UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO 2024

PROYECTO DE INVESTIGACIÓN INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

"Impacto de la inteligencia artificial en la ciberseguridad empresarial: un análisis crítico de la evolución de amenazas y medidas preventivas"

ESTUDIANTE:

Noralma Nathaly Acosta Cortez

TUTOR:

Ing. Alfonso Agama Chico

Año 2024

Dedicatoria

Con gran emoción dedico este proyecto de investigación a mis padres que con esfuerzo me han acompañado durante todo este proceso académico, a mis tutores que han compartido sus conocimientos en cada clase impartida, a mis amigos y seres queridos quienes han brindado su apoyo cuando he querido arrojar la toalla.

Por último, a aquellos que encuentren utilidad y significado en estas palabras, espero que este proyecto de investigación inspire y contribuya al progreso del conocimiento en nuestro campo de estudio.

Con todo mi aprecio,

Nathaly Acosta.

Agradecimiento

En primer lugar, agradezco a Dios por permitirme llegar hasta el final de este proyecto de investigación.

Gracias a todas las personas que me han apoyado de alguna u otro forma en todo este proceso académico, a mi familia, que ha sido el pilar fundamental para no rendirme, a mis amigos que me dieron palabras de aliento siempre que sentía que ya no podía más, gracias por esa motivación.

A mi tutor, que estuvo pendiente de todo el proceso investigativo, le agradezco por su orientación experta, sus valiosos consejos y su constante apoyo.

A todos ustedes, mi más sincero agradecimiento.

Resumen

Este estudio está a la vanguardia de la investigación que tiene como objetivo comprender y evaluar el impacto real de la inteligencia artificial en la evolución de las ciberamenazas y la efectividad de las medidas preventivas en el entorno empresarial regional. Para optimizar las operaciones y los servicios, las empresas utilizan tecnología de inteligencia artificial para mejorar la eficiencia y la competitividad. Sin embargo, estas innovaciones también han introducido nuevas vulnerabilidades, ya que las amenazas cibernéticas cada vez más sofisticadas han aprovechado las capacidades de la IA para superar las defensas tradicionales, planteando interrogantes sobre la seguridad de los activos digitales y la totalidad de los datos.

Particularmente relevante es el contexto de aceleración de la digitalización y la implementación de procesos en línea, especialmente impulsado por las restricciones impuestas durante la pandemia de COVID-19 en los últimos años. Si bien esto ha permitido a muchas organizaciones continuar con sus operaciones, también ha aumentado la interconexión y dependencia de sistemas informáticos, abriendo espacios de vulnerabilidad que los actores malintencionados están aprovechando.

Los hallazgos de esta investigación permitirán identificar brechas entre la evolución de los ciberataques y las capacidades preventivas actuales de las empresas. Se formularán recomendaciones concretas para mejorar los mecanismos de predicción, detección y respuesta ante esta nueva generación de amenazas computacionales. Abordar esta problemática contribuirá a comprender y gestionar de manera más adecuada los desafíos y oportunidades que presenta la IA para la seguridad informática empresarial.

Desde una metodología exploratoria y descriptiva, esta investigación se propone examinar de manera integral una temática de creciente interés, considerando resultados iniciales, evolución esperada y áreas de mejora en el campo emergente de la IA en la ciberseguridad empresarial. Mediante la integración de técnicas de exploración conceptual y descripción sistemática de evidencias, busca proporcionar conocimientos útiles para la toma de decisiones informada tanto por la comunidad académica como por las empresas.

Palabras clave: ciberseguridad, inteligencia artificial, amenazas cibernéticas, protección de activos, tecnologías emergentes.

Abstract

This study is at the forefront of research that aims to understand and evaluate the real impact of artificial intelligence on the evolution of cyber threats and the effectiveness of preventive measures in the regional business environment. To optimize operations and services, companies use artificial intelligence technology to improve efficiency and competitiveness. But these innovations also create new vulnerabilities as increasingly sophisticated cyber threats use artificial intelligence capabilities to overcome traditional defenses, challenging the security of digital assets and entire data.

This is particularly important in an environment where digitalization and online processes are accelerating, especially given the restrictions imposed in recent years during the Covid-19 pandemic. While this has allowed many organizations to continue their operations, it has also increased the interconnection and dependence on computer systems, opening spaces of vulnerability that malicious actors are exploiting.

The findings of this research will allow us to identify gaps between the evolution of cyberattacks and the current preventive capabilities of companies. Concrete recommendations will be made to improve prediction, detection and response mechanisms for this new generation of computational threats. Addressing this issue will help to better understand and manage the challenges and opportunities that AI presents for enterprise IT security.

Using an exploratory and descriptive methodology, this research aims to comprehensively examine a topic of growing interest, considering initial results, expected evolution and areas of improvement in the emerging field of AI in business cybersecurity. By integrating conceptual exploration techniques and systematic description of evidence, it seeks to provide useful knowledge for informed decision making by both the academic community and companies.

Keywords: cybersecurity, artificial intelligence, cyber threats, asset protection, emerging technologies

Índice general

Índice de figuras

Índice de tablas

INTRODUCCIÓN

En la era digital actual, el entorno empresarial se enfrenta a un desafío ineludible: la ciberseguridad en un mundo impulsado por la inteligencia artificial. En un intento de las empresas para optimizar sus operaciones y servicios han adoptado tecnología de IA, permitiéndoles ser más eficientes y competitivas. No obstante, estas innovaciones también han traído consigo nuevas vulnerabilidades, las amenazas cibernéticas cada vez más sofisticadas han evolucionado han aprovechado las capacidades de la inteligencia artificial IA superando las defensas tradicionales de las organizaciones, poniendo en duda la protección de activos digitales y la integridad de la información.

Este estudio se posiciona en la vanguardia de la investigación, buscando entender y evaluar el impacto real de la inteligencia artificial en la evolución de amenazas cibernéticas y la eficacia de las medidas de prevención en el contexto regional. Mediante un estudio cuantitativo y cualitativo, se identificarán las modificaciones en las modalidades de amenazas cibernéticas apoyadas en IA que han afectado a empresas de la región. Asimismo, se evaluará que tan efectivas han resultado las adaptaciones en las medidas de seguridad con IA que han implementado para protegerse.

En particular, el uso masificado de internet e implementación de procesos en línea se aceleró significativamente debido a las restricciones impuestas durante la pandemia de COVID-19 en los últimos años. Gracias a Internet muchas personas han podido continuar con su trabajo y muchas organizaciones públicas y privadas han decidido utilizar este método.

Sin embargo, la creciente interconexión y dependencia de sistemas informáticos también ha abierto espacios de vulnerabilidad que están siendo aprovechados por actores maliciosos. El interés de la sociedad por parte de la ciberseguridad ha crecido durante los últimos años debido a la magnitud de pérdidas económicas causadas por ciberataques en programas gubernamentales y empresas multinacionales.

Los hallazgos permitirán determinar brechas existentes entre la evolución de los ciberataques y las capacidades preventivas actuales de las empresas, formulando recomendaciones concretas para mejorar los mecanismos de predicción, detección y respuesta ante esta nueva generación de amenazas computacionales. Abordar esta problemática apoyará a comprender y gestionar de manera más adecuada los desafíos y oportunidades que presenta la IA para la seguridad informática corporativa.

CAPÍTULO I. PROBLEMA

1.1. Marco contextual

1.1.1. Contexto internacional

A nivel mundial, la ciberseguridad se ha convertido en una preocupación importante a medida que las ciberamenazas provenientes de tecnologías avanzadas de inteligencia artificial continúan apareciendo. Los gobiernos, las organizaciones internacionales y las empresas multinacionales han reconocido la necesidad de fortalecer sus estrategias de ciberseguridad para proteger los sistemas de infraestructura crítica y proteger los datos confidenciales en un entorno de interconexión global.

El aumento de los ciberataques en todo el mundo revela importancia de utilizar métodos de IA para responder a las amenazas que evolucionan día a día. Para hacer frente a estas situaciones transfronterizas, la cooperación entre países y el uso de estándares internacionales se tornan importantes (J. Cano, 2023).

1.1.2. Contexto nacional

Ecuador ha visto un aumento en el cibercrimen a medida que se acelera la digitalización de su infraestructura y economía. El gobierno ecuatoriano reconoce la necesidad de fortalecer sus capacidades de ciberseguridad para proteger los activos digitales y la información confidencial. La estrategia del país apunta no sólo a reducir las amenazas tradicionales, sino también a adaptarse a la naturaleza evolutiva de las amenazas cibernéticas impulsadas por la IA.

La ley ecuatoriana incluye regulaciones de ciberseguridad que enfatizan la importancia de proteger las infraestructuras críticas y garantizar la integridad de los datos. El país enfrenta el desafío de conciliar la tecnología con la seguridad, conjunto a la necesidad de respuestas locales efectivas (Salazar Rodríguez, 2023).

1.1.3. Contexto local

A nivel local principalmente las pequeñas y medianas empresas, intentan adaptarse a las necesidades digitales y al mismo tiempo protegerse de las ciberamenazas en constante evolución. Las iniciativas en ciberseguridad están influenciadas por la dinámica del mercado y las características únicas de la región. La alianza entre los sectores público y privado se presenta como un elemento clave para promover la resiliencia cibernética en un entorno regional que presenta desafíos y oportunidades únicas.

El sector público es uno de los más riesgosos porque las inversiones son bajas. Además de utilizar soluciones tecnológicas que protegen los datos, también se deben desarrollar medidas preventivas efectivas para reducir los riesgos existentes. El vector de ataque más común en los ciberataques a las empresas es la falta de conocimiento entre los empleados, siendo estos la primera línea de alerta temprana (Pabon et al., 2023).

1.2. Situación problemática

La transformación digital requiere que las empresas integren la inteligencia artificial para mejorar los procesos y obtener una ventaja competitiva. Sin embargo, los ciberdelincuentes han utilizado las capacidades de la IA para crear nuevos tipos de malware, ransomware y programas de ataque sofisticados, causando enormes pérdidas financieras a empresas de todo el mundo. Por consiguiente la cuestión problemática sería ¿Las estrategias de seguridad actuales de las organizaciones realmente son capaces de salvaguardar sus activos ante amenazas basadas en IA?

Este tema es de suma importancia atender puesto que es necesario comprender la realidad de las medidas estratégicas de ciberseguridad en una época donde estas amenazas evolucionan a diario. El no comprender la situación puede exponer a las empresas a grandes riesgos, cómo la pérdida de datos confidenciales, interrupciones en los sistemas y daños a la reputación con costos de millones de dólares.

1.3. Planteamiento del problema

La transformación digital requiere que las empresas incorporen nuevas tecnologías, como la inteligencia artificial, para mejorar los procesos y tomar mejores decisiones. Para abordar estos desafíos las organizaciones implementan estrategias integrales de seguridad con las tecnologías emergentes, de esta manera pueden fortalecer sus defensas y mitigar proactivamente posibles vulnerabilidades y amenazas; asegurando un entorno digital a la vanguardia y seguro (de Azambuja et al., 2023).

En particular, se ha observado un significativo aumento de los ciberataques dirigidos al sector empresarial, aprovechando las capacidades de la IA para generar malware más sofisticado y evasivo. Diversos reportes señalan que las pérdidas económicas por estos incidentes se cuentan en millones de dólares anualmente (European Union Agency for Cybersecurity, 2023).

Por lo tanto, el problema de investigación radica en la necesidad de realizar un análisis crítico y actualizado sobre la evolución de amenazas cibernéticas aprovechando la IA, así como evaluar la capacidad de respuesta de las empresas ante este desafío emergente de seguridad. Los hallazgos permitirán identificar brechas en las estrategias de prevención e impulsar mejoras al respecto.

1.4. Delimitación de la investigación

Se analizará el periodo durante el año 2023, para evaluar el impacto reciente de la incorporación de técnicas de IA tanto en tácticas de ataque como en defensas cibernéticas de empresas de la región a través de fuentes como estadísticas institucionales y reportes de ciberseguridad.

La investigación servirá para reconocer la eficacia de las estrategias de ciberseguridad en la protección de sus activos contra el aumento de amenazas sofisticadas que trazan las herramientas de IA. Se dará prioridad a revisar y analizar las herramientas de IA mayormente utilizadas, los tipos de ciberamenazas encontradas y los ajustes realizados en las políticas de seguridad. La investigación no abordará aspectos específicos de las políticas gubernamentales en ciberseguridad ni evaluará estrategias implementadas por organizaciones gubernamentales.

1.5. Justificación

La creciente complejidad y diversificación de las amenazas cibernéticas plantean una urgencia en comprender y mejorar las estrategias de ciberseguridad empresarial. Esta investigación sobre la implementación de la inteligencia artificial en dicho contexto busca proporcionar una comprensión crítica y detallada sobre estos vectores de ataque. Los beneficios derivados incluyen el reconocimiento de los ataques por las personas, la optimización de las medidas preventivas, la reducción de vulnerabilidades y, en última instancia, la fortificación de la seguridad cibernética empresarial.

Debido a la variedad de tipos de ataque se encuentra necesario un estudio para detallar estos diferentes tipos de ataques y como han ido evolucionando con la revolución de la IA. En la actual era digital resulta fundamental que las personas tengan un mínimo del conocimiento sobre seguridad informática para evitar ser víctimas o poner en riesgo los activos de la empresa para la que trabajan.

Del análisis final de este trabajo de investigación se desarrollará un compendio de buenas prácticas a tener en cuenta, que recopilen consejos, métodos y herramientas de soporte para evitar ser víctimas de algún vector de ataque cibernético.

1.6. Objetivos

1.6.1. Objetivo general

Evaluar el impacto de la IA en la evolución de amenazas cibernéticas como en la eficacia de las medidas de prevención para las empresas.

1.6.2. Objetivos específicos

- Analizar cómo el uso de la IA ha contribuido tanto en ataques como defensas en el campo de la ciberseguridad.
- Investigar casos reales y analizar las experiencias de cómo la IA ha afectado las medidas de seguridad ante amenazas cibernéticas en las organizaciones.
- Identificar tendencias emergentes que enfrentan empresa en el ámbito de la ciberseguridad y establecer recomendaciones puntuales.

CAPÍTULO II. MARCO TEÓRICO

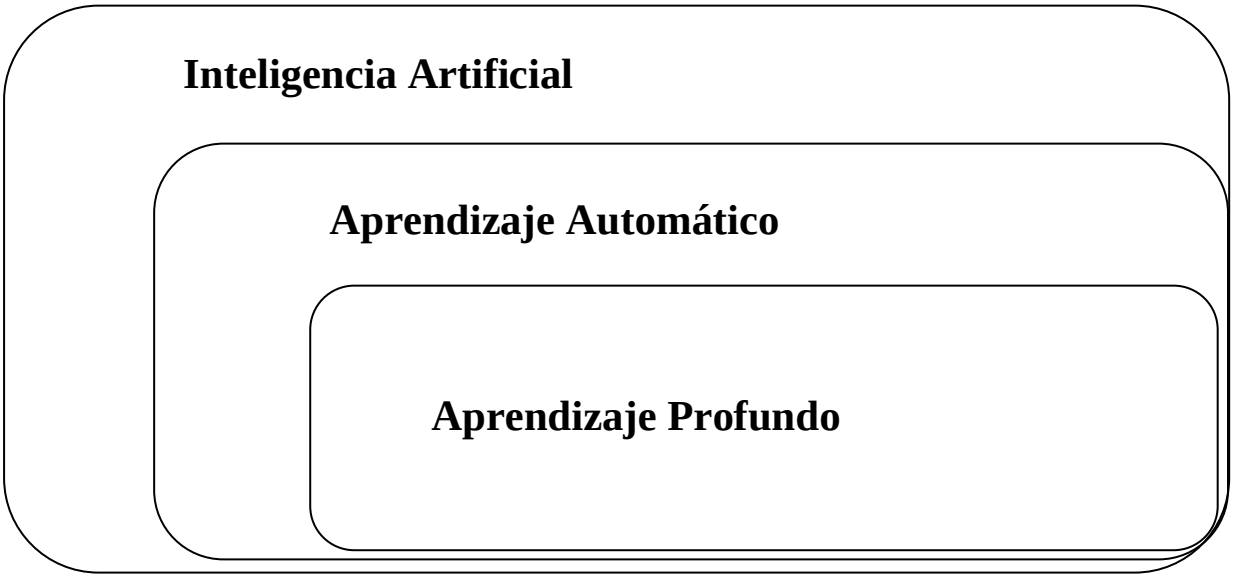
2.1. Marco conceptual

2.1.1. Implementación de la Inteligencia Artificial en la ciberseguridad empresarial

2.1.1.1. Conceptos y tipos de IA

La inteligencia artificial es un área de la informática que busca crear modelos que puedan resolver problemas que normalmente requieren del razonamiento humano. En ciberseguridad, esta tecnología se puede utilizar para analizar grandes cantidades de información para encontrar datos sospechosos y alertar a los encargados en ciberseguridad sobre las posibles amenazas (Ortiz Centurion et al., 2023).

Figura 1. Áreas de la IA.



Fuente: Elaboración propia.

El aprendizaje automático implica la capacidad de crear modelos informáticos para que a través de una serie de datos pueda de cierta manera aprender y tomar decisiones sin la intervención de una persona. Este modelo de aprendizaje se puede utilizar en el campo de la ciberseguridad para analizar grandes cantidades de datos para detectar procedimientos sospechosos y detectar amenazas, entre los principales tipos se encuentran (Wiafe et al., 2020):

- **Aprendizaje Supervisado:** modelo que utiliza datos previamente conocidos para identificar patrones.
- **Aprendizaje no supervisado:** modelo para reconocer patrones irregulares sin necesidad de tener información previa.
- **Aprendizaje por refuerzo:** modelo para resolver problemas a base de un proceso de ensayo y error hasta mejorar los resultados.

El aprendizaje profundo es una subcategoría del aprendizaje automático que utiliza un modelo de redes neuronales para simular la estructura del cerebro humano. En el ámbito de la ciberseguridad, el aprendizaje ofrece capacidades avanzadas de análisis y detección. Algunos de estos modelos son (Wiafe et al., 2020):

- **Redes Neuronales Convolucionales (CNN):** ideal para la detección de malware basado en el comportamiento analizando los patrones reconocidos.

- **Redes Neuronales Recurrentes (RNN):** ideal para analizar flujos de datos para identificar amenazas en tiempo real y sus comportamientos.

Estos tipos de IA proporcionan capacidades analíticas avanzadas, permitiendo a los sistemas defenderse proactivamente contra ataques cibernéticos.

2.1.1.2. Herramientas y algoritmos de Inteligencia Artificial aplicados a la ciberseguridad

Los profesionales de ciberseguridad deben trabajar con grandes cantidades de datos y la IA constituye, por tanto, una ayuda importante para el desarrollo del trabajo porque permite aprender a trabajar sin intervención humana gracias a los modelos de aprendizaje expuestos anteriormente, la tabla 1 define algunos de los algoritmos empleados en ciberseguridad de acuerdo con el tipo.

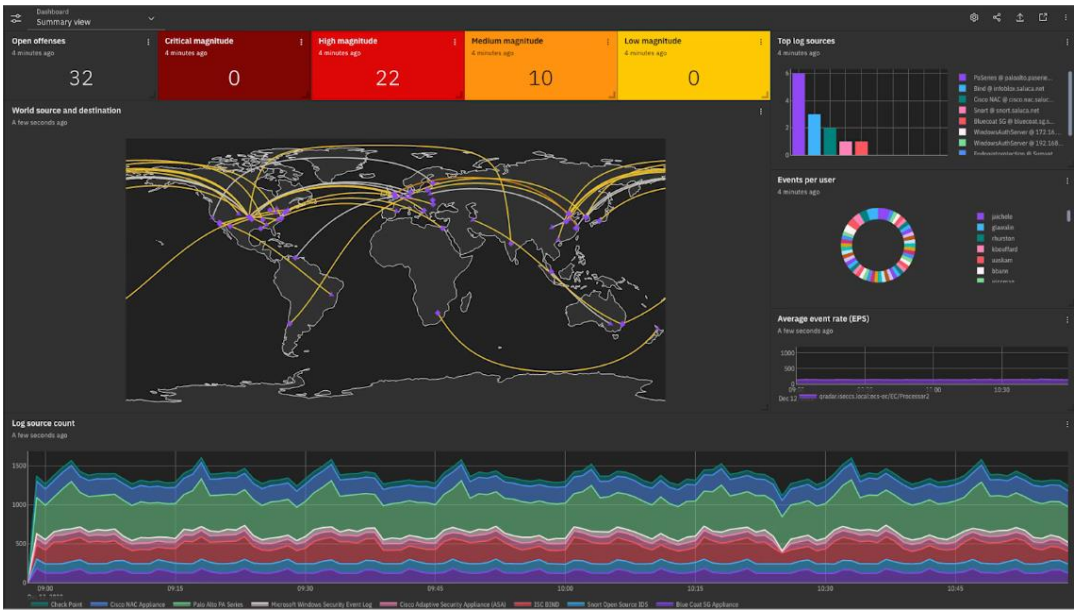
Tabla 1. *Algoritmos de IA en Ciberseguridad.*

Machine Learning	Deep Learning
Algoritmos de clasificación: estos son utilizados para categorizar datos y determinar si son benignos o maliciosos, apoyando la toma de decisiones en tiempo real	**Redes neuronales artificiales:** estos algoritmos sirven para reconocer patrones complejos y realizar análisis predictivos.
Algoritmos de clustering: En grandes conjuntos de datos identifican patrones extraños , por lo que ayudan en la facilitación de la detección de amenazas.	**Procesamiento del lenguaje natural:** Esto ayuda a analizar e interpretar el lenguaje utilizado para posibles amenazas en comunicaciones escritas como el phishing.

También existen algunas herramientas de software que ya utilizan estos algoritmos de IA, ejemplos son:

- **IBM QRadar**, este programa utiliza Machine Learning para analizar datos de eventos de seguridad, identificando patrones y comportamientos sospechosos.

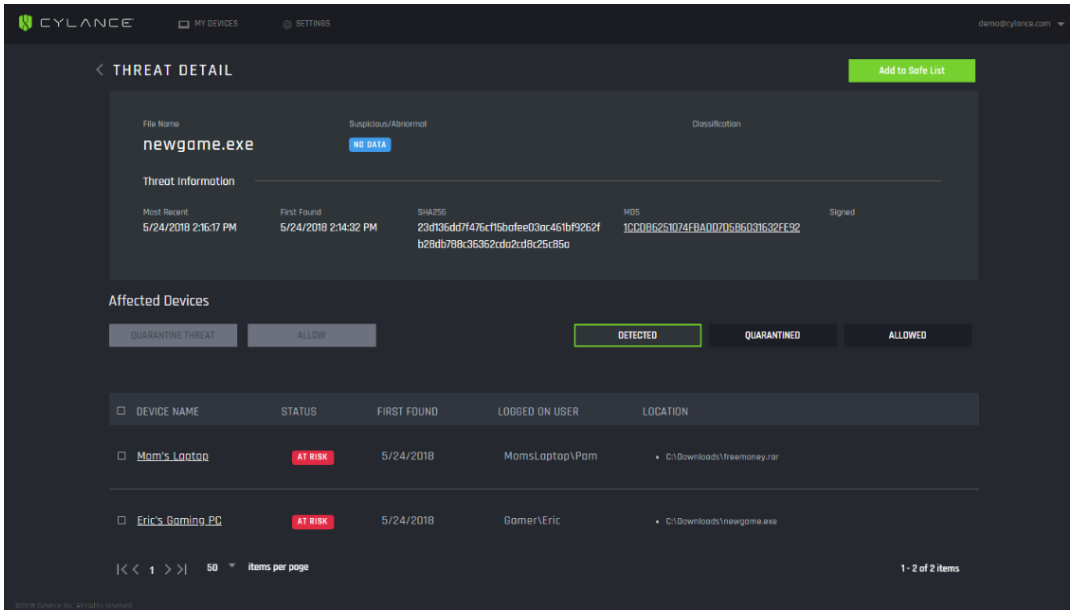
Figura 2. Interfaz IBM QRadar.



Fuente: https://www.ibm.com/es-es/products/qradar-siem

- **CylancePROTECT**, este programa en cambio aprovecha algoritmos de Deep Learning para analizar el comportamiento de archivos y aplicaciones con procederes dudosos.

Figura 3. CyclancePRTECT Interfaz.



Fuente: https://es.several.com/antivirus/cylance

La aplicación de herramientas y algoritmos de IA en ciberseguridad ofrece una defensa más dinámica contra las amenazas cibernéticas. Estas soluciones no solo automatizan la detección, sino que también permiten una respuesta más rápida y adaptativa (Khoei et al., s. f.).

2.1.2. Evolución de las amenazas cibernéticas

2.1.2.1. Tipos de amenazas cibernéticas y sus características

Comprender los distintos tipos de amenazas y sus características es esencial para desarrollar estrategias efectivas de ciberseguridad, la tabla 2 expone algunos de las amenazas con sus características:

Tabla 2. *Amenazas cibernéticas y sus características.*

Amenaza	Características
Malware	• Software malicioso diseñado para dañar, acceder o tomar control de sistemas. • Incluye virus, gusanos, troyanos y ransomware. • Propagación a través de descargas, correos electrónicos y dispositivos extraíbles.
Phishing	• Engañan a los usuarios y los inducen a revelar datos sensibles. • Usan correos electrónicos y sitios web falsos. • Se pretende conseguir información financiera de la víctima.
Denegación de servicio DDoS	• Sobrecargan sistemas o redes, impidiendo el acceso legítimo. • Suelen bots o múltiples dispositivos para realizar el ataque. • El objetivo es inhabilitar servicios en la red.
Amenaza interna	• Provienen de empleados, contratistas u otros dentro de la organización. • Acciones accidentales o intencionadas que comprometen la seguridad.
Ingeniería social	• Manipulación psicológica para obtener información confidencial. • Puede implicar engaños, pretextos o suplantación de identidad. • Aprovecha la confianza y la falta de conciencia de seguridad.

La variedad de amenazas cibernéticas demanda enfoques holísticos en la ciberseguridad y la comprensión de las características específicas de cada tipo de amenaza es crucial para implementar medidas preventivas y de respuesta efectivas (Pereira, 2020).

2.1.2.2. Dinámica de cambio en las amenazas cibernéticas

La dinámica constante del entorno cibernético requiere una comprensión constante de las amenazas en evolución. Es un riesgo en evolución que se desarrolla de maneras inesperadas en el contexto de un ecosistema digital caracterizado por una alta interacción y acoplamiento. En este sentido, la gestión no puede responder a una práctica estándar basada en riesgos conocidos y defensas tradicionales (Ray, 2022).

La adaptación tecnológica como la incorporación de nuevas tecnologías y los avances en IA y automatización, amplía superficies de ataque y complejiza los métodos de defensa lo que impacta en la detección y respuesta inmediata ante ataques más sigilosos y persistentes. Además, la colaboración y grupos especializados de ciberatacantes indica una mayor sofisticación y

diversificación de las amenazas con la constante de nuevas variantes de malware, la falta de conciencia de los usuarios y nuevas técnicas de evasión exigen actualizaciones frecuentes en los sistemas de detección de amenazas. (J. Cano, 2023)

La capacidad de la IA para procesar enormes cantidades de datos, detectar patrones y generar nuevo contenido está permitiendo crear malware más avanzado con un importante componente de autoaprendizaje. Esto se traduce en amenazas más dinámicas, adaptativas y evasivas que dificultan su detección por parte de las soluciones de ciberseguridad tradicionales.

Monitorizar de cerca estos cambios en las modalidades de amenazas apoyadas en IA resulta indispensable para que las medidas de protección puedan estar al día con las innovadoras capacidades ofensivas y mitigar proactivamente su impacto. (J. Cano, 2023)

2.1.3. Medidas preventivas en ciberseguridad para empresas

2.1.3.1. Estrategias tradicionales de ciberseguridad

Las estrategias tradicionales de ciberseguridad han sido fundamentales para proteger los sistemas informáticos durante décadas. Estos enfoques, aunque sólidos, enfrentan el desafío constante de adaptarse a la evolución de las amenazas cibernéticas.

Figura 4. Prácticas tradicionales en ciberseguridad.

Fuente: https://www.bureauveritas.es/magazine/10-consejos-para-la-ciberseguridad-en-la-empresa

El mantenimiento regular de versiones de software, sistemas operativos y dispositivos, así como la incorporación de mejoras de seguridad proporcionadas por actualizaciones era y sigue siendo una estrategia para mitigación de vulnerabilidades conocidas y protección contra fallos de seguridad. Además de la integración de múltiples capas de seguridad incluyendo firewalls, sistemas de detección y prevención de intrusiones, protección de puntos finales y cifrado de datos dificultaba la penetración de los atacantes (Ortiz Centurion et al., 2023).

El análisis periódico de las posibles vulnerabilidades y riesgos de seguridad de acuerdo con las políticas de seguridad de la empresa es otra estrategia funcional para la mitigación de amenazas, así como el cumplimiento normativo. La formación de los trabajadores de la empresa es una buena medida de seguridad ya que fortalece la primera línea de defensa contra los ciberatacantes y es una responsabilidad por parte de los individuos dentro de la organización.

Otra estrategia es desarrollar o gestionar planes de emergencia de manera que se minimice el impacto en el tiempo de recuperación ante algún ataque. Además de implementar soluciones de respaldo regulares para garantizar la continuidad del negocio tras pérdidas de datos. También es aconsejable la a asociación con profesionales especializados en ciberseguridad para obtener servicios y soluciones personalizadas mejorando así la postura de seguridad de la empresa (Ortiz Centurion et al., 2023).

2.1.3.2. Adaptando estrategias de seguridad con IA en las empresas

La adaptación de modelos de IA dentro del plan de seguridad permite a las empresas adentrarse en la innovación frente a las amenazas en evolución. Estos algoritmos de IA pueden incorporarse en las estrategias de seguridad para predecir, detectar y reducir las amenazas de las siguientes maneras (Rodríguez, 2020):

- **Detección proactiva:** El desarrollo de modelos inteligentes posibilita el reconocimiento de patrones conductuales y la detección de amenazas antes de que se transformen en riesgos concretos

- **Análisis predictivo:** A través de modelos de aprendizaje avanzado se anticipan potenciales vectores de ataque.

- **Respuesta automatizada:** Implementar respuestas automáticas configuradas con plantillas adaptables, diseñadas para contrarrestar amenazas en tiempo real.

- **Adaptación continua:** Los sistemas de inteligencia artificial aprenden ininterrumpidamente y se adaptan a las nuevas amenazas, ajustando automáticamente las políticas de seguridad de su empresa.

Al integrar los métodos de IA en la estrategia general de ciberseguridad de su organización, puede asegurarse de que sus defensas están orientadas con los últimos métodos para combatir las amenazas actuales y en desarrollo.

En este contexto, resulta crucial que los altos mandos de la organización implementes estrategias y procesos que permitan gestionar y controlar las amenazas cibernéticas de una manera más estructuradas, así como también desarrollar y mantener los recursos necesarios para afrontar y superar situaciones adversas que puedan surgir a causa de estas. Una buena inversión en ciberseguridad da como resultado en una mayor tranquilidad a nivel corporativo al permitir a la empresa gestionar las operaciones y alcanzar sus objetivos incluso después de un ataque exitoso. (J. J. Cano, 2021)

De esta manera la IA es una herramienta con alto potencial para robustecer la postura de ciberseguridad organizacional, pero debe estar integrada dentro de procesos más complejos de gobernanza, gestión colaborativa del riesgo y las operaciones de seguridad. (Salazar Rodríguez, 2023)

2.2. Antecedentes investigativos

A continuación, se analizará la información de algunos trabajos realizados hasta el momento que tienen relación con el trabajo de investigación.

- **"Ciberseguridad empresarial: Ransomware y el impacto de la inteligencia artificial y la inteligencia artificial generativa." Alexis Arraz Almirall, Barcelona 2023.**

Este proyecto analiza el impacto de las herramientas de IA generativa en la ciberseguridad empresarial. Si bien la IA ha beneficiado a las estrategias de protección informática corporativas, también podría representar una amenaza al facilitar la creación de códigos maliciosos como ransomware. Para evaluar este riesgo, se realizaron pruebas en ChatGPT forzando la generación de ransomware en distintos idiomas (inglés, español, catalán, italiano), con el fin de verificar si el uso de lenguajes con menor presencia en la red o menos hablantes podría debilitar sus barreras de seguridad.

Los resultados, aunque acotados y no representativos de la seguridad integral de ChatGPT, arrojaron la efectiva obtención de código de ransomware, sugiriendo que los filtros éticos de la herramienta podrían verse más fácilmente eludidos en ciertos idiomas. Finalmente, se anexa una guía sobre el empleo responsable de tecnologías de IA generativa en el contexto empresarial, ante los riesgos revelados sobre su posible aprovechamiento para actividades maliciosas. (Almirall, 2023)

- **"La inmunización de la red: la inteligencia artificial basada en Python como bloqueo contra los ciberataques." Johnny Fernando Guerrero, José Luis Romero, Guayaquil 2023.**

Este trabajo analiza en profundidad la relación simbiótica entre ciberseguridad e inteligencia artificial destacando que pueden tanto colaborar para robustecer las defensas informáticas como ser utilizadas con fines maliciosos en ciberataques. Se conoce que esta tecnología tiene grandes ventajas a la hora de mejorar la protección de los sistemas de información, pero también hay que tener en cuenta que corre un grave peligro de que individuos malintencionados la utilicen para sus propios fines.

Hay que procurar que la implementación de la tecnología de IA en una laorganización se utilice para beneficio de la empresa. Además, se resalta la necesidad urgente de coordinación estratégica entre ciberseguridad, inteligencia artificial e innovación para crear soluciones que incorporen protección multifacética desde el diseño (Guerrero Panchana & Romero Ibarra, 2023).

- **“Inteligencia artificial en la seguridad de la información en una organización.” Cristhian Aldair Villacorta, Elvis Steve Ortiz, Alberto Carlos Mendoza de los Santos, Trujillo 2023**

El siguiente estudio se apoya en la metodología PRISMA para identificar las diversas implicaciones, tanto positivas como negativas, de la integración de la inteligencia artificial en la seguridad de la información empresarial. La pregunta principal que promueve a esta investigación es: ¿Cuál es el impacto de incorporar inteligencia artificial en los sistemas de seguridad de las empresas? Este estudio es significativo ya que destaca las ventajas potenciales, como la automatización de respuestas, la prevención de pérdida de datos y la identificación de amenazas avanzadas, así como aspectos éticos y de privacidad relacionados con la aplicación de la IA.

Sin embargo, también identifica desafíos emergentes, como el malware basado en IA y los ataques de ingeniería social mejorados, que subrayan la necesidad de una mayor privacidad y seguridad. Los hallazgos de esta investigación proporcionarán a las organizaciones una visión general de los posibles escenarios a enfrentar para proteger la información empresarial en un entorno cada vez más digitalizado y complejo. (Ortiz Centurion, et al., 2023)

- **“La inteligencia artificial en la empresa: evolución y futuro en la era digital.” Carlos Veiga Fernández, Madrid 2023**

El presente documento aborda la introducción y la implementación de la IA en el entorno empresarial y la sociedad contemporánea. A través de un análisis exhaustivo, se examina cómo estas herramientas inteligentes están transformando los fundamentos de diversos sectores económicos, explorando su aplicación en el ámbito empresarial y los desafíos que ello conlleva.

Se enfatiza la importancia de establecer un marco legal que gestione la responsabilidad derivada del uso de la inteligencia artificial en las empresas. A su vez, se analiza el abanico de posibilidades beneficiosas para los negocios en cada campo que se integre la inteligencia artificial. Estas aplicaciones son diversas y numerosas, algunos ejemplos son el procesamiento del Big Data, asistentes virtuales, chatbots, herramientas de IA generativa para contenido audiovisual, etc.

Se resalta la ciberseguridad y los riesgos asociados con estas avanzadas herramientas, se lleva a cabo un estudio sobre el uso de IA con usuarios reales. Para finalizar se hacen recomendaciones para el uso estratégico de la IA en las empresas y se esbozan algunas perspectivas próximas sobre el desarrollo de esta potente tecnología. (Veiga Fernández, 2023)

- **“Confiar en la inteligencia artificial en ciberseguridad es un arma de doble filo.” Maria Rosaria Taddeo, Tom McCutcheon, Luciano Floridi 2019**

El siguiente estudio ostenta que las aplicaciones de inteligencia artificial para tareas de ciberseguridad están atrayendo una mayor atención del sector privado y público. Las más recientes estrategias nacionales de ciberseguridad y defensa de varios gobiernos mencionan explícitamente capacidades de IA. Al mismo tiempo, están surgiendo globalmente iniciativas para definir nuevos estándares y procedimientos de certificación que promuevan la confianza de los usuarios en la IA.

Sin embargo, la confianza en la IA (tanto en aprendizaje automático como en redes neuronales) para tareas de ciberseguridad tiene dos filos: puede mejorar sustancialmente las prácticas de ciberprotección, pero también facilitar nuevas formas de ataques a las propias aplicaciones de IA, lo que puede representar graves amenazas. Sostenemos que la confianza en la IA para ciberseguridad no está garantizada y que, para reducir los riesgos de seguridad, alguna forma de control para garantizar el despliegue de una "IA confiable" es necesaria. (Taddeo et al., 2019)

2.3. Hipótesis

Se hipotetiza que la implementación efectiva de la inteligencia artificial en la ciberseguridad empresarial estará positivamente asociada con una mayor eficacia en la mitigación de amenazas cibernéticas, identificando áreas de mejora en las medidas preventivas y fortaleciendo la seguridad global de las organizaciones.

2.4. Variables

Variable independiente: Uso de IA como estrategia de ciberseguridad.

Variable dependiente: Efectividad de las medidas de seguridad.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Método de investigación

Se adoptará un enfoque inductivo para explorar la compleja relación entre la implementación de técnicas de inteligencia artificial y la evolución de amenazas cibernéticas en el ámbito empresarial. Este método se selecciona con el objetivo de profundizar desde lo particular hacia lo general, comenzando con el análisis detallado de causas y fenómenos específicos para derivar conclusiones y principios más amplios.

El método inductivo permitirá un estudio analítico y sintético de la información recopilada, iniciando con la observación y evaluación de la implementación de estrategias de ciberseguridad en las empresas, considerando herramientas específicas y medidas preventivas adoptadas. Este proceso analítico proporciona una comprensión detallada de circunstancias específicas.

A continuación, sintetiza los patrones y contextos identificados a través del análisis de casos para identificar tendencias comunes, retos recurrentes y adaptaciones exitosas que pueden extrapolarse para desarrollar principios generales aplicables a la ciberseguridad empresarial.

3.2.Modalidad de investigación

La investigación adoptará una modalidad mixta, combinando elementos tanto cuantitativos como cualitativos. Esta elección se basa en el reconocimiento de la complejidad del fenómeno estudiado, que requiere una comprensión integral desde diversas perspectivas para proporcionar una visión completa y enriquecedora.

Se hará uso de métodos cuantitativos para recopilar estadísticas relacionadas con la implementación de estrategias de ciberseguridad. El análisis de datos cuantitativos proporciona datos más cuantificables sobre la popularidad de las herramientas de IA mayor usadas, la eficacia percibida de las medidas de seguridad y otros aspectos cuantificables. Nuevamente se utilizarán métodos cualitativos para recopilar información.

El análisis de casos de estudio ayudará a recopilar experiencias, perspectivas y desafíos que enfrentan las empresas al aplicar técnicas de IA a sus procesos. La seguridad informática mediante el uso de métodos mixtos se puede lograr una comprensión integral y profunda del fenómeno en estudio. Perspectivas cuantitativas y cualitativas que aumentan la credibilidad del estudio.

3.3. Tipo de investigación

La presente investigación se enmarca dentro de un enfoque exploratorio y descriptivo en relación con la problemática de la implementación de IA en la ciberseguridad del sector empresarial.

El carácter exploratorio de este estudio busca examinar integralmente una temática de creciente interés, pero sobre la cual aún no se dispone de suficientes evidencias conclusivas respecto a su efectividad e impactos derivados. En este sentido, la investigación permitirá abordar de manera abierta y crítica la interrelación entre la adopción de IA y la protección ante amenazas informáticas en empresas, considerando resultados e indicadores iniciales, evolución esperada y posibles áreas de mejora o desarrollo futuro en este campo emergente.

A su vez, la faceta descriptiva posibilitará elaborar una caracterización y diagnóstico actualizado respecto al estado del arte sobre el uso de capacidades de IA en las ciberdefensas implementadas por compañías contra modalidades de ataques contemporáneas. Así, se analizará con detenimiento la situación global y regional, para determinar el grado de efectividad que han demostrado hasta ahora estas tecnologías en la práctica por parte de las organizaciones.

De esta manera, mediante la integración de técnicas de exploración conceptual y descripción sistemática de evidencias, la investigación buscará constituirse en una plataforma de conocimientos y propuestas útiles por parte de la comunidad académica como para la toma de decisiones informada por parte de empresas en Latinoamérica respecto al uso estratégico de IA para la ciberseguridad.

3.4. Técnicas e instrumentos de recolección de la información

Se considerará población de estudio a empresas de diversos sectores que hayan implementado medidas de ciberseguridad haciendo uso de la inteligencia artificial durante el último año.

Se hará una revisión exhaustiva de literatura científica para establecer el marco teórico y antecedentes relacionados a la implementación de la inteligencia artificial en ciberseguridad en conjunto con las amenazas cibernéticas y las medidas preventivas en las empresas basándonos en reportes y bases de datos sobre modalidades o frecuencias de ciberataques con IA, inversiones en soluciones de ciberdefensa con IA y su adopción. Aplicación de técnicas estadísticas para analizar la relación entre la implementación de la inteligencia artificial y la efectividad de las medidas preventivas.

Utilizando esta información actualizada, se llevará a cabo un estudio observacional para determinar el comportamiento y los resultados de la integración de la inteligencia artificial en una estrategia de prevención de delitos cibernéticos, incluida la efectividad y la evaluación del impacto de las amenazas críticas actuales.

Por lo tanto, a través de un buen proceso de investigación y amplios datos, se estudiará el estado actual de la industria que utiliza la IA en ciberseguridad, mostrando su nivel de efectividad e integrando métodos de análisis de alto nivel poder identificar factores importantes para fortalecer el sistema de seguridad de TI.

3.5. Cronograma del proyecto de investigación

N°	Actividades	Meses	Enero				Febrero				Marzo				Abril			
		Sem	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Selección del tema			X														
2	Aprobación del tema				X													
3	Recopilación de la información				X													
4	Desarrollo del capítulo I					X												
5	Desarrollo del capítulo II						X											
6	Desarrollo del capítulo III							X										
7	Investigación crítica								X									
8	Desarrollo del capítulo IV									X								
9	Elaboración de las conclusiones									X								
10	Presentación de la tesis										X							
11	Sustentación previa										X							
12	Sustentación											X						

3.6. Recursos

3.6.1. Recursos humanos

Tabla 3. *Recursos humanos.*

PERSONAL	NOMBRE
INVESTIGADOR	**NATHALY ACOSTA CORTEZ**
DIRECTOR DEL PROYECTO	**ING. ALFONSO AGAMA CHICO**

3.6.2. Recursos económicos

Tabla 4. *Recursos económicos.*

Recurso	Inversión
Computador portátil	**$300**
Paquete Office	**$0**
Internet	**$24**
Impresiones	**$20**
Total	**$360**

CAPÍTULO IV. RESULTADOS DE LA INVESTIGACIÓN

4.1. Resultados obtenidos de la investigación

4.1.1. Metaanálisis

Se realizó una investigación exhaustiva de casos de estudio y reportes científicos que permitan analizar sistemáticamente la información recopilada sobre métodos de ciberseguridad con implementaciones de IA. A través de una búsqueda de información en bases de datos pertinentes como Scopus y Google académico para identificar estudios o artículos relevantes sobre la modalidad o frecuencia de los ciberataques haciendo uso de técnicas o herramientas de IA, y su adopción en el ámbito empresarial.

En la búsqueda se utilizó criterios de inclusión y exclusión para seleccionar estudios de la más alta calidad metodológica que cumplieran con los parámetros de investigación, publicaciones desde el año 2023 para recopilar la información más actualizada sobre el auge de la IA y su pronta implementación en las empresas.

A continuación, se describe el proceso de investigación que comprende el método de búsqueda de la información, la selección de las fuentes, el registro de los hallazgos y finalmente el análisis e interpretación de la información obtenida.

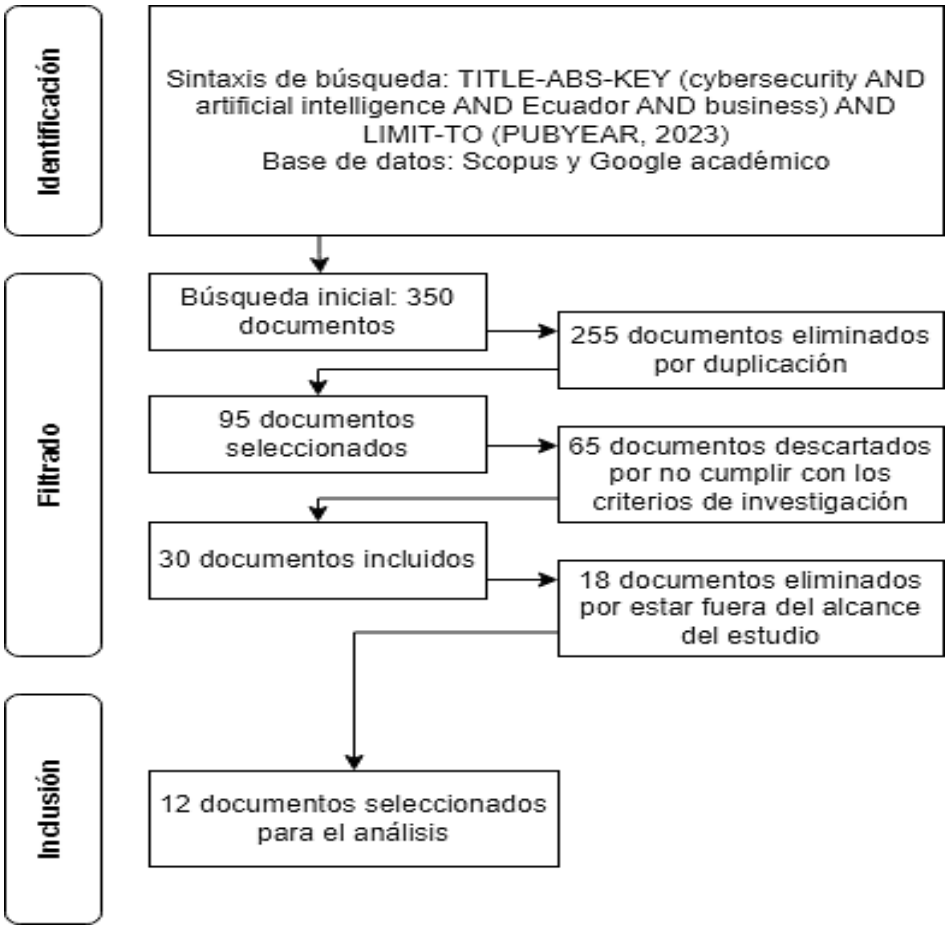
4.1.2. Revisión sistemática

Para cumplir con el objetivo del trabajo de investigación se consideró las siguientes cuestiones como método de inclusión de la información recopilada en la etapa de búsqueda.

- ¿Se han implementado métodos de IA en la empresa?
- ¿Qué porcentaje de eventos de seguridad son procesados mediante IA?

Para garantizar que los resultados se acerquen a lo esperado, son filtrados por la subárea de la informática para dirigir las investigaciones de seguridad informática durante el periodo más reciente del último año 2023. Asimismo, incluye resultados de investigaciones, análisis y comentarios de fuentes confiables y reconocidas en el campo de la IA y la ciberseguridad.

Figura 5. Proceso de extracción de datos



Fuente: Elaboración propia.

Entre los criterios de exclusión los documentos descartados en su mayoría no están directamente relacionados con el objetivo de estudio y son anteriores al periodo especificado. También se excluyen fuentes no confiables como sitios web sin verificación ni respaldo científico o artículos de revistas no indexadas sin revisión por pares.

Se consideran para la selección aquellos trabajos investigativos difundidos en revistas de prestigio, congresos académicos y centros de investigación reconocidos. También se realiza una investigación crítica del impacto de estos estudios y de los distintos aspectos relacionados con la IA en el ámbito de la seguridad de la información empresarial, este procedimiento contribuye a consolidar la robustez de los resultados.

Durante el proceso de recolección de la información se identificaron algunos términos de importancia, tales como: “Inteligencia artificial”, “ciberseguridad”, “seguridad IT”, “ataque cibernético”, “seguridad empresarial”. Durante este procedimiento se realiza una búsqueda exhaustiva en los archivos de distintas bases de datos, bibliotecas y portales académicos en la web, se consideran los documentos relevantes para la investigación abarcando un análisis cualitativo y cuantitativo.

La información recopilada en la búsqueda comprende el impacto de la IA en varios aspectos del campo de la ciberseguridad, de los cuales luego de una etapa de filtrado y extracción de información se obtuvo como resultado un total de 12 estudios para analizar.

4.2. Análisis e interpretación

En el siguiente apartado se procede a exponer las fuentes de investigación con sus principales aspectos detallados en la tabla 5.

Tabla 5. *Análisis de los estudios seleccionados.*

N°	Titulo	Autores y año	Aporte
1	A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America	Flor-Unda O, Simbaña F, Larriva-Novo X, Acuña Á, Tipán R, Acosta-Vargas P. (2023)	Flor-Unda et al., (2023) El informe destaca la falta de concienciación sobre la ciberseguridad, la ausencia de normas y reglamentos adecuados, el uso de software obsoleto, las deficiencias en la protección de infraestructuras críticas y la falta de formación especializada. El documento también cita los graves retos a los que se enfrenta la región para defenderse de los ciberataques en los organismos gubernamentales y a nivel individual. Subraya la importancia de invertir en educación, formación y concienciación en materia de ciberseguridad, así como en la cooperación nacional e internacional y el refuerzo de las defensas legales y tecnológicas. Esto establece las bases para un futuro digital más seguro y resiliente en América Latina.
2	Malicious Use of Artificial Intelligence and Threats to Psychological Security in Latin America: Common Problems, Current Practice and Prospects	Evgeny Pashentsev y Darya Bazarkina (2023)	Pashentsev & Bazarkina (2023) analizan las amenazas actuales y futuras derivadas del uso malicioso de la inteligencia artificial en América Latina, destacando la influencia de un entorno económico y socio-político inestable en el aumento de ciberataques y operaciones psicológicas intensificadas por la IA. Se resalta el uso de bots políticos y algoritmos de redes sociales en campañas en línea previas a las elecciones. Además, se señala el crecimiento de empresas que ofrecen servicios de comunicación política en línea con IA, con fines lucrativos. También se abordan las amenazas relacionadas con los intentos de EE. UU. de desacreditar productos chinos en el mercado tecnológico latinoamericano. Se concluye que la sociedad latinoamericana aún no está suficientemente consciente de estas amenazas en el ámbito de la seguridad psicológica.
3	Study on the importance of artificial intelligence in network cybersecurity	Maryam Abdulsalam Ali y Ali Alqaraghuli (2023)	Ali & Alqaraghuli (2023) Se centran en la intersección de la inteligencia artificial y la ciberseguridad y se ocupan de proteger los sistemas informáticos de ataques, hackeos y robo de datos. En este contexto, se presentarán trabajos relevantes sobre aprendizaje automático y aprendizaje profundo, cómo estos algoritmos ayudan a prevenir la intrusión en los sistemas informáticos al predecir y comprender el comportamiento y el tráfico del malware, fortaleciendo las defensas contra el acceso no autorizado. Esta publicación tiene como objetivo mejorar la seguridad, privacidad y confidencialidad de

			los datos personales y proteger a los usuarios y organizaciones en entornos virtuales críticos.
4	The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review	Maad Mijwil, Israa Ezzat Salem, Marwa M. Ismaeel (2023)	Mijwil et al. (2023) defienden los sistemas informáticos de ataques piratas informáticos y sustracción de datos mediante una examinación de técnicas de ciberseguridad, enfocándose en la inteligencia artificial. Incluye una revisión de la literatura que analiza el impacto del aprendizaje automático y las técnicas de aprendizaje profundo en la ciberseguridad. Los resultados muestran que estas tecnologías desempeñan un papel fundamental en la protección de los sistemas informáticos al pronosticar y entender el comportamiento y el tráfico del malware.
5	Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS	Villegas-Ch W, Govea J, Ortiz-Garces I (2023)	Villegas-Ch et al. (2023) destaca el potencial de la inteligencia artificial y la computación en la nube de Amazon Web Services (AWS) para mejorar la ciberseguridad. A través una serie de experimentos, se muestran que la inteligencia artificial, en los modelos OpenAI GPT-3 y DALL-E, puede generar datos sintéticos de alta calidad que simulan amenazas reales en línea. Estos datos son esenciales para entrenar los sistemas de detección de amenazas y aumentar la resiliencia los dispositivos. Además, se ha demostrado que la IA supera muchas veces a los métodos tradicionales en términos de velocidad de generación de datos y economía de recursos. Al reconocer las limitaciones inherentes y la importancia de abordar cuestiones éticas y de privacidad, este estudio es un paso importante hacia el logro de este objetivo. Ciberseguridad más eficaz y precisa en un ambiente tecnológico en constante variación.
6	Influence of Customer Perception Factors on AI-Enabled Customer Experience in the Ecuadorian Banking Environment	Tulcanaza-Prieto AB, Cortez-Ordoñez A, Lee CW (2023)	Tulcanaza-Prieto et al. (2023) Analizan la relación entre los factores de percepción del cliente y la experiencia del cliente habilitada por la inteligencia artificial en la industria bancaria ecuatoriana. Emplearon un cuestionario en línea diseñado por los propios investigadores, abordando cinco factores de percepción del cliente y dos categorías de experiencia del cliente por la IA. Los hallazgos principales destacan que los factores de percepción del cliente tienen un efecto positivo y significativo en la experiencia del cliente haciendo uso de IA en la banca ecuatoriana. Sin embargo, se señala la falta de un índice de percepción del cliente para los sectores económicos ecuatorianos como una limitación, junto con el enfoque en servicios financieros virtuales/móviles en detrimento de otros productos y servicios financieros que también incorporan IA.

7	Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0	de Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR (2023)	de Azambuja et al. (2023) analiza el surgimiento de los ciberataques en la era de la Industria y sus cambios impulsados por la inteligencia artificial 4.0. Se reconoce la importancia de comprender las estrategias de los ciberdelincuentes y crear medidas de seguridad efectivas. Mediante un análisis completo, se ofrece una visión detallada de los ataques cibernéticos potenciados por IA y se proponen estrategias defensivas para hacerles frente. Este estudio contribuye significativamente a la investigación, proporcionando orientación para la creación de estrategias defensivas contra futuras amenazas en el ámbito de la Industria 4.0. Además, a medida que la tecnología contra los delitos cibernéticos y sus defensas continúan evolucionando, se resalta la necesidad de actualizar constantemente la ciberseguridad.
8	Ciberseguridad empresarial: Ransomware y el impacto de la inteligencia artificial y la inteligencia artificial generativa	Alexis Arraz Almirall (2023)	Almirall (2023) afirmó que se ha estudiado en detalle el impacto de las herramientas de Inteligencia Artificial, especialmente las herramientas generativas. Cabe señalar como lo demuestran diversos experimentos que el uso incorrecto de estas herramientas, puede suponer una grave amenaza para las empresas, especialmente en la distribución de ransomware. Los resultados resaltan la importancia crítica de entrenar adecuadamente las herramientas de IA, especialmente en el contexto de la seguridad cibernética empresarial, con el fin de reducir posibles ciberataques. Se hace hincapié en la dualidad de la IA en este campo: si bien puede ayudar a descubrir y la concienciación sobre amenazas cibernéticas, también conlleva riesgos si se utiliza con malicia.
9	Cybersecurity in health sector: a systematic review of the literature	Peve Herrera, Catherine Mendoza, Jonathan Díaz, Mónica Herrera, Jose Luis Laberiano (2023)	Peve Herrera et al. (2023) enfatiza la importancia de la seguridad informática en la industria de la salud, especialmente en terminos de protección de estructuras y datos personales y la estructura organizativa de los centros de salud. Las tecnologías emergentes como la inteligencia artificial, el Internet de las Cosas Médicas (IoMT) y sensores se consideran herramientas fundamentales para reducir riesgos cibernéticos. Asimismo, se indica que ataques comunes como el phishing y el ransomware representan una amenaza significativa para la industria médica, especialmente durante la pandemia de COVID-19. Se sugiere el empleo de Blockchain como una solución destacada debido a su capacidad para gestionar información de manera segura y aumentar la confiabilidad de los datos del paciente y los equipos médicos. Este análisis contribuye a entender las acciones necesarias para reforzar la seguridad y privacidad de los datos en el ámbito médico, proponiendo un modelo basado en blockchain que promete mejorar la seguridad y la eficacia en los procesos sanitarios.
10	Security Operations	Cristóbal Muñoz y Aura Dolores	Muñoz-Zambrano & Zambrano-Rendón (2023) enfatizan el papel crucial del Centro de Operaciones de Seguridad (SOC) como un

	Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador.	Zambrano (2023)	componente clave para monitorear, analizar y coordinar las actividades relacionadas con la seguridad de la información en entornos informáticos. También se resalta la importancia de llevar a cabo una evaluación previa para comprender el estado actual de los sistemas, la infraestructura y las prácticas de seguridad de una empresa. Utilizando estándares como ISO 27001 e ISO 27002, se identifican las fortalezas, debilidades, oportunidades, amenazas y activos existentes, junto con los riesgos asociados. Se implementan procedimientos para establecer controles basados en políticas y prácticas, con el fin de manejar incidentes, incluyendo su identificación, mitigación y recuperación. En resumen, este enfoque estratégico en ciberseguridad resguarda la información y los activos digitales de una organización, promoviendo una cultura de seguridad y contribuyendo a un proceso continuo de mejora.
11	Beneficios y Riesgos de la Implementación de Inteligencia Artificial en los Procesos de Diagnóstico Médico en el Ecuador	Katherine Galarza Medina, Katherine Maldonado, Mónica Silvana Herrera (2023)	(Medina et al., 2023) Este análisis se centra en cómo la inteligencia artificial está afecta en la medicina, particularmente mejorando los procesos de diagnóstico y su aplicabilidad al sistema de salud de Ecuador. Se examinó una extensa gama de literatura científica de fuentes confiables, encontrando que la IA puede acelerar los procedimientos, predecir diagnósticos con precisión y brindar orientación personalizada para promover un estilo de vida saludable. Aunque se destacan los beneficios, se enfatiza la importancia de establecer políticas éticas para garantizar la seguridad y la privacidad de los datos de los pacientes. A nivel local, a pesar de algunos avances, persisten desafíos como la escasez de recursos y la capacitación del personal. En conclusión, es de suma importancia capacitar al personal y crear un ambiente de trabajo colaborativo y automatizado en las instituciones de salud para aprovechar completamente el potencial de la IA en la medicina.
12	Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad	Medina Astudillo Iván Daniel (2024)	Medina Astudillo (2024) abordó el creciente desafío de los ciberataques y la urgente necesidad de fortalecer la ciberseguridad para proteger los activos digitales y la infraestructura de las organizaciones. Se propone un enfoque innovador en I+D+i en ciberseguridad, centrado en contrarrestar problemas en áreas críticas mediante la evaluación de su impacto. Los resultados demuestran la viabilidad de implementar este modelo en el contexto ecuatoriano, considerando la diversidad de ataques y la constante evolución de las amenazas cibernéticas. Se enfatiza la importancia de especializarse en seguridad informática y adaptar los modelos de ciberseguridad a las necesidades y recursos individuales de cada organización.

En la siguiente tabla se presenta cada documento evaluado con el estudio realizado sobre el impacto de IA en cuestión de ciberseguridad, lo que permitirá conocer las implicaciones tanto positivas como negativas del uso de IA en la seguridad de la información dentro de las organizaciones.

Tabla 6. *Evaluación de la IA en la seguridad de la información.*

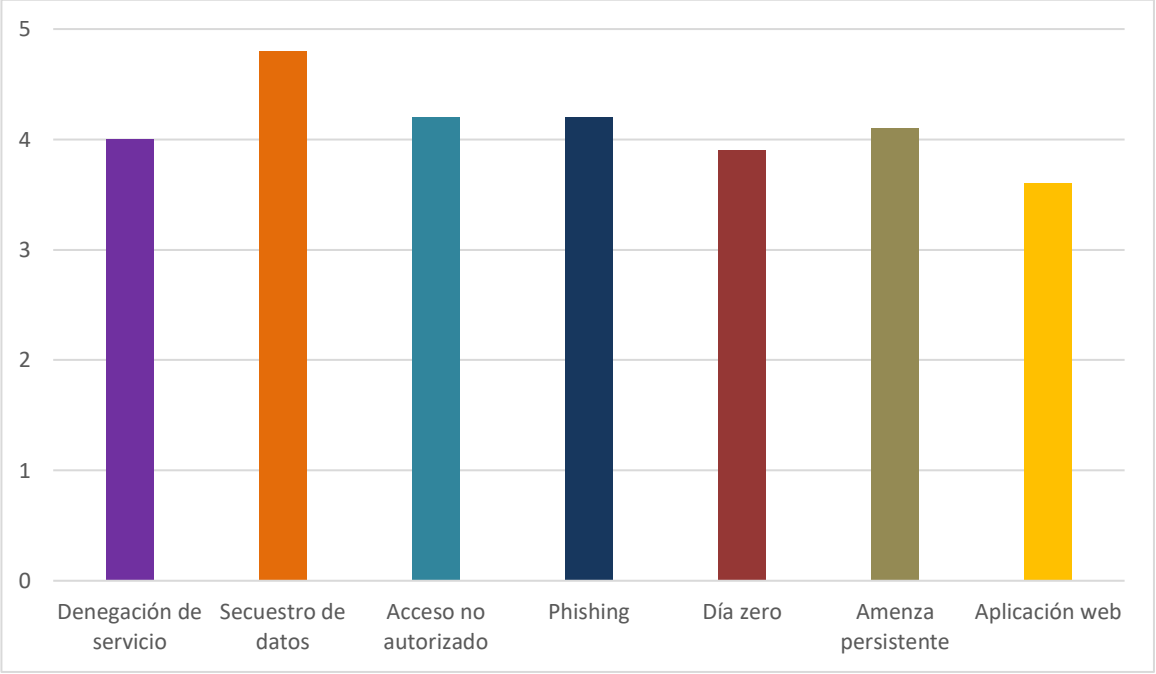
Título	La IA como medida de seguridad de la información	La IA como amenaza en la seguridad de la información
A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America	Invertir en conciencia en ciberseguridad para el fortalecimiento de la defensa tecnológica establece un punto fuerte para un futuro digital más seguro	La falta de concienciación y políticas de seguridad incrementan la posibilidad de un ataque como ingeniería social y phishing de manera efectiva.
Malicious Use of Artificial Intelligence and Threats to Psychological Security in Latin America: Common Problems, Current Practice and Prospects	Con el correcto uso de herramientas de IA puede facilitar la identificación de grandes cantidades de datos electorales y evitar fraudes.	La falta de conocimiento de los usuarios en tema de ciberseguridad y su psicología permite a los atacantes aprovecharse de la primera línea de defesa en la organización, las personas.
A Survey on the Significance of Artificial intelligence in Network cybersecurity	Los sistemas de inteligencia artificial desempeñan un papel importante a la hora de fortalecer la seguridad de la red frente a amenazas, hackers y el robo de información sensible.	Una mayor dificultad también puede comprometer la seguridad de la información, ya que los hackers pueden aprovecharla para desarrollar ataques más avanzados.
The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review	La capacidad de la IA de examinar automáticamente conductas anómalas en los programas informáticos, fortificando la autenticación de identidades.	Del mismo modo la IA da paso al desarrollo de ataques automatizados en los sistemas de seguridad, aumentando el riesgo de infiltraciones.
Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS	La integración de tecnología mejora la capacidad de aplacar los riesgos para la infraestructura digital de las empresas, mejora su capacidad para resistir ataques cibernéticos.	Es importante entender los avances de la IA y sus aplicaciones en ciberataques, lo que subraya la necesidad de aumentar la atencion y respuesta por parte de las organizaciones.
Influence of Customer Perception Factors on AI-	El uso de sistemas de inteligencia artificial facilita la adaptación de	La falta de comprensión y conciencia por parte de los usuarios puede generar

Enabled Customer Experience in the Ecuadorian Banking Environment	servicios a las demandas individuales de los usuarios y las capacidades disponibles en una empresa.	una percepción negativa de las mejoras con IA en los procesos comerciales de la empresa, lo que genera una falta de confianza en la seguridad de los datos.
Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0	Con medidas de seguridad efectivas la implementación de la IA en el contexto de la industria 4.0 se prevé una oportunidad competitiva en el mercado.	Los riesgos asociados con la transformación digital, particularmente en ciberseguridad, pueden verse exacerbados por el uso de IA en ciberataques que pueden comprometer la seguridad de la información organizacional.
Ciberseguridad empresarial: Ransomware y el impacto de la inteligencia artificial y la inteligencia artificial generativa	La creación adecuada de los modelos de inteligencia artificial puede ayudar a las organizaciones a evitar posibles ataques informáticos.	Las capacidades de generativas de inteligencia artificial, como la de ChatGPT y otros sistemas similares, puede ser utilizada para generarl códigos maliciosos que constituyen una seria amenaza para las empresas.
Cybersecurity in health sector: a systematic review of the literature	El uso de tecnologías emergentes como IA y el IoT (Internet de las Cosas) de manera responsable y consciente ayuda a mitigar riesgos cibernéticos, ya que usualmente la tecnología IoT suele utilizar mecanismos de Blockchain para protección de la información.	Ningún sistema es 100% seguro por lo que se pueden vulnerar estas herramientas para hacer un uso mal intencionado de las mismas, lo que representa una amenaza significativa más aún en la industria médica.
Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador.	Los estándares de seguridad de la información siempre son importantes tenerlos en cuenta para evaluar el estado de los sistemas informáticos previo a una mejora con la implementación de la IA.	Las brechas de seguridad por la falta de capacitación o regulación con estándares en las empresas y malas prácticas de seguridad provocan que los atacantes tengan una mayor facilidad de vulnerar la infraestructura de la empresa.
Beneficios y Riesgos de la Implementación de Inteligencia Artificial en los Procesos de Diagnóstico Médico en el Ecuador	La aplicación de la IA en los procesos empresariales mejoran la viabilidad y eficiencia en la agilización de los procedimientos habituales, logrando predecir y detectar anomalías con precisión.	La falencia de recursos y capacitación de personal representa un desafío para aprovechar plenamente el potencial de la IA de manera correcta. De lo contrario sigue existiendo la posibilidad de estar expuestos a amenazas por la sofisticación en los ataques

		informáticos.
Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad	El incremento de los ataques informáticos está impactando en las operaciones de las empresas en diversas industrias, resaltando la urgencia de adoptar medidas de seguridad en las cuales la inteligencia artificial pueda desempeñar un rol crucial para salvaguardar dicha información.	El progreso en Inteligencia Artificial demanda una continua evolución de las tácticas de seguridad informática para contrarrestar su potencial uso en ataques cibernéticos, destacando la importancia de ser más flexibles y robustos en nuestras medidas de protección.

La evolución de los ciberataques en el último tiempo tiene muchas variantes, técnicas y métodos de ejecución. Sin embargo, los ataques informáticos más recurrentes en empresas ecuatorianas son los que se muestran en la siguiente gráfica, dónde se considera un rango de valores 0 al 5, siendo este último una representación de mayor incidencia del ataque en cuestión.

Figura 6. Ciberataques de mayor recurrencia en el país.



La figura 6 expone que los ataques del tipo secuestro de datos y suplantación de identidad (Phishing) son los más habituales en el país. La siguiente tabla muestra cómo operan y afectan estos dos ataques a una organización.

Tabla 7. *Identificando los ataques más recurrentes.*

Tipo de ataque	Cómo funciona	Cómo afecta
Secuestro de datos	Este tipo de ataque niega el acceso a los usuarios bloqueando el sistema hasta que se pague un rescate por la información secuestrada.	Los ataques de ransomware tienen un impacto significativo en las víctimas y las organizaciones. Esto limitará su trabajo y afectará su productividad hasta que la tarifa sea cancelada, corre el riesgo de perder sus datos.
Suplantación de identidad	El phishing involucra la integridad de su información personal y financiera. Induce a personas a revelar información confidencial, como contraseñas o datos de tarjetas de crédito, puede provocar robo de identidad, fraude financiero y acceso no autorizado. Además, puede dañar el prestigio de la empresa involucrada y causar desconfianza por parte de los clientes.	El phishing opera enviando correos electrónicos que parecen legítimos, pero incluye enlaces falsos a sitios web adulterados. Los usuarios son engañados para proporcionar información confidencial, que los atacantes luego utilizan. El phishing se realiza utilizando diferentes métodos , como el correo electrónico, mensajes de texto, redes sociales y otros métodos que tengan acceso a la red .

A pesar de los beneficios de la IA al servicio de mejorar la seguridad y automatizar tareas para maximizar la eficiencia de los métodos de seguridad y salvaguardar la información de actores maliciosos, estos últimos también se pueden aprovechas de herramientas con IA para sus propios beneficios y desarrollar métodos de ataques desconocidos o mejorar los vectores de ataques tradicionales.

Gracias al modelo de IA es posible identificar y analizar a los usuarios y sus comportamientos. Curiosamente, esto mejorará nuestra capacidad para detectar y responder a amenazas. Aún más eficaz es el hecho de que los ciberdelincuentes están encontrando formas creativas de eludir estas medidas de seguridad. Es por este motivo que se debe enfatizar la importancia de desarrollar defensas efectivas y adaptativas para proteger los activos de las organizaciones en un entorno digital cada vez más complejo y en constante evolución.

4.3. Conclusiones

La ciberseguridad en entornos corporativos está adquiriendo cada vez más importancia debido al aumento de los ciberataques, especialmente en los sectores financiero y sanitario donde la falta de concienciación y formación del personal puede exponer vulnerabilidades críticas de la organización.

La adopción de tecnologías en el contexto de Industria 4.0 han proporcionado beneficios significativos, sin embargo, también se ha visto en aumento los riesgos respecto a seguridad de la información, lo que demuestra la necesidad de implementar medidas de seguridad efectivas que incluyan técnicas de IA y medidas preventivas estratégicas para no ser afectados por la misma. Usar la inteligencia artificial en ciberataques brinda nuevos desafíos para la protección de la información, resaltando la necesidad de indagar y cimentar defensas sólidas.

A su vez, la IA no solo mejora la detección de amenazas, sino que también mejora la creación en seguridad y facilita la cooperación entre profesionales de la seguridad. También juega un papel importante en la detección y respuesta a los ciberataques. En algunos casos, como blockchain y el Internet industrial de las cosas (IIoT), la IA mejora la preservación de la confidencialidad y la integridad de los sistemas, pero el aumento de los ciberataques basados en IA es una preocupación importante.

Los ciberdelincuentes están aprovechando las capacidades de la IA para crear malware más sigiloso y utilizar tácticas de control más poderosas. La utilización de sistemas de inteligencia artificial para reunir y examinar grandes cantidades de datos puede arriesgarse la privacidad de la información y crear rechazo en la toma de decisiones. En este ambiente dinámico, la incorporación de la IA en la seguridad de la información se ha convertido en una forma relevante de continuar el progreso para seguir avanzando en la actualidad.

4.4. Recomendaciones

En los últimos años, el país ha implementado actividades y programas destinados a promover el conocimiento y la formación profesional en ciberseguridad. Sin embargo, es importante continuar invirtiendo en formación, educación y concienciación sobre ciberseguridad a nivel individual, empresarial y gubernamental.

La convergencia de la inteligencia artificial y el ciberdelito ha cambiado el panorama de los ciberataques, permitiendo a los delincuentes atacar vulnerabilidades sin revelarse. Pero la respuesta es masiva y las organizaciones están utilizando la misma IA para identificar y contrarrestar las amenazas.

A continuación, se establecen algunas recomendaciones en base al estudio realizado sobre las tendencias de la IA y su impacto en la ciberseguridad:

- Es de suma importancia mantenerse informado con las últimas tendencias en ciberseguridad, específicamente en áreas donde se utiliza IA para defenderse y para llevar a cabo ataques. Esto asegura una mejor respuesta frente a nuevas amenazas y la ejecución de medidas más estrictas.

- La incorporación de soluciones de ciberseguridad basadas en IA es esencial para proteger los recursos de la organización contra las amenazas en constante variación. Eso significa identificar y combatir ataques mediante sistemas de prevención y detección de intrusiones que se apoyan en modelos de IA para identificar y contrarrestar ataques.

- Es importante realizar evaluaciones periódicas de riesgos de ciberseguridad para identificar posibles lagunas y áreas de mejora en las medidas de seguridad actuales. La inteligencia artificial se puede utilizar para analizar datos e identificar patrones y anomalías que puedan indicar un ataque cibernético.

- Invertir en desarrollar el personal de la organización en capacitaciones y cursos dónde profesionales inculquen las mejores prácticas en ciberseguridad, incluida la identificación de posibles ataques y la respuesta adecuada antes de que se produzcan violaciones de seguridad.

- Establecer políticas y procedimientos para manejar un incidente de ciberseguridad, incluida la asignación de responsabilidades y la comunicación efectiva en caso de una ocurrencia que pueda costarle a la organización.

Referencias bibliográficas

Ray, A. (2022). Riesgos líquidos. Los nuevos desafíos a la seguridad global. Tampa, Florida. USA: *Kindle Direct Publishing.*

Ali, M. A., & Alqaraghuli, A. (2023). A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity. *Babylonian Journal of Networking*, *2023*, 21-29. https://doi.org/10.58496/BJN/2023/004

Almirall, A. A. (2023). *Ciberseguridad empresarial: Ransomware y el impacto de la inteligencia artificial y la inteligencia artificial generativa*. https://openaccess.uoc.edu/handle/10609/149629

Cano, J. (2023, noviembre 7). Pronósticos de seguridad/ciberseguridad 2024. Una visión holística y situada. *Ciberprisma - alianza por la ciberseguridad*. https://ciberprisma.org/2023/11/07/pronosticos-de-seguridad-ciberseguridad-2024-una-vision-holistica-y-situada/

Cano, J. J. (2021). Resiliencia digital: La nueva frontera para las organizaciones del siglo XXI. *Revista Sistemas*, *159*, Article 159. https://doi.org/10.29236/sistemas.n159a6

de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), Article 8. https://doi.org/10.3390/electronics12081920

European Union Agency for Cybersecurity. (2023). *Artificial intelligence and cybersecurity research: ENISA research and innovation Brief.* Publications Office. https://data.europa.eu/doi/10.2824/808362

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics*, *10*(3), Article 3. https://doi.org/10.3390/informatics10030071

Guerrero Panchana, J. F., & Romero Ibarra, J. L. (2023). La inmunización de la red: La inteligencia artificial basada en Python como bloqueo contra los ciberataques. *Sinergia Académica*, *6*(Especial). https://doi.org/10.51736/sa.v6iEspecial.178

Khoei, T. T., Slimane, H. O., & Kaabouch, N. (s. f.). *A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions*.

Medina Astudillo, I. D. (2024). *Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/26727

Medina, K. X. G., Coronel, K. M., & Guanopatin, M. S. H. (2023). Beneficios y Riesgos de la Implementación de Inteligencia Artificial en los Procesos de Diagnóstico Médico en el Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(6), 7276-7299. https://doi.org/10.37811/cl_rcm.v7i6.9274

Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. *Iraqi Journal For Computer Science and Mathematics*, *4*(1), Article 1. https://doi.org/10.52866/ijcsm.2023.01.01.008

Muñoz-Zambrano, C., & Zambrano-Rendón, A. D. (2023). Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador. *MQRInvestigar*, *7*(3), Article 3. https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236

Ortiz Centurion, E. S., Mendoza de los Santos, A. C., & Villacorta Vidal, C. A. (2023). Inteligencia artificial en la seguridad de la información en una organización. *Investigación Universitara de la Universidad Nacional de Ucayali*, *13*(2), 1046-1063. https://doi.org/10.53470/riu.v13i2.120

Pabon, J. F., Aizaga, M., Recalde, H., & Toasa, R. M. (2023). Revisión de literatura sobre impacto de la Inteligencia Artificial y su aplicación en el Ecuador. *Universidad Tecnológica Israel*, *55*, 100-113.

Pashentsev, E., & Bazarkina, D. (2023). Malicious Use of Artificial Intelligence and Threats to Psychological Security in Latin America: Common Problems, Current Practice and

Prospects. En *The Palgrave Handbook of Malicious Use of AI and Psychological Security* (pp. 531-560). Springer International Publishing. https://doi.org/10.1007/978-3-031-22552-9_20

Pereira, J. J. E. (2020). Detección de anomalías en la red empleando técnicas de machine learning. *Universidade Da Caruña*.

Peve Herrera, C. V., Mendoza Valcarcel, J. S., Díaz, M., Herrera Salazar, J. L., & Andrade-Arenas, L. (2023). *Cybersecurity in health sector: A systematic review of the literature*. https://doi.org/10.11591/ijeecs.v31.i2.pp1099-1108

Rodriguez, L. E. C. (2020). *ESTADO ACTUAL DE LA CIBERSEGURIDAD APLICADA A SISTEMAS DEFENSIVOS Y OFENSIVOS A PARTIR DE INTELIGENCIA ARTIFICIAL*.

Salazar Rodríguez, E. I. (2023). *Revisión de literatura sobre métodos de protección para garantizar ciberseguridad en instituciones financieras en el contexto ecuatoriano* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/25928

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), Article 12. https://doi.org/10.1038/s42256-019-0109-1

Tulcanaza-Prieto, A. B., Cortez-Ordoñez, A., & Lee, C. W. (2023). Influence of Customer Perception Factors on AI-Enabled Customer Experience in the Ecuadorian Banking Environment. *Sustainability*, *15*(16), Article 16. https://doi.org/10.3390/su151612441

Veiga Fernandez, C. (2023). La inteligencia artificial en la empresa: Evolución y futuro en la era digital. *Universidad Rey Juan Carlos*. https://eciencia.urjc.es/handle/10115/26580

Villegas-Ch, W., Govea, J., & Ortiz-Garces, I. (2024). Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS. *Applied Sciences*, *14*(2), Article 2. https://doi.org/10.3390/app14020679

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, *8*, 146598-146612. https://doi.org/10.1109/ACCESS.2020.3013145

Elsaeidy, A. A., Jamalipour, A., & Munasinghe, K. S. (2021). A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City. IEEE Access, 9, 154864–154875. https://doi.org/10.1109/ACCESS.2021.3128701

S. Chen et al. (2018) "Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach," computers & security, vol. 73, pp. 326–344.

Stevens, Tim, Knowledge in the grey zone: AI and cybersecurity (2020). Knowledge in the grey zone: AI and cybersecurity. Digital War 1(1): 164-170., SSRN: https://ssrn.com/abstract=4031502

Escalante Quimis, O. A. (2021). Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica. http://dspace.ups.edu.ec/handle/123456789/20576