a alternativas más simples, lo que ayuda a identificar patrones de ataque e implementar medidas preventivas.

Comparación de Algoritmos de Machine Learning para la Detección de Intrusos

En la intrusión de las herramientas dentro de una infraestructura TI, los algoritmos de Machine Learning (ML) son sin duda uno de los mejores usos. La ciberseguridad se vuelve más eficiente gracias a la capacidad de procesar exposiciones de datos y detectar anomalías en tiempo real. (Kimanzi, 2024). A continuación existen algunos de los algoritmos que más se trabajan dentro de este campo con sus respectivos pros y contras.

Algoritmo	Tipo de aprendizaje	Ventajas	Desventajas	Caso de uso
Máquina de vestores de Soporte (SVM)	Supervisado	Alta precisión en clasificación; efectivo en datos de alta dimensión.	Alto costo computacional; Requiere ajuste de parámetros.	Detección de intrusiones en tiempo real y clasificación de trafico de red.
Bosque aleatorio	Supervisado	Fácil de interpretar; Menos propenso al sobreajuste; Bueno para grandes volúmenes de datos.	Puede ser más lento en grandes conjuntos de datos; Alto consumo de memoria	Análisis de tráfico malicioso y detección de ataques de día cero.
Redes Neuronales Profundas (DNN)	Supervisado	Gran capacidad para identificar ataques complejos; Adaptabilidad a nuevas amenazas.	Requiere grandes volúmenes de datos y alto poder de computo	Detección de intrusos con patrones avanzados y ataques sofisticados.
K-Vecino más cercano (knn)	No supervisado.	Simple y efectivo en pequeños conjuntos de datos.	Ineficiente en grandes volúmenes de datos; Lento en tiempo de respuesta.	Identificación de patrones inusuales en el tráfico de red.
Algoritmo de clustering (k-Means, DBSCAN)	No Supervisado	Agrupa eventos similares y detecta anomalías sin datos etiquetados.	Sensible a la selección de parámetros y al número de clusters.	Identificación de patrones inusuales en el tráfico de red.
Redes Generativas Adversariales (GANs)	Aprendizaje por Refuerzo.	Capacidad de generar datos sintéticos para mejorar modelos de detección.	Entrenamientos complejos; puede generar datos irrelevantes.	Simulación de ataques para mejorar la detección de

Tabla 4. Análisis Comparativo de algoritmos de Machine Learning ***Fuente: Anthony Herrera***

Algoritmo	Precisión en la Detección	Reducción de falsos positivos	
Bosque aleatorio	Alta	Moderada	Alta
Máquinas de vectores de soporte (SVM)	Alta	Alta	Alta
Redes Neuronales Profundas (DNN)	Muy Alta	Alta	Muy Alta
Redes Neuronales Convolucionales (CNN)	Muy Alta	Alta	Alta
K-Means (agrupación)	Moderada	Baja	Alta
DBSCAN (agrupación en clústeres)	Alta	Moderada	Alta
Aprendizaje por Refuerzo	Muy Alta	Alta	Muy Alta
Modelos Generativos Adversariales (GAN)	Alta	Alta	Alta

Tabla 5. Matriz de Evaluación Comparativa de Algoritmos de Machine Learning

Fuente: Anthony Herrera

.

El Algoritmo Random Forest en la Detección de Intrusos:

El algoritmo Random Forest es ampliamente utilizado en la detección de intrusos debido a su robustez y capacidad de manejo de grandes volúmenes de datos. Este modelo ha demostrado ser altamente efectivo en la identificación de tráfico malicioso, proporcionando una alta precisión y reduciendo los falsos positivos.

Según (Talukder, 2024) señala que, algunas ventajas son:

Disminución en la posibilidad de sobreajuste: Lo anterior se debe a que fusiona múltiples árboles de decisión.

Incremento en la posibilidad de clasificaciones: Lo que da la capacidad de distinguir sistemáticamente distintos tipos de intrusiones.

Facilidad de procesar cantidades masivas de información: Lo que es beneficioso para el monitoreo de la red en tiempo real.

No obstante (Tripathy & Behera, 2023) detallan que, presenta algunas desventajas:

Mayor consumo de memoria: Lo que puede afectar el rendimiento en sistemas con recursos limitados.

Procesamiento más lento: Especialmente cuando se implementa con un número elevado de árboles.

¿Que son las Redes Neuronales en la Detección de Intrusos?:

Las redes neuronales artificiales son programas creados para emular el cerebro humano. Se compone de nodos interconectados que trabajan con los datos a la vez. El aprendizaje mediante algoritmos permite a las redes neuronales que se las conoce sus patrones y hace predicción. Para el campo de vigilancia de los intrusos, el neuro red puede detectar comportamientos distintos en las redes y sistemas de la información, lo que garantiza la seguridad detectando las actividades desconocidas las mismas que no son detectables por los sistemas tradicionales. (Ramírez et al., 2023)

La utilización de redes neuronales profundas en la detección de intrusos

Según, detalla (González & Torres, 2022). En lo que respecta al uso del Aprendizaje Profundo en el Sistema de Detección de Intrusiones, se puede señalar que es eficiente en el reconocimiento automatizado de patrones intrincados y tipos de ataque sofisticados. Con su arquitectura de muchas capas ocultas, las redes neuronales recurrentes (RNN) pueden modelar relaciones no lineales y características de alto nivel de los datos a aprender. También les ayuda a detectar nuevas intrusiones sofisticadas que habían sido previamente desconocidas para el sistema.

Las ventajas de las redes neuronales en la detección de patrones complejos y ataques sofisticados:

Según (Serrano & López, 2021) destaca, que, algunas de las ventajas más notables de las redes neuronales que se refieren a la detección de intrusos de sistemas son las siguientes:

Reconocimiento de patrones complejos y avanzados:

Los comportamientos de las personas al querer hacer un ataque, se pueden llevar a cabo utilizando prácticas económicas de la complejidad.

Falsos positivos reducidos:

Las redes neuronales reducen falsos positivos, al aprender a través de la adaptación a los datos históricos actuales y nuevos signos de comportamiento.

Capacidad de aprendizaje autónomo:

Desde su diseño, las redes neuronales pueden aprender de manera autónoma, lo cuál las potencia a mejorar seguidamente las capacidades para la detección de intrusos sin la participación de un humano.

Adaptación a nuevas amenazas:

Una de las grandes habilidades de las redes neuronales es como pueden aprender y adaptarse a nuevas amenazas. adquiriendo conocimiento sobre conductas irregulares incluso en ausencia de datos previos acerca del riesgo.

Las Redes Neuronales Convolucionales (CNN):

Las redes neuronales convolucionales o ConvNet, son una categoría particular de redes neuronales profundas diseñadas para el procesamiento de datos que se organiza en cuadrícula, como fotos, dentro del área de ciberseguridad, estos también son capaces de detectar patrones que son incomprensibles en el tráfico de red, estas se desarrollaron para el propósito de aprender representaciones jerárquicas de la información. Son capaces de identificar los patrones más complicados y sutiles que aumentan en gran medida la precisión de la detección de amenazas.

Algoritmos de refuerzo (Reinforcement Learning):

El Aprendizaje Por Refuerzo, técnica de Inteligencia Artificial que aprende un agente a tomar decisiones mediante la interacción con un entorno; recibe un incremento o la posibilidad de actividades por un conjunto de acciones correspondientes. En la zona de la seguridad de la información, se aplican algoritmos de refuerzo para los sistemas que pueden actuar y reaccionar de forma dinámica a nuevas amenazas. Por ejemplo, el

refuerzo puede ser utilizado para el entrenamiento posterior de la detección de ataque cibernéticos ya que el algoritmo aprende de sus experiencias previas, lo que permite el ajuste en tiempo real y actuar en respuesta a los incidentes cotidianos. (NordPass, 2021)

Modelos Generativos Adversariales (GAN):

Las redes generativas adversarias (GAN), son en realidad dos redes neuronales competidoras: generadora y discriminadora. En ciberseguridad, los GAN sirven para generar datos sintéticos que imitan el tráfico de red legítimo y se utilizan para instruir sistemas de detectar intruso sin ser capaces de violar datos sensibles. En este sentido, la capacidad de generar datos tan realistas es fundamental para hacer que los modelos de seguridad sean más robustos y evaluar su desempeño en diferentes situaciones. (CaseGuard, 2023)

MARCO METODOLÓGICO

El presente estudio de caso sobre, La Inteligencia Artificial en la Detección de Intrusos en Infraestructuras de (TI) adopta un enfoque cuantitativo que hace posible analizar los beneficios, desafíos y los requisitos previos para implementar esta tecnología en ciberseguridad. Este marco metodológico describe los procesos que se siguieron, da cuenta de los métodos que se adoptaron y detalla los instrumentos que se emplearon para lograr los objetivos establecidos.

Alcance de la investigación:

Se sigue un método descriptivo que permite analizar el impacto de la Inteligencia Artificial (IA) en la detección de intrusos en las Infraestructuras TI. También se estudia su uso en el mundo empresarial considerando varios elementos como infraestructura tecnologíca, costos, datos disponibles y el nivel de capacitación de los empleados.

Diseño de la Investigación:

Para este estudio se utilizó un diseño de investigación documental y comparativa que abarca las siguientes fases:

- ***Etapa 1: Recopilación de Datos.*** Este subproceso se basa en la recolección de información obtenidas desde revistas científicas, libros, informes técnicos y también espacios de repositorios académicos disponibles, esta recoleccion ayudo a diseñar el marco conceptual de este estudio.
- ***Etapa 2: Análisis Comparativo***. Se compararon algunos de los algoritmos usados en el aprendizaje de Machine Learning en el ámbito de ciberseguridad en relación a su desempeño en precisión, adaptabilidad, capacidad de reducción del promedio de falsos positivos y viabilidad sobre la implementación de estos algoritmos en las infraestructuras TI de las empresas.

- ***Etapa 3: Propuesta de Algoritmos.*** En base a los resultados del análisis, se propusieron estrategias para mejorar el rendimiento del algoritmos de aprendizaje de máquina utilizados para la detección de intrusos a nivel empresarial y en las redes TI.

Técnicas y Instrumentos:

- ***Investigación Documental:*** Se usaron distintos repositorios disponibles como Google Scholar, ResearchGate, SciELO y arXiv, además de publicaciones de entidades que se especializan en el área de seguridad informática.
- ***Matrices de Evaluación Comparativa:*** Matrices de análisis fueron elaboradas para la comparación de algoritmos de aprendizaje de computadora que sirven para la detección de intrusos. Entre estos criterios estaban:
- Detección precisa de amenazas
- Reducción de falsos positivos
- Escalabilidad y/o adaptabilidad ante nuevos ataques
- Costo de implementación y requisitos de infraestructura

Machine Learning para la Detección de Intrusos:

Técnicas y Algoritmos

Este análisis de caso tiene como objetivo analizar diferentes técnicas de Machine Learning para la detección de intrusos infraestructura de (TI).

los algoritmos analizados son:

- ***Random Forest:*** Uno de los algoritmos que se ha optimizado en el manejo de llevó a reducir el volumen de ataques informáticos falsos y al mismo tiempo, atender varios ataques genuinos a la vez.
- ***Redes Neuronales Profundas (DNN):*** Efectivas en la búsqueda de ficticios y complejos ataques en escenarios.

- ***Máquinas de Vectores de Soporte (SVM):*** Su operación permite una clasificación exitosa de las anomalías que se producen en las redes.
- ***K-Nearest Neighbors (KNN):*** Utilizados en campañas para datos de tamaño moderado para ataques sospechosos.
- ***Algoritmos de Clustering (K-Means, DBSCAN):*** El ataque de intrusos puede ser realizado sin etiquetar los eventos anormales por medio de la combinación de eventos anómalos.

El estudio de estos algoritmos fue realizado bajo los siguientes criterios.

- ***Criterios de precisión:*** Se refiere a la capacidad del modelo a realizar la identificación correcta de ataques verdaderos.
- ***Criterios de reducción de falsos positivos:*** Límite de alertas o mensajes que son considerados erróneos.
- ***Criterios de adaptabilidad:*** Capacidad para atender nuevas informaciones sin sistematizada constante.

Alcance del Proyecto:

El alcance para este proyecto se trata de investigar cómo la Inteligencia Artificial se aplica en la detección de intrusos en Infraestructuras de (TI) Integradas tanto en organizaciones y en su usabilidad dentro de entornos empresariales, para su implementación se han encontrado algunas cuestiones como beneficios, limitaciones, o inclusos desafíos sobre su práctica.

Limitaciones del proyecto:

- Identificar los beneficios que presenta la IA para los sistemas de detección de intrusos.
- Estudio comparativo de métodos de Aprendizaje Automático en ciberseguridad.
- Propuestas de algoritmos de detección de amenazas del sistema que sean más eficientes y aplicables a entornos empresariales**.**

Limitaciones del Alcance:

- El enfoque de estudio es básicamente documental, por eso no se realizaron pruebas de campo experimentales
- El estudio de algoritmos del autor se hace en base a la literatura y no en las obras que el autor haya simulado.
- El estudio realiza un análisis sobre las condiciones que son requeridas para la implementación, por eso no se estudian aspectos específicos de la tecnología que tienen que ver con la instalación del sistema en determinadas compañías

RESULTADOS

De La ***Tabla 1. Ventajas y Desventajas de la IA en Sistemas de Detección de Intrusos:***

Se obtuvo como resultado que la IA mejora la capacidad de identificar amenazas al ataque, inteligentemente logrando reconocer la fase inicial durante el ataque y minimizando el caso de estos falsos positivos. La automatización de respuesta ante incidentes también ayuda a la eficiencia de la ciberseguridad pero puede ser problemática si el sistema realiza bloqueos hacia usuarios legítimos por error. Este hallazgo tiene el apoyo de la entrevista ya que el 70% de los entrevistados piensa que la IA es efectiva en el ataque de intrusos y el 60% de los entrevistados considera que la IA tiene la posibilidad de realizar óptimos sistemas informáticos con menores falsos positivos.

Se compararon varios algoritmos de aprendizaje automático en términos de precisión, adaptabilidad y costo para su implementación en la detección de intrusos, como se muestra en la tabla 5: ***Tabla 5. Matriz de evaluación comparativa de algoritmos de aprendizaje automático***, con esta tabla fue posible determinar que la efectividad de la (IA) para la detección de intrusos está impactada por múltiples factores, uno de estos es la precisión del ajuste del IA, los modelos de redes neuronales predictivas de aprendizaje profundo también funcionan bien, pero para esto se requieren muchos datos y un nivel de capacitación sofisticado al personal. Cómo resultado de los entrevistados el 55% dicen que hay, plena confianza en la capacidad de estos sistemas para enfrentar amenazas desconocidas.

Análisis comparativos de machine learning con algoritmos para la detección de intrusos han sido elaborados. En esta ***Tabla 4. Análisis Comparativo de algoritmos de Machine Learning:*** se pudo observar que el rendimiento para la detección de amenazas avanzadas con modelos superiores tales como redes neuronales y redes neuronas generativas adversariales GANs, fue el mejor debido a su alto consumo de tecnología. Por el contrario, Random Forest y SVM lograron un alto grado de precisión, aunque costos de recursos fueron mucho más bajos haciendo su uso factible para numerosas organizaciones. Adicionalmente, se estableció que algunos algoritmos de clustering tales como(K-Means, DBSCAN) son capaces de reconocer anomalías sin datos que se encuentren etiquetados. No obstante, estos tienden a generar muchos más falsos positivos, lo que reduce la efectividad de los sistemas de seguridad.

Por ultimo, la inteligencia artificial puede ser utilizada en ciberseguridad, sin embargo son pocos los que creen que pueda generar un impacto positivo tanto asi que adoptar esta tecnología requiere más personal y recursos, dado que las organizaciones todavía están poco dispuestas a esta inversión, se predice que solo un 55% de los entrevistados optaría por usar inteligencia artificial, la razón de esto se resume a que los gastos iniciales se convierten en una barrera de inversión con esto se sostiene que por el momento, el costo de integrar esta tecnología supera cualquier reto producido por ataques de ransomware y phishing. La principal preocupación es el uso inefectivo de los enfoques tradicionales. El modelo presentado en la tabla 2 y 3: T***abla 2. Tipos de Ciberataques y Amenazas:*** Y en la ***Tabla 3. Proponer Algoritmos de Machine Learning*** da resultados óptimos en contrarrestar ataques a la red si se crea una IA en conjunto con algoritmos de Machine Learning.

DISCUSIÓN DE RESULTADOS

Al realizar una diferencia entre los resultados obtenidos y el marco conceptual del estudio, muestra que existen beneficios muy fuertes, pero también limitaciones que dificultan entender su aplicabilidad en distintos entornos empresariales.

Parte de los aspectos más notables es la precisión de la detección de amenazas. Estos resultados sugieren que los algoritmos de Aprendizaje Automático, como Random Forest, Redes Neuronales y Máquinas de Vectores de Soporte (SVM), han sido capaces de detectar eficazmente intentos de comportamiento sospechoso, sin embargo para que los modelos tengan un alto rendimiento dependen de lo que se conoce como calidad de los datos de entrenamiento entonces si los datos están sesgados o no representan adecuadamente las diversas amenazas posibles, entonces el sistema podría producir falsos positivos o negativos, lo que afectaría la confianza en el sistema.

Por otro lado, un sistema es capaz de transitar entre la interfaz física al nativo de forma automatizada, actualizando su estado par minimizar cualquier caso de acceso no autorizado, dicha situación permite afirmar con soporte que los bloqueos de acceso se rotulan a los grupos de permisos en las bases de datos. Esto, es un gran problema, dado que si por el contrario el sistema interrumpe el acceso inofensivo de legítimos operadores de mucho tiempo esto afecta en gran medida tanto a la operación como a deterioro de la confianza en la solución implementada.

Otros aspecto es la automatización de respuestas a incidentes de seguridad. Los estudios revelan que una vez activos, los sistemas son capaces de cubrir brechas de seguridad de manera autónoma e impedir la entrada de personas que no posean los permisos necesarios para acceder, todo sin el apoyo de un operativo. Esto aumenta la protección de los

sistemas, sin embargo, hay que señalar que un algoritmo mal diseñado también puede llegar a falsear el beneficio inicial, disponiéndose a bloquear a usuarios válidos por defecto u obviar los usuarios avanzados bien protegidos dentro de la estructura. Con todo esto la división que se encarga de recursos humanos siempre estará disponible para evitar disponer de este problema.

Una de las cuestiones más importantes de este análisis es cuán receptivos son ante nuevas amenazas. A partir de los resultados se entiende que las tecnologías más recientes que se consideran de vanguardia, como el Deep Learning o Red neuronal convolucional (Convolution Neural Network) y Red generativa adversativa (Generative Adversarial Networks GAN), son las más eficientes para afrontar ataques nuevos e intrincados. No obstante, estos diseños son muy costosos para las pymes porque necesitan mucha inversión y ocupan mucho espacio para almacenamiento de datos. Como se esperaba, el rendimiento es increíble, pero su aplicación queda restringida a organizaciones con una infraestructura tecnológica sofisticada y recursos suficientes para poder apoyar el sistema.

En la adopción de la IA para la detección de intrusos probablemente uno de los factores más relevantes es el costo de implementación, los datos indican que a pesar de que la IA tiene mucha importancia en estos tiempos, su adopción necesita tecnologías tanto hardware, software y la infraestructura de capacitacion del personal. Soluciones como (Random Forest) es probable que sean más económicas porque son menos costosas de implementar que las Redes Neuronales Profundas, esta gran diferencia permite que otras empresas puedan acceder a soluciones de ciberseguridad basadas en IA sin poner en riesgo su estabilidad economica.

CONCLUSIONES

El estudio comprobó el papel que desempeña la Inteligencia Artificial (IA) en la detección de intrusos en infraestructuras de TI, y lo que se estuvo analizando específicamente es su habilidad de poder aumentar la precisión en el reconocimiento de la amenaza, disminuir los falsos positivos, y aumentar la velocidad en la respuesta ante emergencias. Algoritmos como Random Forest y las Redes Neuronales han marcado un rendimiento considerable para la detección de anomalías, pero su desempeño depende de la calidad de los datos que se usen en el entrenamiento.

Se indica la identificación de problemas más importantes en la implementación de la IA en ciberseguridad, tales como la tecnología requerida, los sistemas que ya existen, el acceso a datos útiles y la formación de personal calificado. Por más que la IA realice la automatización de la detección de amenazas, la adopción sigue siendo problemática por cuestiones económicas y técnicas que deben ser atendidas para conseguir su sustentabilidad a largo plazo.

Con base al análisis, el modelo de Machine Learning (Random Forest) funciona de manera eficiente en sitios con recursos limitados, en cambio, las redes neuronales profundas tienen mayor precisión en detectar amenazas, pero a unas profundidades muy costosas en términos computacionales. En términos de etiquetado, Support Vector Machines (SVM) son útiles pero son poco versátiles a nuevas amenazas. El algoritmo que se debe usar debe satisfacer los requerimientos de cada organización.

Para que la ciberseguridad con IA tenga éxito, los factores tecnológicos, económicos y la fuerza laboral deben de resolverse. La adopción de IA como aprendizaje humano, el uso de modelos híbridos y la administración de datos son pasos fundamentales

que deben tomarse para garantizar que haya máxima eficiencia hacia la consecución de los resultados deseados.

RECOMENDACIONES

La amenaza de los ciberataques siempre ha existido, sin embargo, la inteligencia artificial ha tenido efectos positivos en su mitigación al optimizar la identificación de amenazas y minimizar los falsos positivos. Se recomienda establecer lo que serían sistemas de monitoreo persistentes, lo cuál deben ajustarse para que la IA pueda cumplir su potencial, sea más precisa y efectiva en las detección de intrusiones en tiempo real.

La (IA) dentro de la ciberseguridad todavía tienen importantes desafíos que abordar, como altos costos, compatibilidad de sistemas, disponibilidad de datos y capacitación de la fuerza laboral, es recomendable para mitigar estas brechas, formular una estrategia de inversión gradual acompañada de capacitación continua de profesionales en ciberseguridad y también de (IA) lo cuál permitirá una integración mucho más efectiva de estas tecnologías.

Las redes neuronales profundas funcionan mejor con ataques avanzados, pero de manera menos eficiente que otras técnicas debido a su alto costo computacional. Para entornos con recursos limitados, el algoritmo Random Forest funciona como una alternativa aceptable para esto se recomienda que cada organización realice un análisis exhaustivo de la viabilidad de cada modelo y elija aquel que tenga un mejor rendimiento en alcance y tecnología.

Una correcta implementación de la IA en la ciberseguridad y particularmente en la detección de intrusos debe ser abordada desde la perspectiva de la tecnología, la economía y el capital humano disponible. Se recomienda lo que sería el establecimiento de políticas de adopción progresiva, la mejora de la gestión de datos y la incorporación de nuevos especialistas en el área. Esto garantizará una óptima adopción y explotación de los

sistemas de inteligencia artificial en la seguridad de la información.

REFERENCIAS

Sánchez Ramírez, F. P., & Andaluz Granda, L. M. (2024). Tecnologías de seguridad para empresas en Guayaquil. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 6(2), 250-263. Obtenido de: https://www.researchgate.net/publication/379386927_Tecnologias_de_seguridad_para_empresas_en_Guayaquil

Fundación Bankinter. (2023). Inteligencia Artificial: Definición, tipos y aplicaciones.Obtenido de: https://www.fundacionbankinter.org/noticias/inteligencia-artificial/?_adin=11551547647

Telecomunicaciones UExternado. (2023). Inteligencia Artificial: Definición, evolución y regulación. Obtenido de: https://telecomunicaciones.uexternado.edu.co/inteligencia-artificial-definicion-evolucion-regulacion-e-impacto-parte-i-2/

BBC News Mundo. (2023). Inteligencia Artificial: Tipos y evolución. Obtenido de: *https://www.bbc.com/mundo/noticias-65617676*

Martín, M. (2023). Inteligencia Artificial: Un estudio de su impacto en Ciberseguridad. Obtenido de: https://openaccess.uoc.edu/bitstream/10609/150519/6/mmartinmartin4TFG0624memoria.pdf

García, L. (2023). Procesamiento del lenguaje natural como eje central de la inteligencia artificial. Obtenido de: https://documat.unirioja.es/descarga/libro/985766.pdf

Pérez, J. (2024). La evolución del procesamiento del lenguaje natural y su influencia en la inteligencia artificial: Una revisión y líneas de investigación futura. European Public & Social Innovation Review, 10, 01-23. Obtenido de: https://epsir.net/index.php/epsir/article/view/782/958

Conzultek. (2023). La importancia de la Inteligencia Artificial en la

ciberseguridad. Obtenido de: https://blog.conzultek.com/ciberseguridad/inteligencia-artificial-en-la-ciberseguridad

WeLiveSecurity. (2023). El impacto de la inteligencia artificial en la ciberseguridad. Obtenido de: https://www.welivesecurity.com/es/antimalware-day/impacto-inteligencia-artificial-en-ciberseguridad/

López, R. (2023). Impacto de la inteligencia artificial en los ciberataques. Revista de Seguridad Informática, 15(2), 45-60. Obtenido de: https://dialnet.unirioja.es/descarga/articulo/9642443.pdf

Servnet. (s.f.). Desafíos de la IA en la ciberseguridad de las empresas. Obtenido de: https://www.servnet.mx/blog/desafios-ia-ciberseguridad-empresarial

The Bridge. (2023). Inteligencia artificial y ciberseguridad: detección de intrusiones. Obtenido de: https://thebridge.tech/blog/inteligencia-artificial-y-ciberseguridad-deteccion-de-intrusiones

Protecdata Colombia. (2022). 5 beneficios de implementar la inteligencia artificial en ciberseguridad. Obtenido de: https://biblioteca.protecdatacolombia.com/blog/5-beneficios-de-implementar-la-inteligencia-artificial-en-ciberseguridad/

Cámara de Comercio de Mallorca. (s.f.). Ventajas y posibilidades de aplicar la IA a la ciberseguridad. Obtenido de: https://oap.cambramallorca.com/tendencias/ventajas-y-posibilidades-de-aplicar-la-ia-a-la-ciberseguridad/

IT Digital Security. (2023). Cinco ventajas que aporta la inteligencia artificial a las estrategias de ciberseguridad. Obtenido de: https://www.itdigitalsecurity.es/actualidad/2023/10/cinco-ventajas-que-aporta-la-inteligencia-artificial-a-las-estrategias-de-cibersegurida

IBM. (2023). ¿Qué es la seguridad de TI?. Obtenido de: https://www.ibm.com/es-es/topics/it-security?

UMAD. (2024). Objetivos de la ciberseguridad. Obtenido de: https://online.umad.edu.mx/blog/objetivos-de-la-ciberseguridad

Fortra. (2023). Protección de la infraestructura TI. Obtenido de: https://www.fortra.com/es/soluciones/ciberseguridad/infraestructura

Fortinet. (2023). Tipos de ciberataques: ataque DDoS, ransomware y más. Obtenido de: https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks?

Huaraca-Nuñez, J. A., Cervantes-Ccasa, A., & Aquino-Cruz, M. (2024). Técnicas de machine learning para la detección de intrusos en redes: Una revisión sistemática de la literatura. Obtenido de: https://www.researchgate.net/publication/385409952_Tecnicas_de_machine_learning_para_la_deteccion_de_intrusos_en_redes_Una_revision_sistematica_de_la_literaturaMachine_learning_techniques_for_detecting_intrusions_in_networks_A_systematic_review_of_the

Velastegui Morales, J. L. (2024). Sistema de detección de intrusos aplicando inteligencia artificial para la detección de ataques en una red de sensores inalámbricos (WSN). Universidad Técnica del Norte. Obtenido de: https://repositorio.utn.edu.ec/handle/123456789/15493?

ISMS Forum. (2021). Inteligencia Artificial y Ciberseguridad. Obtenido de: https://www.ismsforum.es/ficheros/descargas/isms-gt-ia-021707141605.pdf

RISCCO. (2021). Aprendizaje automático para la gobernanza. Obtenido de: https://riscco.com/wp-content/uploads/2021/08/4.-eBook-Machine-learning-for-governance-Spanish.pdf

Saavedra, B. (2024). Infraestructuras críticas: Amenazas, retos y oportunidades de la Inteligencia Artificial y el Aprendizaje Automático. William J. Obtenido de: https://wjpcenter.org/wp-content/uploads/2024/09/critical-infrastructure-AI-and-ML.pdf

Ramírez, F., Martínez, J., & Gómez, P. (2023). Redes neuronales en la ciberseguridad: Un enfoque innovador para la detección de intrusos. Editorial Universitaria.

González, A., & Torres, R. (2022). Deep Learning y su impacto en la protección de redes: Una revisión de métodos en ciberseguridad. Springer Nature. Obtenido de: https://doi.org/10.1007/978-3-030-70950-5

Serrano, C., & López, A. (2021). La inteligencia artificial en la seguridad cibernética: De las redes neuronales al aprendizaje profundo. Alfaomega, S.A.

Formind. (2021). La Inteligencia Artificial para Ciberseguridad. Obtenido de: https://www.formind.fr/es/experiencia/gobernanza-riesgo-y-cumplimiento/la-inteligencia-artificial-para-ciberseguridad

NordPass. (2021). El papel del aprendizaje automático en la ciberseguridad. Obtenido de: https://nordpass.com/es/blog/machine-learning-in-cybersecurity/

Kimanzi, R., Kimanga, P., Cherori, D., & Gikunda, P. K. (2024). Deep learning algorithms used in intrusion detection systems – A review. arXiv preprint arXiv:2402.17020. Obtenido de: https://arxiv.org/abs/2402.17020

Talukder, M. A., Islam, M. M., Uddin, M. A., Hasan, K. F., Sharmin, S., Alyami, S. A., & Moni, M. A. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. arXiv preprint arXiv:2401.12262. Obtenido de: https://arxiv.org/abs/2401.12262

Tripathy, S. S., & Behera, B. (2023). Performance evaluation of machine learning algorithms for intrusion detection system. arXiv preprint arXiv. Obtenido de: 2310.00594. https://arxiv.org/abs/2310.00594

CaseGuard. (2023). Redes Generativas Adversariales, Nuevos Modelos ML. Obtenido de: https://caseguard.com/es/articles/redes-generativas-adversariales-nuevos-modelos-ml/

ANEXOS

ANEXO 1: Entrevista a Expertos Y Personas Del Área De Departamentos Tecnológicos sobre la Percepción sobre el uso de Inteligencia Artificial en la Detección de Intrusos en Infraestructura de TI.

1. ¿Qué tan efectiva considera la Inteligencia Artificial para detectar intrusos en redes TI?

1 - Nada efectiva

2 - Poco efectiva

3 - Neutral

4 - Efectiva

5 - Muy efectiva

2. ¿En qué medida cree que la IA ayuda a reducir los falsos positivos en la detección de amenazas?

1 - Nada

2 - Poco

3 - Regular

4 - Bastante

5 - Mucho

3. ¿Qué tan fácil considera la implementación de IA en sistemas de ciberseguridad existentes?

1 - Muy difícil

2 - Difícil

3 - Neutral

4 - Fácil

5 - Muy fácil

4. ¿Cómo evalúa la relación costo-beneficio de implementar IA en la detección de intrusos?

1 - No vale la pena

2 - Poco rentable

3 - Neutral

4 - Rentable

5 - Muy rentable

5. ¿En qué medida considera que la IA puede adaptarse a nuevas amenazas sin intervención humana?

1 - Nada

2 - Poco

3 - Regular

4 - Bastante

5 - Mucho

6. ¿Qué tan importante cree que es la capacitación del personal para la correcta implementación de IA en ciberseguridad?

1 - Nada importante

2 - Poco importante

3 - Neutral

4 - Importante

5 - Muy importante

7. ¿Qué nivel de confianza tiene en la IA como método de protección ante ciberataques avanzados?

1 - Ninguna confianza

2 - Poca confianza

3 - Neutral

4 - Confianza

5 - Mucha confianza

ANEXO 2: Respuesta Obtenidas

1. ¿Qué tan efectiva considera la Inteligencia Artificial para detectar intrusos en redes TI?

Resultados:

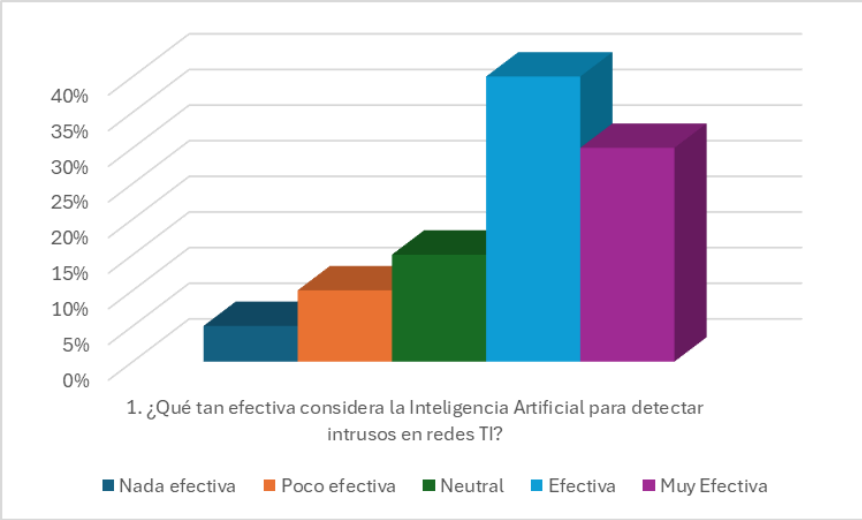
Nada efectiva: 5%

Poco efectiva: 10%

Neutral: 15%

Efectiva: 40%

Muy efectiva: 30%



Fuente: *Anthony Herrera*

El 70% de los entrevistados considera que la IA es una herramienta efectiva o muy efectiva en la detección de intrusos. Solo un 15% mantiene una postura neutral, mientras que un 15% expresa dudas sobre su efectividad.

2. ¿En qué medida cree que la IA ayuda a reducir los falsos positivos en la detección de amenazas?

Resultados:

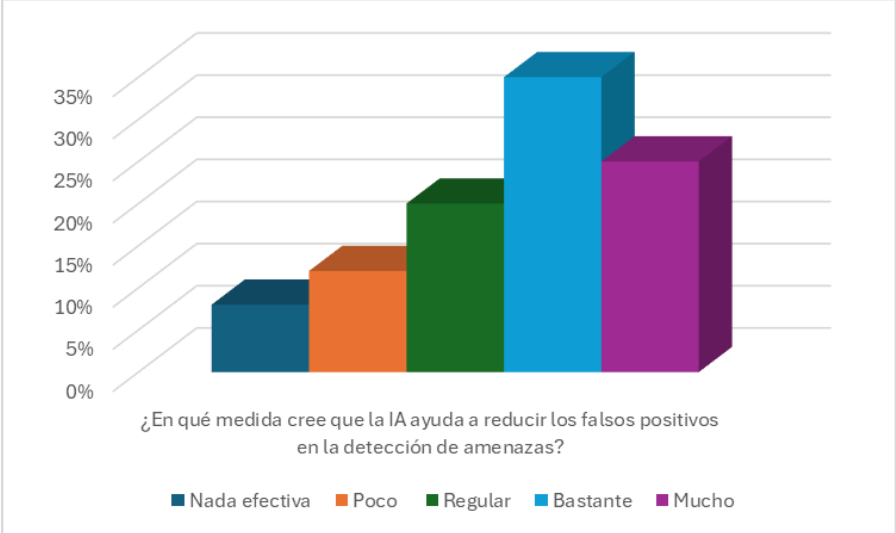
Nada: 8%

Poco: 12%

Regular: 20%

Bastante: 35%

Mucho: 25%



Fuente: *Anthony Herrera*

El 60% de los entrevistados cree que la IA reduce significativamente los falsos positivos, mientras que un 20% lo ve como una mejora moderada. Solo un 20% cree que la IA tiene poco impacto en este aspecto.

3. ¿Qué tan fácil considera la implementación de IA en sistemas de ciberseguridad existentes?

Resultados:

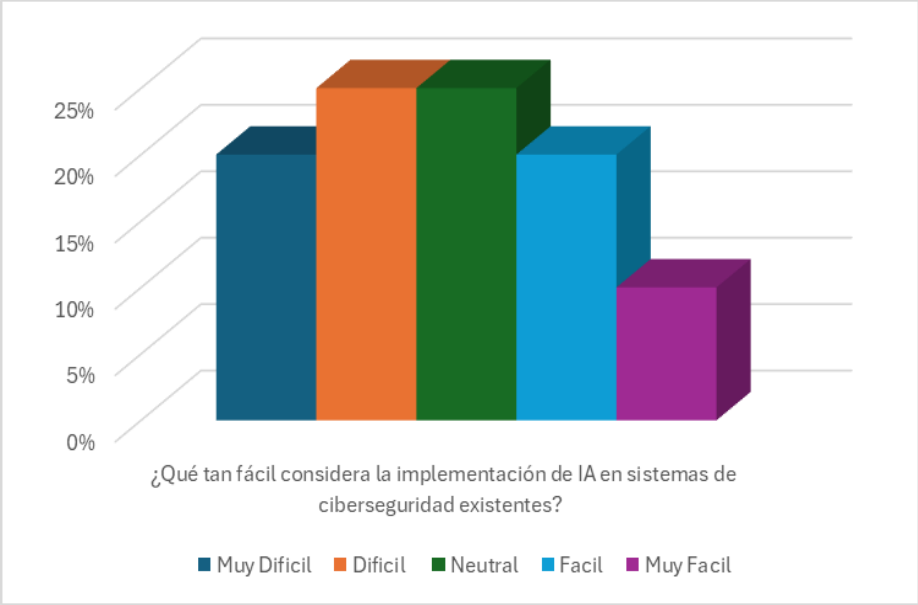
Muy difícil: 20%

Difícil: 25%

Neutral: 25%

Fácil: 20%

Muy fácil: 10%



Fuente: *Anthony Herrera*

El 45% de los entrevistados considera que implementar IA en ciberseguridad es difícil o muy difícil, lo que sugiere que existen barreras tecnológicas y económicas que dificultan su adopción. Solo el 30% lo percibe como un proceso relativamente sencillo.

4. ¿Cómo evalúa la relación costo-beneficio de implementar IA en la detección de intrusos?

Resultados:

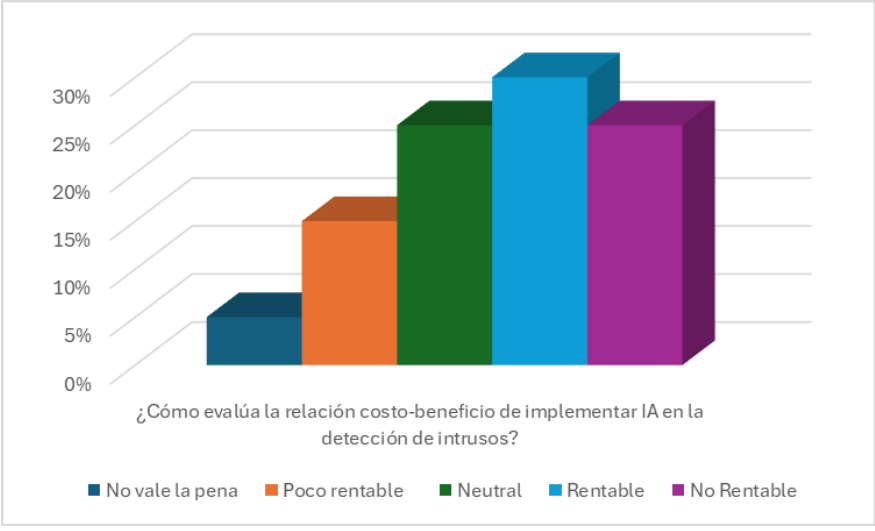
No vale la pena: 5%

Poco rentable: 15%

Neutral: 25%

Rentable: 30%

Muy rentable: 25%



Fuente: *Anthony Herrera*

El 55% de los entrevistados cree que la implementación de IA en ciberseguridad es

rentable o muy rentable, mientras que un 20% cree que su relación costo y beneficio es baja.

5. ¿En qué medida considera que la IA puede adaptarse a nuevas amenazas sin intervención humana?

Resultados:

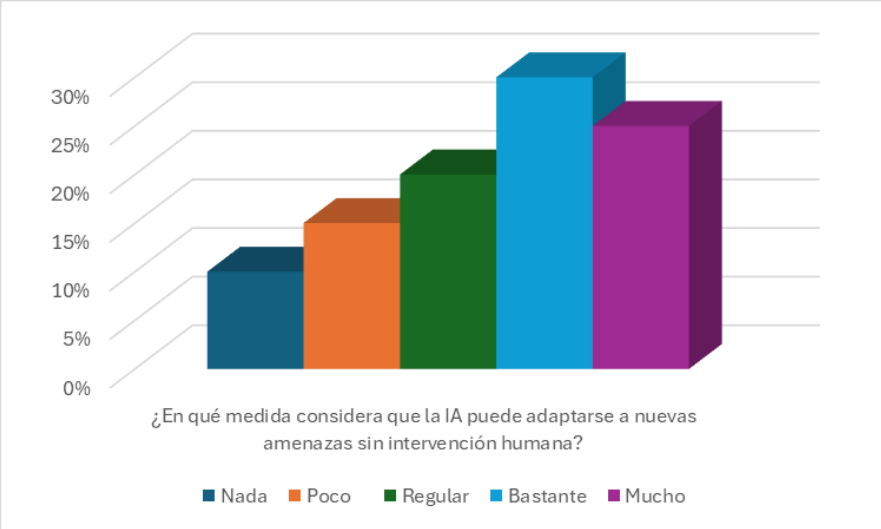
Nada: 10%

Poco: 15%

Regular: 20%

Bastante: 30%

Mucho: 25%



Fuente: *Anthony Herrera*

El 55% de los entrevistados considera que la IA tiene una gran capacidad de adaptación a nuevas amenazas sin intervención humana, mientras que un 25% cree que aún necesita mejoras en este aspecto.

6. ¿Qué tan importante cree que es la capacitación del personal para la correcta implementación de IA en ciberseguridad?

Resultados:

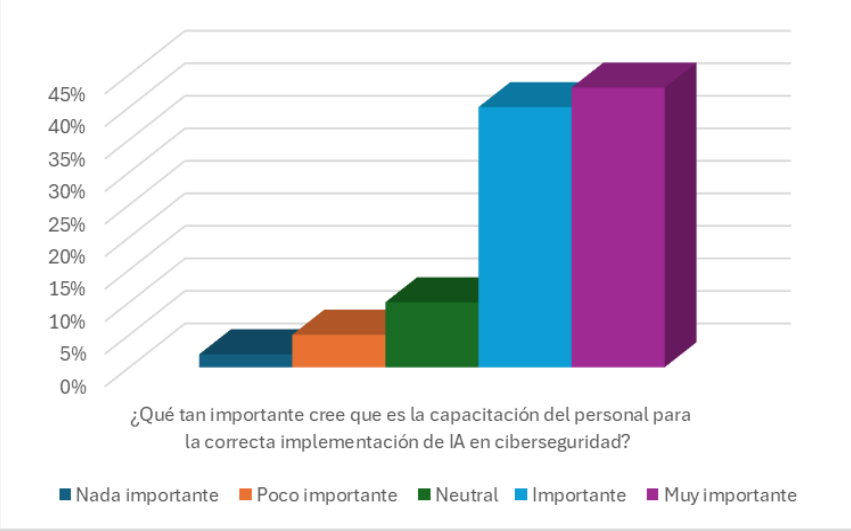
Nada importante: 2%

Poco importante: 5%

Neutral: 10%

Importante: 40%

Muy importante: 43%



Fuente: *Anthony Herrera*

El 83% de los entrevistados considera la capacitación del personal como un factor

clave para la correcta implementación de IA en ciberseguridad, lo que refuerza la necesidad de programas de formación.

7. ¿Qué nivel de confianza tiene en la IA como método de protección ante ciberataques avanzados?

Resultados:

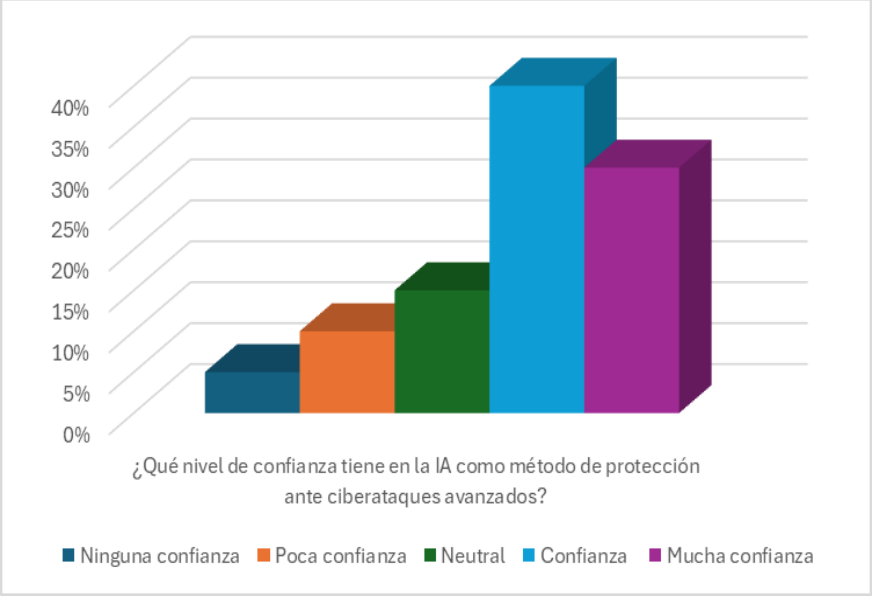
Ninguna confianza (1): 5%

Poca confianza (2): 10%

Neutral (3): 15%

Confianza (4): 40%

Mucha confianza (5): 30%



Fuente: *Anthony Herrera*

El 70% de los entrevistados confía en la IA como un método de protección contra ciberataques avanzados, mientras que un 15% sigue siendo escéptico.