EXPLORACIÓN DE LAS PERSPECTIVAS EMERGENTES EN CIBERSEGURIDAD: UN ANÁLISIS DE LAS TENDENCIAS ACTUALES EN RANSOMWARE, INTELIGENCIA ARTIFICIAL E INTERNET DE LAS COSAS (IOT)

NOMBRE DEL ESTUDIANTE

ANGY DANIELA JEREZ PINZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2024

EXPLORACIÓN DE LAS PERSPECTIVAS EMERGENTES EN CIBERSEGURIDAD: UN ANÁLISIS DE LAS TENDENCIAS ACTUALES EN RANSOMWARE, INTELIGENCIA ARTIFICIAL E INTERNET DE LAS COSAS (IOT)

NOMBRE DEL ESTUDIANTE

ANGY DANIELA JEREZ PINZÓN

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

NOMBRE TUTOR
EDGAR ROBERTO DULCE VILLAREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bucaramanga, 01 abril 2024

DEDICATORIA

Agradezco a Dios y a mis padres porque me han brindado su apoyo incondicional en cada momento, también a los instructores que han ofrecido sus conocimientos para llevar a cabo esta especialización.

AGRADECIMIENTOS

Agradezco a Dios por darme la salud y trabajo, para seguir continuando mis estudios.

A mis padres por darme ese apoyo en todo momento y mis amigos por siempre dar esa voz de aliento.

Finalmente agradezco a los docentes que con sus conocimientos inculcan a seguir adelante y aprender, también a la universidad que nos da ese apoyo de seguir trabajando y estudiando a la vez la cual nos ayuda para seguir adquiriendo esa experiencia.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Análisis de tendencias: La evaluación de patrones y cambios en el tiempo para anticipar futuras amenazas o soluciones de ciberseguridad.

Ciber amenaza: Una amenaza cibernética que puede causar daño a sistemas, datos o redes.

Ciber inteligencia: La recopilación y análisis de información sobre amenazas cibernéticas para tomar decisiones informadas en seguridad.

Ciberseguridad: La protección de sistemas, redes y datos contra amenazas cibernéticas.

Criptovirus: Un tipo de malware utilizado en ataques de ransomware para cifrar datos.

Inteligencia Artificial (IA): La simulación de procesos de inteligencia humana mediante sistemas informáticos, utilizada en ciberseguridad para la detección de amenazas.

Internet de las Cosas (IoT): Conexión de dispositivos físicos a Internet para recopilar y compartir datos, lo que plantea desafíos de seguridad.

Ransomware: Un tipo de malware que cifra los datos de una víctima y exige un rescate para su desbloqueo.

Phishing: Un ataque que engaña a las víctimas para que revelen información confidencial, como contraseñas, a menudo a través de correos electrónicos fraudulentos.

Zero-Day: Una vulnerabilidad de software desconocida o no parcheada que puede ser explotada por atacantes.

RESUMEN

El panorama de la ciberseguridad está experimentando una transformación significativa en la actualidad, impulsada por una serie de tendencias emergentes que incluyen el aumento del ransomware, la creciente influencia de la inteligencia artificial (IA) y la proliferación de dispositivos de Internet de las cosas (IoT). El ransomware se ha convertido en una amenaza omnipresente en el ciberespacio. Los ciberdelincuentes utilizan el ransomware para cifrar datos y exigir un rescate a cambio de su liberación. Este tipo de ataques ha afectado a empresas, instituciones gubernamentales y usuarios individuales por igual.

La inteligencia artificial está desempeñando un papel cada vez más importante en la ciberseguridad. Las soluciones basadas en IA pueden analizar grandes volúmenes de datos en tiempo real para detectar patrones de actividad sospechosa y prevenir ataques cibernéticos.

La expansión de los dispositivos IoT también está aumentando la superficie de ataque cibernético. Los dispositivos IoT, desde cámaras de seguridad hasta termostatos inteligentes, a menudo carecen de medidas de seguridad adecuadas y pueden ser vulnerables a intrusiones.

Para abordar estas tendencias, las organizaciones están adoptando enfoques multifacéticos. Esto incluye la capacitación de empleados en ciberseguridad, la implementación de soluciones avanzadas de detección y respuesta, y la inversión en investigación y desarrollo de tecnologías de seguridad basadas en IA. Además, se están promoviendo estándares de seguridad para dispositivos IoT y se están desarrollando políticas de gestión de amenazas más sólidas a nivel gubernamental y corporativo.

ABSTRACT

The cybersecurity landscape is undergoing a significant transformation today, driven by a number of emerging trends including the rise of ransomware, the growing influence of artificial intelligence (AI), and the proliferation of Internet of Things (IoT) devices. Ransomware has become a ubiquitous threat in cyberspace. Cybercriminals use ransomware to encrypt data and demand a ransom in exchange for its release. These types of attacks have affected companies, government institutions, and individual users alike.

Artificial intelligence is playing an increasingly important role in cybersecurity. AI-based solutions can analyze large volumes of data in real time to detect patterns of suspicious activity and prevent cyber attacks.

The expansion of IoT devices is also increasing the cyber attack surface. IoT devices, from security cameras to smart thermostats, often lack adequate security measures and can be vulnerable to intrusions.

To address these trends, organizations are taking multifaceted approaches. This includes training employees in cybersecurity, implementing advanced detection and response solutions, and investing in research and development of AI-based security technologies. Additionally, security standards for IoT devices are being promoted and stronger threat management policies are being developed at the government and corporate levels.

INTRODUCCIÓN

La ciberseguridad se ha convertido en un tema de máxima importancia en la era digital actual. A medida que la dependencia de la tecnología continúa creciendo, también lo hacen las amenazas cibernéticas que buscan explotar nuestras vulnerabilidades en línea. En este contexto, es fundamental analizar las perspectivas de las tendencias actuales en ciberseguridad, con un enfoque especial en tres factores clave: el ransomware, la inteligencia artificial (IA) y el Internet de las cosas (IoT).

El ransomware[1] ha emergido como una de las amenazas más destructivas y lucrativas en el mundo digital. Este tipo de malware cifra los datos de las víctimas y exige un rescate a cambio de su liberación. Las organizaciones de todo el mundo se enfrentan a una creciente ola de ataques de ransomware que no solo causan pérdidas financieras significativas, sino que también socavan la confianza de los consumidores y la integridad de los datos.

Por otro lado, la inteligencia artificial[2] está desempeñando un papel cada vez más importante en la ciberseguridad. Las soluciones basadas en IA tienen la capacidad de analizar grandes cantidades de datos en tiempo real, identificar patrones anómalos y mejorar la detección y respuesta ante amenazas cibernéticas. Sin embargo, este avance tecnológico también plantea cuestiones éticas y de seguridad, ya que los atacantes pueden utilizar la IA para perfeccionar sus tácticas de ataque.

---

[1] Sharma, P., Kapoor, S. y Sharma, R. Detección, prevención y protección de ransomware en dispositivos IoT mediante técnicas de aprendizaje automático basadas en un enfoque de análisis dinámico. {En línea}. 2022. {22 de mayo de 2024}. Disponible en: https://doi.org/10.1007/s13198-022-01793-0

[2] Alrfai, MM, Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M. y Almaiah, MA La influencia de la inteligencia artificial en la eficiencia de los AIS: efecto moderador de la ciberseguridad. {En línea}. 2023. {29 enero del 2024}. Disponible en: https://www.researchgate.net/publication/373139284_The_influence_of_artificial_intelligence_on_the_AISs_efficiency_Moderating_effect_of_the_cyber_security

Finalmente, los dispositivos IoT[3], desde electrodomésticos hasta sistemas de control industrial, a menudo carecen de medidas de seguridad sólidas, lo que los convierte en blancos ideales para los ciberdelincuentes. La seguridad en IoT se ha convertido en una preocupación crítica, y es esencial comprender cómo proteger estos dispositivos interconectados de manera efectiva.

[3] Kouicem, DE, Bouabdallah, A., & Lakhlef, H. Seguridad de Internet de las cosas: una encuesta de arriba hacia abajo. En: Computer Networks . 141 (2018); Pág. 199-221. Disponible en: https://www.researchgate.net/publication/323912995_Internet_of_Things_Security_a_top-down_survey

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años, la ciberseguridad ha experimentado un cambio significativo debido a las tendencias emergentes en ransomware, inteligencia artificial e Internet de las cosas (IoT). El ransomware ha evolucionado hacia ataques más sofisticados, incluyendo el modelo Ransomware como servicio (RaaS). La inteligencia artificial se ha convertido en una herramienta fundamental tanto para defensores como para atacantes, permitiendo automatizar y personalizar ataques. Por otro lado, el crecimiento de dispositivos IoT ha ampliado la superficie de ataque, con botnets de IoT como una amenaza destacada. La regulación y la colaboración se han vuelto cruciales en un entorno donde la conciencia pública sobre la ciberseguridad está en constante crecimiento.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo abordar de manera efectiva las amenazas y desafíos actuales del ransomware, la inteligencia artificial y el Internet de las cosas (IoT) en el ámbito de la ciberseguridad, y cómo pueden las organizaciones desarrollar estrategias sólidas de prevención, detección y respuesta para salvaguardar sus activos digitales y datos?

JUSTIFICACIÓN

La ciberseguridad es un tema de relevancia creciente en la sociedad actual debido a la creciente dependencia de la tecnología y la digitalización de casi todos los aspectos de nuestras vidas. A medida que las amenazas cibernéticas evolucionan, se hacen más sofisticadas y aumentan en frecuencia, es crucial abordar estas tendencias actuales en el campo de la ciberseguridad. Esta justificación se centra en la importancia de comprender y abordar estas tendencias desde diversas perspectivas, incluida la protección de datos personales, la seguridad de las empresas y la estabilidad de las infraestructuras críticas.

Uno de los aspectos más importantes de las tendencias actuales en ciberseguridad es la protección de datos personales. Con el auge de las redes sociales, el comercio electrónico y la digitalización de la atención médica y la educación, los datos personales se han convertido en un activo valioso para las empresas y un objetivo atractivo para los ciberdelincuentes. La exposición de datos personales puede tener consecuencias devastadoras, incluido el robo de identidad, el fraude financiero y la invasión de la privacidad.

Las empresas y organizaciones de todos los tamaños enfrentan una creciente amenaza en el ámbito de la ciberseguridad. Los ataques cibernéticos pueden tener un impacto catastrófico en las operaciones empresariales, desde la pérdida de datos críticos hasta la interrupción de los servicios. La seguridad empresarial no solo afecta a las empresas, sino también a sus clientes, socios y empleados. Las tendencias actuales en ciberseguridad, como el ransomware y los ataques dirigidos, pueden resultar en la pérdida de ingresos y la reputación de la empresa.

OBJETIVOS

1.3 OBJETIVO GENERAL

Demostrar las tendencias y desafíos actuales en el campo de la ciberseguridad, centrándose en las amenazas de ransomware, las aplicaciones de la Inteligencia Artificial y el impacto de Internet de las Cosas (IoT), mediante repositorios documentales a fin de proporcionar soluciones efectivas que fortalezcan la protección de sistemas, redes y datos en el entorno digital actual.

1.4 OBJETIVOS ESPECÍFICOS

- Analizar las vulnerabilidades y riesgos de seguridad asociados con la proliferación de dispositivos IoT por medio de conceptos, identificando las amenazas más comunes y evaluando las estrategias de mitigación existentes para proteger eficazmente estos dispositivos y las redes interconectadas.

- Explicar el impacto de la Inteligencia Artificial en la ciberseguridad, seleccionando las técnicas de IA que se utilizan para detectar, prevenir y responder a amenazas cibernéticas para la mejora de seguridad digital en organizaciones y sistemas informáticos.

- Evaluar la evolución de las tácticas y técnicas de ransomware en los últimos años entre 2020 y 2023 con el método cuantitativo de revisión de documentos, identificando patrones y cambios en los procedimientos utilizados por los ciberdelincuentes en estos ataques, con el fin de comprender mejor la naturaleza cambiante de esta amenaza cibernética.

- Recomendar soluciones tecnológicas que fortalezcan a las organizaciones contra ataques de ransomware, aprovechando el poder de la Inteligencia Artificial (IA) y abordando potenciales vulnerabilidades en el Internet de las Cosas (IoT).

MARCO REFERENCIAL

Se tomará como referencias los siguientes libros, artículos relacionados a continuación:

La "Guía Contra Ataques Ransomware" de Christopher M. Frenz y Christian L. Diaz, publicada por OWASP, proporciona pautas y mejores prácticas para prevenir, detectar y responder a ataques de ransomware. Se abordan aspectos de seguridad cibernética, concientización, respaldo de datos, políticas de acceso y más para mitigar esta amenaza cada vez más común en la ciberseguridad.

Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. Cogent Social Sciences examina cómo la implementación de inteligencia artificial en sistemas de información contable puede mejorar la eficiencia, pero destaca la importancia de la ciberseguridad como un factor clave para mitigar riesgos y garantizar un funcionamiento seguro y eficaz.

Otro referente es Amiruddin, A., Ratna, A. A. P., & Sari, R. F. (2019). Systematic review of internet of things security, ofrece una revisión exhaustiva de la seguridad en el Internet de las cosas (IoT). Examina las amenazas, desafíos y soluciones en la protección de dispositivos y datos IoT, proporcionando una visión general de las preocupaciones clave en este ámbito emergente.

1.5 MARCO TEÓRICO

1.5.1 RANSOMWARE

El ransomware[4] es un tipo de software malicioso que cifra los archivos de una computadora o red y exige un rescate para desbloquearlos. Los ciberdelincuentes utilizan el cifrado para inaccesibilizar datos cruciales, y luego exigen un pago en criptomonedas a cambio de proporcionar la clave de descifrado. Este tipo de ataque puede causar estragos en empresas, gobiernos y usuarios individuales, ya que la pérdida de datos puede ser devastadora. Además, el ransomware puede propagarse a través de correos electrónicos, descargas de software malicioso o vulnerabilidades de seguridad. Para protegerse, es importante mantener el software actualizado, hacer copias de seguridad de los datos y no abrir correos electrónicos sospechosos o descargar archivos de fuentes no confiables. La lucha contra el ransomware es continua y requiere medidas de seguridad sólidas y conciencia cibernética.

Las organizaciones de todo el mundo se enfrentan a una creciente ola de ataques de ransomware que no solo causan pérdidas financieras significativas, sino que también socavan la confianza de los consumidores y la integridad de los datos. Los ataques de ransomware pueden tener graves consecuencias, incluyendo la pérdida de datos, la interrupción de las operaciones comerciales, y la pérdida de reputación. La prevención es la mejor táctica para combatir el ransomware. Esto incluye mantener actualizado el software y los sistemas operativos, utilizar contraseñas seguras, evitar abrir correos electrónicos y enlaces sospechosos, y realizar copias de seguridad regulares de los datos. Además, es importante contar con un plan de respuesta a incidentes de ransomware y capacitar al personal sobre cómo identificar y responder a los ataques de ransomware.

1.5.1.1 EL INTERNET DE LAS COSAS

[4] Moreno, J., Rodríguez, C., & Leguias, I. Revisión sobre propagación de ransomware en sistemas operativos Windows. En: I+D Tecnológico. 16 (2020); N° 1; Pag. 39-45

Se refiere a la interconexión de dispositivos físicos a través de Internet, permitiéndoles recopilar y compartir datos para realizar diversas funciones. Estos dispositivos pueden ser desde electrodomésticos y sensores industriales hasta vehículos y dispositivos médicos. El IoT se basa en la idea de que objetos cotidianos pueden estar equipados con sensores, actuadores y conectividad, lo que les permite comunicarse y tomar decisiones de manera autónoma.

El IoT[5] tiene un amplio alcance de aplicaciones, desde la automatización del hogar y la gestión inteligente de ciudades hasta la monitorización de la salud y la optimización de procesos industriales. Aunque ofrece muchas ventajas, como eficiencia y comodidad, también plantea desafíos de seguridad y privacidad, ya que la cantidad de datos generados y compartidos es inmensa.

A medida que el IoT continúa evolucionando, su influencia en nuestra vida cotidiana y en diversos sectores industriales sigue creciendo, lo que hace que la gestión adecuada de la seguridad y la privacidad sea esencial.

Ofrece una serie de beneficios, incluyendo la mejora de la eficiencia, la automatización de procesos, y la creación de nuevos modelos de negocio. Sin embargo, también presenta una serie de desafíos y riesgos, incluyendo la seguridad cibernética, la privacidad, y la interoperabilidad.

La seguridad cibernética es una preocupación importante en el IoT, ya que los dispositivos conectados pueden ser vulnerables a los ataques de hackers y otros actores malintencionados. La privacidad también es una preocupación, ya que los dispositivos conectados pueden recopilar y compartir grandes cantidades de datos

[5] Amiruddin, A., Ratna, AAP y Sari, RF Revisión sistemática de la seguridad de Internet de las cosas. {En línea}. 2019. {28 enero del 2024}. Disponible en: https://www.researchgate.net/publication/358022729_Systematic_Literature_Review_of_Internet_of_Things_IoT_Security

personales. Además, la interoperabilidad es un desafío importante en el IoT, ya que los dispositivos y sistemas de diferentes fabricantes a menudo no son compatibles entre sí.

1.5.1.1 LA INTELIGENCIA ARTIFICIAL

Es un campo de la informática que se enfoca en desarrollar sistemas y programas capaces de realizar tareas que, en condiciones normales, requerirían inteligencia humana. Estos sistemas emplean algoritmos y modelos matemáticos para aprender de datos y realizar decisiones o tareas de manera autónoma. La IA[6] abarca una variedad de técnicas, como el aprendizaje automático, el procesamiento del lenguaje natural, la visión por computadora y la robótica.

Ha revolucionado en los sectores como el comercio electrónico y la publicidad, mejorando la personalización y la eficiencia. A medida que la IA avanza, surgen desafíos éticos, como la privacidad de los datos y la toma de decisiones automatizadas. No obstante, la IA sigue siendo un campo en constante crecimiento y promete un futuro lleno de avances y cambios significativos en diversos aspectos de la sociedad.

Se puede dividir en dos categorías principales: la AI simbólica y la AI conectivista. La AI simbólica se basa en la representación y el razonamiento simbólico, y se utiliza para tareas como el procesamiento del lenguaje natural y el razonamiento lógico. La AI conectivista, por otro lado, se basa en la conectividad y el aprendizaje automático, y se utiliza para tareas como el reconocimiento de patrones y el aprendizaje de representaciones.

[6] Gómez, WOA La inteligencia artificial y su incidencia en la educación: Transformando el aprendizaje para el siglo XXI. En: Revista Internacional de Pedagogía e Innovación Educativa. 3, n.º 2 (2023); Pag. 217-229. Disponible en: https://editic.net/ripie/index.php/ripie/article/view/133/114

Tiene una amplia variedad de aplicaciones, incluyendo la atención médica, la educación, la fabricación, la energía, y el transporte. En la atención médica, la AI se utiliza para el diagnóstico y el tratamiento de enfermedades, y en la educación, se utiliza para la personalización del aprendizaje y el seguimiento del progreso de los estudiantes. En la fabricación, la AI se utiliza para la automatización de procesos y la predicción de fallos, y en la energía, se utiliza para la optimización de la generación y el consumo de energía. En el transporte, la AI se utiliza para la conducción autónoma y la gestión del tráfico.

Sin embargo, la AI también presenta una serie de desafíos y riesgos, incluyendo la seguridad cibernética, la privacidad, y el impacto social y económico. Es importante abordar estos desafíos y riesgos para aprovechar al máximo el potencial de la AI.

1.6 MARCO CONCEPTUAL

La ciberseguridad se centra en la protección de sistemas, redes, datos y dispositivos contra amenazas cibernéticas. Para comprender las tendencias actuales en este campo, es fundamental establecer un marco conceptual que abarque los conceptos clave y las áreas de interés.

Para el análisis de estas tendencias en ciberseguridad[7] implica una comprensión profunda de cada área, así como la identificación de amenazas y oportunidades. Es esencial que las organizaciones y los profesionales de la ciberseguridad estén al tanto de estas tendencias y evolucionen sus estrategias y medidas de seguridad para mantenerse al día con el panorama de amenazas en constante cambio. Además, la colaboración entre sectores público y privado es crucial para abordar de manera efectiva los desafíos de ciberseguridad asociados con estas tendencias.

[7] Duque, AR Tendencias en Ciberseguridad en Latinoamérica. {En línea}. 2022, 6 de julio. {15 febrero del 2024}. Disponible en: https://revistaempresarial.com/tecnologia/seguridad-informatica/tendencias-en-ciberseguridad-en-latinoamerica/

Los desafíos en el campo de la ciberseguridad son cada vez más complejos y constantemente cambiantes debido a la rápida evolución de la tecnología y las tácticas de los ciberdelincuentes. Uno de los principales desafíos es la sofisticación de los ataques cibernéticos, que incluyen el auge de ataques de ransomware altamente destructivos y la aparición de amenazas impulsadas por inteligencia artificial que pueden eludir sistemas de seguridad tradicionales. Los actores maliciosos están adoptando enfoques más avanzados y específicos, lo que requiere una respuesta igualmente avanzada por parte de las organizaciones.

Un segundo desafío crucial es la creciente superficie de ataque, especialmente con la proliferación de dispositivos IoT. Cada nuevo dispositivo conectado representa una posible puerta de entrada para los atacantes, y muchas veces estos dispositivos carecen de la seguridad adecuada. Gestionar y proteger una red cada vez más compleja y diversa se ha vuelto una tarea abrumadora para las organizaciones.

El tercer desafío importante es la escasez de talento en ciberseguridad. La demanda de profesionales altamente capacitados en ciberseguridad supera con creces la oferta, lo que significa que muchas organizaciones luchan por encontrar y retener expertos en seguridad cibernética. Esto puede dejar a las empresas vulnerables a ataques, ya que no cuentan con el personal necesario para gestionar adecuadamente la seguridad de sus activos digitales. En resumen, los desafíos en ciberseguridad son multidimensionales y requieren una combinación de tecnología avanzada, concienciación y desarrollo de talento para hacer frente a las amenazas en constante evolución.

1.7 MARCO HISTÓRICO

A lo largo de los años[8], el ransomware ha pasado de ser un simple malware a un negocio multimillonario, con ataques dirigidos y extorsiones a gran escala, el

[8] Albors, J. Tendencias 2021: ¿Qué nos depara un futuro incierto en materia de ciberseguridad? {En línea}. {10 febrero dej 2024}. Disponible en: https://blogs.protegerse.com/2020/12/04/tendencias-2021-que-nos-depara-un-futuro-incierto-en-materia-de-ciberseguridad

malware ha existido desde la década de 1980, pero no fue hasta la llegada de las PC con Windows en la década de 1990 que la amenaza del malware apareció repentinamente en las computadoras. La inteligencia artificial se ha utilizado tanto en defensa como en ataques, mejorando la detección y la respuesta, pero también permitiendo ataques más sofisticados. El IoT ha introducido una amplia gama de dispositivos conectados, creando nuevos vectores de ataque y desafíos de seguridad.

La interconexión de estos tres elementos ha creado un panorama de ciberseguridad cada vez más complejo. La detección y prevención de ataques de ransomware requieren soluciones más avanzadas, aprovechando la inteligencia artificial para identificar patrones de comportamiento malicioso. Además, la expansión del IoT ha aumentado la superficie de ataque, lo que exige una atención especial a la seguridad de estos dispositivos.

1.8 ANTECEDENTES O ESTADO ACTUAL

A continuación, mostraremos el avance sobre Ransomware, IA, IoT:

Ransomware ha experimentado una transformación significativa en las últimas décadas. Los primeros ataques eran rudimentarios y se dirigían a usuarios individuales. Sin embargo, se ha producido una transición hacia ataques más dirigidos, a menudo involucrando ransomware como servicio (RaaS). Los atacantes buscan víctimas con la capacidad de pagar rescates sustanciales, como empresas y organizaciones gubernamentales. Esto ha creado un mercado negro próspero de ransomware y una creciente presión para mejorar la prevención y la respuesta.

Por su parte la IA, ha influido en ambas partes del juego de la ciberseguridad. Se utiliza para fortalecer las defensas, identificar amenazas en tiempo real y automatizar la respuesta a incidentes. Simultáneamente, los ciberdelincuentes emplean la IA para perfeccionar sus tácticas y eludir sistemas de seguridad

convencionales. La competencia en torno a la IA en el campo de la ciberseguridad sigue siendo feroz.

Por último, IoT ha agregado otra dimensión a la ciberseguridad. La proliferación de dispositivos conectados ha ampliado la superficie de ataque, ya que muchos de estos dispositivos carecen de medidas de seguridad adecuadas. Los ataques a dispositivos IoT, como cámaras de seguridad y routers, son cada vez más comunes, lo que subraya la necesidad de regulaciones y estándares de seguridad más estrictos.

1.9 MARCO CIENTÍFICO O TECNOLÓGICO

Ransomware: Una de las principales razones de la propagación[9] de este tipo de amenazas se debe a los enormes beneficios económicos de los atacantes. Esto ha provocado el surgimiento de grupos dedicados a su desarrollo, así como un aumento de los recursos dedicados a la creación de ciberdelincuentes, principalmente por los importantes beneficios económicos que obtienen. Por estos motivos, se recomienda revisar las políticas de seguridad y planes de emergencia.

Método de infección[10]

El principal método de transmisión es a través de caballos de Troya en sitios web maliciosos o legítimos que han sido comprometidos por ciberdelincuentes. El vector de infección más común son las páginas web con contenido pornográfico o de juegos, por lo que cuando los usuarios seleccionan uno de los anuncios, son redirigidos a otra página infectada que está infectada con ransomware u otro malware. El segundo modo de transmisión son los correos electrónicos masivos, los

[10] Frenz, Christopher M. & Díaz, Christian L. Guía Contra Ataques Ransomware. {En línea}. 2019. {20 febrero del 2024}. Disponible en: https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf

mensajes instantáneos, los enlaces a sitios infectados en las redes sociales o las descargas de archivos compartidos (P2P). Otra técnica por destacar es el uso de ataques de Protocolo de Escritorio Remoto (RDP) utilizando vulnerabilidades del sistema o ataques de fuerza bruta. Si el ataque tiene éxito, los delincuentes pueden cifrar los datos en el servidor y luego exigir un rescate por la contraseña.

El malware[11] hace una búsqueda de los archivos que va a cifrar y se crea una o varias conexiones con el sistema de control, lo cual realiza a través de las diferentes redes y sistemas, para que desde un servidor central se pueda administrar el malware en todo su sentido (robo de información, ocultamiento, nuevos accesos, cifrado, entre otros) y finalmente, el atacante establece el mecanismo de cobrar la extorsión por la información cifrada y que no pudo ser recuperada por la organización (ver Figura1)

Figura 1.Esquema del funcionamiento ransomware

Fuente: Revista UIS Ingenierías. Revista UIS Ingenierías. marzo 2020. doi:1 https://doi.org/10.18273/revuin.v19n3-2020013

[11] Osorio-Sierra, A., Mateus-Hernández, MJ, & Vargas-Montoya, HF Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. {En línea}. 2020. {Fecha de consulta: 22 de octubre de 2024}. Disponible en: https://doi.org/10.18273/revuin.v19n3-2020013

Un ransomware puede llegar a la víctima de diferentes formas (ver Figura 2), los vectores de ataques pueden ser consolidados en la medida que los servicios informáticos estén activos, dichos vectores pueden ejecutarse de acuerdo con el comportamiento o falta de conocimiento de empleados para la identificación de archivos maliciosos.

Figura 2.Clasificación de vectores de ataque

Fuente: Revista UIS Ingenierías. Revista UIS Ingenierías. marzo 2020. doi: https://doi.org/10.18273/revuin.v19n3-2020013

Inteligencia artificial: Se utiliza de diversas maneras para detectar, prevenir y responder a amenazas cibernéticas.

Estas son algunas de las técnicas IA[12] importante:

- **Aprendizaje automático (Machine Learning):** Se emplea para analizar grandes conjuntos de datos y detectar patrones anómalos que puedan indicar una amenaza. Los algoritmos de aprendizaje automático pueden

[12] Samtani, S., Kantarcıoğlu, M., Chen, H. Pioneros en la inteligencia artificial para la disciplina de ciberseguridad. {En línea}. 2020. {09 mayo de 2024}. Disponible en: https://dl.acm.org/doi/pdf/10.1145/3430360

clasificar comportamientos normales y anómalos en el tráfico de red y en el comportamiento de los usuarios (ver Figura 3).

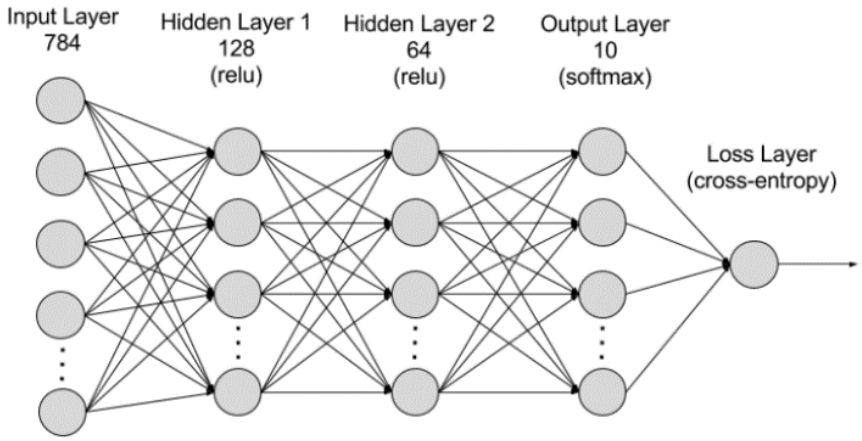
Figura 3. Tipos de aprendizaje automático

Fuente: Algotive 2022 Machine learning: ¿Qué es el aprendizaje automático y cómo funciona? https://www.algotive.ai/es-mx/blog/machine-learning-que-es-el-aprendizaje-autom%C3%A1tico-y-c%C3%B3mo-funciona.

- **Redes neuronales:** Las redes neuronales profundas (deep learning) pueden utilizarse para el análisis de tráfico de red y la detección de malware. Son especialmente efectivas en la identificación de amenazas complejas y en constante evolución.

Un número, denominado peso, representa las conexiones entre un nodo y otro. El peso es un número positivo si un nodo estimula a otro, o negativo si un nodo suprime a otro. Los nodos con valores de peso más altos tienen mayor influencia en los demás nodos (ver Figura 4).

Figura 4.Arquitectura de una red neuronal AI



Fuente: AWS. Amazon Web Services- ¿Qué es una red neuronal? - Explicación de las redes neuronales artificiales, Inc. https://aws.amazon.com/es/what-is/neural-network/.

- Procesamiento del lenguaje natural (NLP):[13] El NLP se utiliza para analizar texto y detectar amenazas en conversaciones en línea, correos electrónicos y redes sociales. Puede identificar discursos de odio, estafas y otros tipos de comportamiento malicioso.

- Análisis de comportamiento: La IA puede rastrear y analizar el comportamiento de los usuarios y sistemas para detectar actividades sospechosas. Por ejemplo, la detección de acceso no autorizado a sistemas o intentos de escalada de privilegios.

- Automatización de respuestas: La IA también se utiliza para tomar medidas en tiempo real frente a amenazas. Esto incluye la capacidad de bloquear

[13] Alrfai, MM, Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M. y Almaiah, MA La influencia de la inteligencia artificial en la eficiencia de los AIS: efecto moderador de la ciberseguridad. {En línea}. 2023. {29 enero del 2024}. Disponible en: https://www.researchgate.net/publication/373139284_The_influence_of_artificial_intelligence_on_the_AISs_efficiency_Moderating_effect_of_the_cyber_security

automáticamente direcciones IP maliciosas, detener ataques DDoS y tomar medidas para mitigar una amenaza antes de que cause daño significativo.

- Inteligencia cibernética: La IA ayuda a recopilar y analizar grandes cantidades de datos de amenazas, como indicadores de compromiso (IoCs) y patrones de ataque. Esto permite a los equipos de seguridad anticiparse a amenazas futuras y prepararse para ellas.

Internet de las cosas (IoT): ha introducido una serie de vulnerabilidades y riesgos de seguridad que pueden afectar a la privacidad, la integridad y la disponibilidad de los datos y sistemas.

Es importante tener en cuenta que las vulnerabilidades de IoT evolucionan constante y periódicamente se descubren nuevas vulnerabilidades, a continuación, describimos cada una (ver Tabla 1).

Tabla 1. Principales vulnerabilidades del IoT

Vulnerabilidad	Descripción
Privacidad	Los dispositivos IoT se conectan a redes inalámbricas sin cifrar, lo que los hace susceptibles a ataques de intercepción y manipulación.
Autorización	Algunos dispositivos IoT no requieren autenticación para conectarse a una red o para usar sus funciones, lo que facilita que los atacantes los descubran y los manipulen.
Cifrado	La mayoría no cifran las comunicaciones entre sí o con otros dispositivos, lo que facilita que los atacantes intercepten y manipulen las comunicaciones.
Interfaz web	No se cuentan con mecanismos de supervisión adecuados, lo que dificulta la detección y respuesta a los ataques.

Software	Algunos dispositivos con versiones antiguas no reciben actualizaciones de seguridad regulares, lo que significa que las vulnerabilidades conocidas no se corrigen y los dispositivos siguen siendo susceptibles a ataques.

Fuente: Propia

1.10 MARCO LEGAL

La Ley 1273 del 5 de enero de 2009[14] de Colombia es una legislación que aborda los delitos informáticos y la protección de la información electrónica. A continuación, se presenta un resumen de los artículos de esta ley:

Artículo 1: Define los delitos informáticos como aquellas conductas que afectan la confidencialidad, integridad, disponibilidad y veracidad de la información y los sistemas informáticos. Establece que estos delitos pueden ser castigados con sanciones penales y económicas.

Artículo 2: Establece que la ley se aplica tanto a personas naturales como a personas jurídicas que cometan delitos informáticos en el territorio colombiano.

Artículo 3: Define los tipos de delitos informáticos que esta ley busca abordar, como el acceso abusivo a sistemas informáticos, la interceptación ilegal de comunicaciones electrónicas, el daño informático y la falsedad informática.

Artículo 6: Establece sanciones penales para quienes cometan delitos informáticos, que pueden incluir multas y penas de prisión.

[14] Congreso de Colombia. Ley 1273 de 2009. {En línea}. 2009. {10 febrero del 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Artículo 7: Se refiere a la prescripción de los delitos informáticos, estableciendo un plazo en el que pueden perseguirse legalmente.

Artículo 8: Hace hincapié en la importancia de la cooperación internacional en la investigación y persecución de delitos informáticos.

Artículo 9: Aborda la protección de la información en el ámbito gubernamental y establece medidas de seguridad para garantizar la integridad y confidencialidad de los datos.

Artículo 10: Se refiere a la competencia de las autoridades judiciales y fiscales en la investigación y persecución de los delitos informáticos.

La Ley de Fraude y Abuso Informático (CFAA, por sus siglas en inglés)[15] es una legislación de los Estados Unidos que aborda los delitos informáticos y el acceso no autorizado a sistemas informáticos. Se centra en la protección de sistemas informáticos y datos contra el acceso no autorizado y el uso malicioso. Las disposiciones de la CFAA tienen como objetivo combatir el cibercrimen y proteger la seguridad de la información y los sistemas informáticos en los Estados Unidos. Los artículos mencionados anteriormente son algunos de los principales componentes de esta legislación, diseñada para abordar una amplia gama de delitos informáticos y actividades relacionadas con el acceso no autorizado a computadoras y sistemas.

A continuación, se presenta un resumen de algunos de sus artículos:

- Artículo 18 USC 1030(a): Este artículo prohíbe el acceso no autorizado a computadoras y sistemas informáticos. Establece que es ilegal acceder

intencionalmente a una computadora sin autorización y obtener información desde ella.

- Artículo 18 USC 1030(b): Este artículo prohíbe el acceso no autorizado con la intención de cometer fraude, obtener información valiosa o causar daño a una computadora protegida.

- Artículo 18 USC 1030(c): Este artículo aborda el tráfico de contraseñas robadas o acceso no autorizado a computadoras protegidas. Prohíbe la venta, tráfico o posesión de contraseñas o información de acceso no autorizada.

- Artículo 18 USC 1030(e): Establece que las penas por delitos informáticos pueden ser graves, con sanciones que incluyen multas y tiempo en prisión.

- Artículo 18 USC 1030(g): Aborda la obtención no autorizada de información protegida por el gobierno federal y establece sanciones para quienes cometan estos actos.

DESARROLLO

1.10.1 VULNERABILIDADES Y RIESGOS DE SEGURIDAD EN DISPOSITIVOS IOT

El Internet de las Cosas (IoT)[16] tiene una amplia gama de sectores de aplicación, y la seguridad es fundamental en todos ellos debido a las implicaciones de la interconexión masiva de dispositivos. Algunos de los sectores más destacados de aplicación de IoT incluyen:

1. **Salud y Asistencia Médica:**[17] En la atención médica, IoT se utiliza para el seguimiento de pacientes, dispositivos médicos conectados y la gestión de datos de salud. La seguridad es crucial para proteger la privacidad de los datos de salud y garantizar que los dispositivos médicos no sean vulnerables a ataques que puedan poner en riesgo la vida de los pacientes.

2. **Manufactura Inteligente:** La IoT se emplea para la monitorización de maquinaria, la optimización de procesos de fabricación y la gestión de la cadena de suministro. La seguridad es esencial para prevenir interrupciones en la producción y proteger la propiedad intelectual.

3. **Ciudades Inteligentes**: Las ciudades utilizan IoT para la gestión de tráfico, la eficiencia energética, la seguridad y la mejora de los servicios públicos. La seguridad es vital para evitar ataques que puedan interrumpir los servicios críticos y la privacidad de los ciudadanos.

[16] Kouicem, DE, Bouabdallah, A., & Lakhlef, H. Seguridad de Internet de las cosas: una encuesta de arriba hacia abajo. En: Computer Networks . 141 (2018); Pág. 199-221. Disponible en: https://www.researchgate.net/publication/323912995_Internet_of_Things_Security_a_top-down_survey

[17] Dang, LM, Piran, MJ, Han, D., Min, K., & Moon, H. Una encuesta sobre Internet de las cosas y computación en la nube para la atención médica. En: Electronics. Vol. 8, No. 7 (2019); Pág. 768.

4. **Agricultura Inteligente:** IoT se aplica en la agricultura para el monitoreo de cultivos, la gestión de ganado y la automatización de procesos agrícolas. La seguridad es importante para garantizar la integridad de los datos y prevenir daños a los activos agrícolas.

5. **Automoción Conectada:** Los vehículos conectados utilizan IoT para la navegación, el entretenimiento y la seguridad. La seguridad es crítica para prevenir el acceso no autorizado a sistemas del automóvil y la manipulación de datos de navegación.

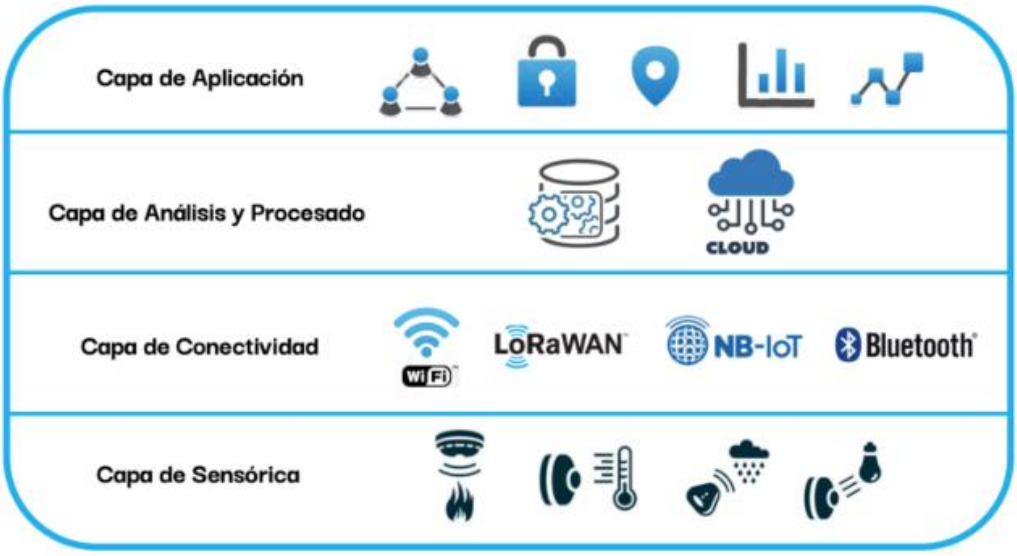
6. **Hogar Inteligente:** En los hogares, IoT se usa para la automatización de viviendas, control de dispositivos y seguridad. La seguridad es esencial para proteger la privacidad de los residentes y evitar que los dispositivos se conviertan en puntos de entrada para ciberataques.

7. **Energía:** IoT se utiliza en la gestión de redes eléctricas, agua y gas, lo que lo hace vital para mantener la continuidad de los servicios y proteger la infraestructura crítica.

1.10.2 CAPAS DE LA ARQUITECTURA IOT Y LA IMPORTANCIA DE SU SEGURIDAD

Existen las siguientes arquitecturas propuestas destinadas a proporcionar una comprensión más clara del concepto de Internet de las cosas (ver Figura 5).

Figura 5.Capas de la arquitectura IoT.



Fuente: Ballester O. 5 de enero de 2022. Internet of things, IoT. Istec Digital. https://www.istecdigital.es/internet-of-things-iot/. Published

1. Capa de aplicación: es crucial porque ofrece funciones personalizadas y aplicaciones basadas en datos recopilados por dispositivos de capas inferiores. Conecta a los usuarios con el ecosistema IoT, permitiendo aplicaciones que aprovechan la información de los dispositivos conectados. La seguridad es fundamental en esta capa, ya que garantiza la privacidad del usuario, la seguridad de los datos y la confiabilidad del sistema.Ofrece una gran variedad de servicios y aplicaciones, que abarcan desde el hogar inteligente hasta la industria. Si bien permite una amplia gama de servicios que aumentan la eficiencia, la comodidad y la toma de decisiones, esta diversidad también plantea desafíos de seguridad significativos que deben mitigarse adecuadamente.

La importancia de tener seguridad en la capa de aplicaciones es mejorar a los usuarios finales y sus datos. En este caso, una brecha de seguridad en esta capa puede tener graves consecuencias, desde la pérdida de privacidad hasta el uso indebido de la información para actividades maliciosas. Además, una capa de aplicación segura ayuda a fomentar la confianza del usuario y el éxito general del ecosistema de IoT. En conclusión, la seguridad a nivel de aplicación no es

simplemente un imperativo sino más bien un requisito para garantizar la integridad y confiabilidad de los servicios que IoT brinda a sus clientes.

2. Capa de análisis y procesado: juega un papel fundamental a la hora de proporcionar una infraestructura que facilite la gestión y coordinación eficiente de dispositivos, datos y servicios dentro del ecosistema de IoT.Esta capa actúa como puente entre las capas inferiores como la percepción y las redes y las capas superiores como las aplicaciones.Su diseño y seguridad son fundamentales para garantizar la funcionalidad y confiabilidad de toda la red de IoT.
Las violaciones de seguridad en esta capa pueden tener consecuencias importantes en toda la red, desde la manipulación de datos hasta la interrupción del servicio. Implementar medidas de seguridad sólidas, como cifrado, autenticación sólida y monitoreo continuo, es fundamental para construir una infraestructura de IoT sólida y confiable. La confianza en la integridad de la plataforma es esencial para facilitar la adopción masiva de IoT y maximizar sus beneficios potenciales.

3. Capa de conectividad: Es un componente importante que facilita la comunicación continua entre dispositivos conectados, asegurando una transferencia de datos eficiente y confiable. Esta capa se encuentra entre la capa de percepción, que genera los datos, y la capa de plataforma, que es responsable de gestionar y procesar esos datos. La seguridad en la capa de conexión es esencial para proteger la integridad, confidencialidad y disponibilidad de la información en tránsito y evitar posibles ataques y vulnerabilidades. Sirve de puente entre los dispositivos físicos y la infraestructura de red. Las brechas de seguridad en esta capa pueden provocar ataques de escucha, manipulación de datos y toma de control no autorizada de dispositivos, comprometiendo la integridad de toda la red de IoT. Por lo tanto, implementar medidas de seguridad sólidas, como cifrado, autenticación y monitoreo continuo, es fundamental para establecer conexiones de IoT seguras y confiables. Esto no sólo protege los datos y los dispositivos, sino que también aumenta la confianza en la adopción generalizada de soluciones de IoT.

4. Capa de sensorial: Constituye la base del ecosistema y es la interfaz entre los mundos físico y digital. Esta capa consta de una red de sensores y actuadores que recopilan datos del entorno físico y los convierten en información digital para su posterior procesamiento. La seguridad en la capa de registro es fundamental porque los dispositivos de esta capa son puertas de entrada a datos críticos y cualquier violación puede comprometer la integridad y confidencialidad de la información recopilada. Es la base de IoT porque proporciona la entrada de datos que impulsa todo el sistema. La importancia de esta capa de seguridad es garantizar la confiabilidad y validez de los datos recopilados, así como proteger la privacidad de la información sensible. La implementación de sólidas prácticas y tecnologías de seguridad a nivel de percepción sienta una base sólida para un ecosistema de IoT confiable y resistente a las amenazas.

1.10.2.1 AMENAZAS DE SEGURIDAD EN LAS CAPAS IOT

El Internet de las Cosas (IoT) presenta amenazas de seguridad en varias capas. En la capa de dispositivos, las debilidades en autenticación y contraseñas débiles permiten el acceso no autorizado. En la capa de comunicación, la falta de encriptación facilita la interceptación de datos. La capa de plataforma puede ser vulnerable a problemas de autenticación y autorización, mientras que la seguridad en la nube es esencial. La capa de aplicaciones enfrenta vulnerabilidades de software y ataques DDoS. En la capa de usuarios finales, la falta de conciencia de seguridad es un problema. Abordar estas amenazas requiere medidas de seguridad sólidas en todas las capas, como autenticación fuerte, cifrado y actualizaciones regulares del firmware.

Aquí se detallan algunas de las amenazas comunes en cada capa del IoT:

1. **Capa de Dispositivos[18]:**

Esta capa incluye los sensores y actuadores que recopilan y transmiten datos desde el entorno físico al sistema IoT, los dispositivos IoT suelen ser pequeños y con recursos limitados, como microcontroladores.
La seguridad en esta capa es esencial para evitar la manipulación de datos y el acceso no autorizado.

2. **Capa de Comunicación:**

Aquí se gestionan las conexiones entre dispositivos IoT y la infraestructura de red, Protocolos de comunicación como MQTT y CoAP se utilizan para transmitir datos de manera eficiente.
La seguridad en esta capa implica la encriptación de datos y la autenticación de dispositivos.

3. **Capa de Plataforma:**

Esta capa se encuentra en la nube o en servidores locales y gestiona la recopilación y procesamiento de datos de IoT, Ofrece herramientas para el almacenamiento, análisis y visualización de datos.
La seguridad en esta capa involucra el control de acceso y la protección de datos almacenados.

4. **Capa de Aplicación:**

[18] Singh, D., Tripathi, G. y Jara, AJ Un estudio sobre Internet de las cosas: visión, arquitectura, desafíos y servicios de futuro. {En línea}. 2014. {28 abril de 2024}. Disponible en: https://ieeexplore.ieee.org/ielaam/6245516/8128656/7562568-aam.pdf

Aquí se desarrollan las aplicaciones que aprovechan los datos generados por los dispositivos IoT, se incluyen aplicaciones móviles, aplicaciones web y sistemas de control.
La seguridad implica proteger las aplicaciones de vulnerabilidades y ataques.

1.10.2.2 VULNERABILIDADES Y AMENAZAS IOT

Las vulnerabilidades y amenazas en el Internet de las Cosas (IoT) representan un desafío crítico en el mundo de la tecnología. IoT se refiere a la interconexión de dispositivos cotidianos a través de Internet, y esta interconexión plantea preocupaciones de seguridad significativas, las vulnerabilidades más comunes en IoT incluyen contraseñas débiles o predeterminadas, falta de cifrado de datos, software y firmware desactualizados, interfaces web inseguras, API sin protección y controles de acceso inadecuados. Estas debilidades pueden permitir a los atacantes acceder a dispositivos, robar datos o interrumpir su funcionamiento.

Las amenazas [19]incluyen ataques de denegación de servicio distribuido (DDoS) utilizando dispositivos comprometidos, la posibilidad de manipulación física de dispositivos y la suplantación de dispositivos legítimos. También se plantean preocupaciones de privacidad debido a la recopilación de datos personales por parte de dispositivos IoT.

¿Cómo afectan las vulnerabilidades de los dispositivos IoT a los usuarios?

Los ciberdelincuentes buscan vulnerabilidades en dispositivos de IoT para lanzar ataques contra organizaciones y usuarios finales. Ejemplos de cómo las vulnerabilidades de los dispositivos IoT pueden afectar a los usuarios incluyen:

[19] Internet de las cosas (IoT): oportunidades, problemas y desafíos hacia un futuro inteligente y sostenible (2020) Revista de Producción Más Limpia, 274, art. No. 122877 https://dialnet.unirioja.es/descarga/articulo/8914181.pdf

- **Movimiento lateral de la red:** los ciberdelincuentes pueden utilizar la infracción inicial de un dispositivo vulnerable para penetrar más profundamente en las redes corporativas. Un atacante busca explotar una vulnerabilidad en una máquina y luego aumentar sus privilegios. Luego utilizan el movimiento lateral para alcanzar datos críticos y propagar malware a través de una red.

- **Botnets de IoT:** son grandes redes de dispositivos, como enrutadores, para lanzar ciberataques a gran escala, como ataques de denegación de servicio distribuido (DDoS). Las botnets agrupan varios dispositivos infectados administrados desde un servidor de comando y control (C&C) . Por ejemplo, en 2016, la botnet Mirai eliminó una serie de servicios y sitios web importantes, incluidos servicios de juegos. Mirai apuntó a dispositivos inseguros utilizando un código de botnet que se liberó para que otros piratas informáticos lo explotaran.

- **Botnets en evolución:** el crecimiento de IoT plantea el riesgo de que los botnets evolucionen y se conviertan en una amenaza aún más importante para los usuarios. Esto podría suceder a través de tecnologías de intercambio de archivos peer-to-peer (P2P) que permiten a un atacante conectar dispositivos sin necesidad de un servidor central, lo que hace que la prevención sea casi imposible.

- **Dispositivos domésticos:** IoT está impregnando cada vez más el hogar con electrodomésticos conectados, asistentes digitales, dispositivos portátiles, rastreadores de salud y más. Las vulnerabilidades del servicio de IoT pueden presentar nuevos puntos de entrada a otros dispositivos conectados a redes domésticas, como portátiles y ordenadores.

- **Problemas de dispositivos existentes:** los atacantes pueden apuntar a dispositivos de IoT con problemas existentes conocidos para acceder a las redes internas. Luego pueden lanzar ataques, como ataques de Re vinculación del sistema de nombres de dominio (DNS), para extraer datos de redes y dispositivos conectados a redes domésticas o corporativas.

Principales vulnerabilidades de dispositivos IoT[20]

Los dispositivos de IoT pueden verse comprometidos a través de una amplia gama de vulnerabilidades. Las principales vulnerabilidades de IoT incluyen:

1. **Contraseñas débiles o codificadas:** Las contraseñas débiles o codificadas se encuentran entre los métodos más frecuentes que utilizan los atacantes para comprometer los dispositivos de IoT. Las contraseñas débiles y reutilizadas, que son cortas o fáciles de adivinar, son fáciles de descifrar para los atacantes, que luego utilizan para comprometer dispositivos y lanzar ataques a gran escala.

2. **Redes inseguras:** Las redes inseguras facilitan que los ciberdelincuentes aprovechen las debilidades de los protocolos y servicios que se ejecutan en los dispositivos IoT. Una vez que han explotado una red, los atacantes pueden violar datos confidenciales o sensibles que viajan entre los dispositivos del usuario y el servidor. Las redes inseguras son particularmente susceptibles a los ataques de intermediario (MITM) , cuyo objetivo es robar credenciales y autenticar dispositivos como parte de ataques cibernéticos más amplios.

3. Interfaces de ecosistemas inseguras: Las interfaces inseguras del ecosistema, como las interfaces de programación de aplicaciones (API) y las aplicaciones

[20] Singh, D., Tripathi, G. y Jara, AJ Un estudio sobre Internet de las cosas: visión, arquitectura, desafíos y servicios de futuro. {En línea}. 2014. {Fecha de consulta: 22 de octubre de 2024}. Disponible en: https://ieeexplore.ieee.org/ielaam/6245516/8128656/7562568-aam.pdf

móviles y web, permiten a los atacantes comprometer un dispositivo. Las organizaciones necesitan implementar procesos de autenticación y autorización que validen a los usuarios y protejan sus interfaces móviles y en la nube. Las prácticas herramientas de identidad ayudan al servidor a diferenciar los dispositivos válidos de los usuarios malintencionados.

4. Mecanismos de actualización inseguros: Los dispositivos con procesos de actualización inseguros corren el riesgo de instalar código, firmware y software maliciosos o no autorizados. Las actualizaciones corruptas pueden comprometer los dispositivos de IoT, lo que podría ser fundamental para las organizaciones de los sectores energético, sanitario e industrial. Las actualizaciones deben ser seguras y en canales cifrados, mientras que todo el software debe estar validado y aprobado.

5. Componentes inseguros u obsoletos: El ecosistema de IoT puede verse comprometido por vulnerabilidades de código y software y sistemas heredados. El uso de componentes inseguros u obsoletos, como código fuente abierto o software de terceros, puede presentar vulnerabilidades que amplían la superficie de ataque de una organización.

6. Falta de protección adecuada de la privacidad: Los dispositivos de IoT a menudo recopilan datos personales que las organizaciones necesitan almacenar y procesar de forma segura para cumplir con diversas regulaciones de privacidad de datos. No proteger estos datos puede exponerlos a multas, pérdida de reputación y pérdida de negocios. No implementar una seguridad suficiente puede provocar fugas de datos que pongan en peligro la privacidad del usuario.

7. Transferencia y almacenamiento de datos inseguros: Los datos que los dispositivos de IoT reciben o transmiten a través de las redes deben protegerse y restringirse frente a usuarios no autorizados. Esto es fundamental para mantener la

integridad y confiabilidad de las aplicaciones de IoT y los procesos de toma de decisiones de las organizaciones.

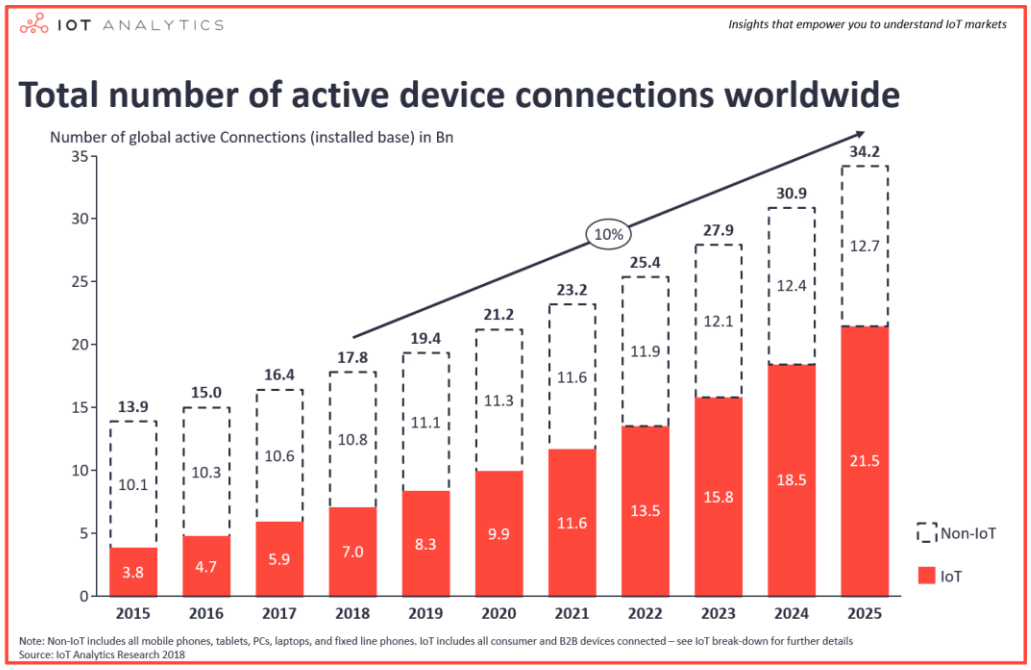
8. Gestión inadecuada del dispositivo: No gestionar adecuadamente los dispositivos a lo largo de su ciclo de vida los deja expuestos a la explotación de vulnerabilidades, incluso si ya no están en uso. Las empresas deben comprender qué activos o dispositivos están conectados a sus redes y administrarlos adecuadamente. Los dispositivos no autorizados o inactivos pueden proporcionar a los atacantes acceso a redes corporativas, permitiéndoles robar o interceptar datos confidenciales. Esto hace que el descubrimiento y la identificación de dispositivos de IoT sean cruciales para monitorear y proteger los dispositivos.

9. Configuración predeterminada insegura: Los dispositivos IoT, como los dispositivos personales, se envían con configuraciones predeterminadas y codificadas que permiten una configuración sencilla. Sin embargo, estas configuraciones predeterminadas son muy inseguras y fáciles de violar para los atacantes. Una vez comprometidos, los piratas informáticos pueden explotar las vulnerabilidades en el firmware de un dispositivo y lanzar ataques más amplios contra las empresas.

10. Falta de endurecimiento físico: La naturaleza de los dispositivos de IoT hace que se implementen en entornos remotos en lugar de situaciones controladas que sean fáciles de gestionar. Esto hace que sea más fácil para los atacantes atacarlos e interrumpirlos, manipularlos o sabotearlos.

La cantidad de dispositivos conectados que se utilizan en todo el mundo supera ahora los 17 mil millones, y la cantidad de dispositivos IoT asciende a 7 mil millones (ver Figura 6).

Figura 6.Evolución del número de dispositivos IoT



Fuente: Lueth KL. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. IoT Analytics. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. Published 31 de mayo de 2022.

Se espera que el mercado global de Internet de las cosas (gasto del usuario final en soluciones de IoT) crezca un 37% desde 2017 hasta alcanzar los 151.000 millones de dólares. Debido a la aceleración del mercado de IoT (como se analizó anteriormente), esas estimaciones se han revisado al alza y ahora se espera que el mercado total alcance los 1.567 mil millones de dólares para 2025.

1.11.1 IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD

La aplicación de inteligencia artificial (IA) en la detección de amenazas empresariales ha transformado la ciberseguridad. Utilizando técnicas como el aprendizaje automático, las redes neuronales y el procesamiento del lenguaje natural, las soluciones de IA analizan patrones y comportamientos para identificar actividades anómalas. Estos sistemas ofrecen una detección proactiva de amenazas, superando las limitaciones de métodos tradicionales. Además, la

integración de fuentes de datos y la automatización de respuestas permiten respuestas rápidas y eficientes ante posibles violaciones de seguridad. Aunque estas técnicas mejoran la postura de seguridad, es esencial abordar desafíos como la calidad de los datos y consideraciones éticas. La IA se erige como un componente clave en la defensa cibernética, proporcionando a las empresas herramientas avanzadas para enfrentar amenazas en constante evolución.

El futuro[21] de la inteligencia artificial aplicada a la seguridad informática se vuelve interesante y necesario. El malware moderno se convierte en un desafío computacional al que hay que enfrentarse procesamiento inteligente de grandes cantidades de datos no estándar. Los ataques son cada vez más especializados y la inteligencia artificial representa un medio ideal para abordar estos problemas.

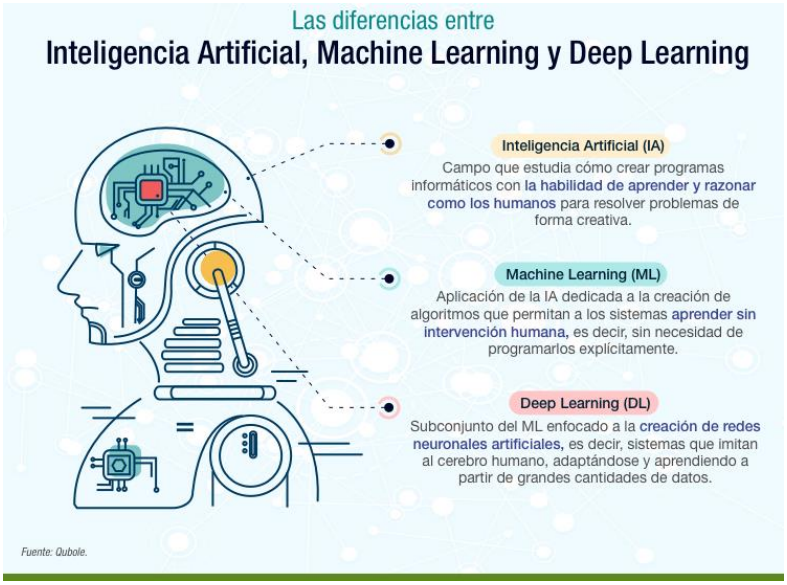
Las tendencias en materia de ciberdelincuencia son cada vez más peligrosas y sofisticadas por lo cual se debe usar si es necesario sistemas de detección de intrusos con conceptos neurobiológicos que nos permiten simular el cerebro humano para una mejor detección de ataques.

1.11.1.1 MACHINE LEARNING

Realiza un papel en la detección de amenazas cibernéticas. Al analizar patrones en grandes conjuntos de datos, los algoritmos de ML identifican comportamientos anómalos sin depender de firmas específicas. Esta técnica proactiva permite a las empresas detectar nuevas amenazas y adaptarse a evoluciones en tiempo real. La capacidad del ML para reconocer patrones complejos mejora la precisión en la identificación de amenazas, fortaleciendo la seguridad digital mediante un enfoque adaptativo y dinámico.

[21] Samtani, S., Kantarcıoğlu, M., Chen, H. Pioneros en la inteligencia artificial para la disciplina de ciberseguridad. {En línea}. 2020. {09 mayo de 2024}. Disponible en: https://dl.acm.org/doi/pdf/10.1145/3430360

Figura 7.Diferencias entre Inteligencia Artificial, 'Machine Learning' y 'Deep Learning'.



Fuente: Iberdrola. 22 de abril de 2021 DEEP LEARNING. Iberdrola. https://www.iberdrola.com/innovacion/deep-learning

1.11.1.2 DEEP LEARNING

Se destaca en la detección de amenazas cibernéticas al analizar patrones y relaciones en datos complejos. Mediante redes neuronales profundas, DL mejora la capacidad de identificar y prevenir ataques sofisticados en tiempo real. Su habilidad para reconocer patrones no lineales y adaptarse a nuevas amenazas lo convierte en una herramienta fundamental para la seguridad digital. Al permitir un análisis más profundo y preciso, el Deep Learning[22] refuerza las defensas cibernéticas, ofreciendo una respuesta avanzada y eficaz contra las amenazas emergentes en el paisaje digital en constante evolución.

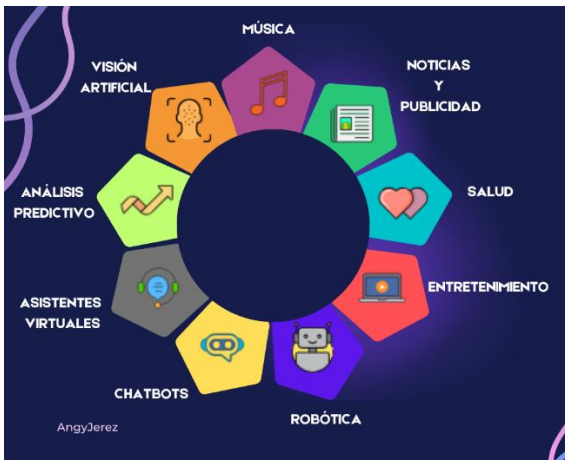
¿Cómo funciona el deep learning?

[22] Wang, X., Zhao, Y., & Pourpanah, F. (2020). Recent advances in deep learning. *International Journal of Machine Learning and Cybernetics*, *11*, 747-750.

Utiliza redes neuronales profundas para el procesamiento de datos. Compuestas por capas interconectadas, estas redes aprenden patrones complejos mediante ajustes de pesos durante el entrenamiento. La información fluye a través de capas, utilizando funciones de activación. Este enfoque permite al Deep Learning realizar tareas avanzadas sin intervención humana, como reconocimiento de patrones, procesamiento de lenguaje natural y detección de anomalías.

El aprendizaje profundo tiene una amplia gama de aplicaciones en diversos campos (ver Figura 8) lo cual hace que permita que las máquinas comprendan y generen el lenguaje humano.

Figura 8.Aplicaciones del deep learning



Fuente: propia

1.11.1.3 PROCESAMIENTO DEL LENGUAJE NATURAL

Es una rama de la inteligencia artificial que se enfoca en la interacción entre las computadoras y el lenguaje humano. Su objetivo es permitir a las máquinas entender, interpretar y generar texto de manera similar a como lo hacen los humanos. El PLN abarca tareas como reconocimiento de voz, traducción automática, análisis de sentimientos y extracción de información. Utiliza algoritmos y modelos lingüísticos avanzados para analizar patrones y estructuras en el

lenguaje, permitiendo a las máquinas procesar información textual de manera eficiente y realizar tareas cognitivas complejas en diversos contextos.

¿Cómo funciona el procesamiento de lenguaje natural?

Implica descomponer el lenguaje humano para que las máquinas lo comprendan y procesen. Comienza con la tokenización, dividiendo el texto en unidades más pequeñas. Luego, realiza análisis morfológico y sintáctico para entender la estructura gramatical. El análisis semántico busca el significado, mientras que la desambiguación resuelve posibles interpretaciones. Se identifican entidades y se analiza el sentimiento del texto. En ciertos casos, se utiliza aprendizaje automático. Este proceso permite a las máquinas realizar tareas como traducción automática, análisis de sentimientos y generación de texto, mejorando continuamente mediante la evaluación y retroalimentación.

A continuación, se visualiza en la imagen (ver Figura 9) las aplicaciones de PLN que ayuda a las máquinas a comprender el lenguaje humano y proporciona información valiosa a partir de grandes cantidades de datos de texto.

Figura 9.Aplicaciones de PLN

Fuente: propia

Herramientas para el procesamiento de lenguaje natural

- Natural Language Toolkit: Esta biblioteca de Python es ampliamente utilizada que proporciona herramientas para tareas como tokenización, etiquetado de partes del discurso y análisis sintáctico.
- Spacy: es una de las bibliotecas de procesamiento de lenguaje natural en Python que ofrece eficientes capacidades para el análisis morfológico, sintáctico y semántico, así como el reconocimiento de entidades.
- Gensim: Librería de Python especializada en modelado de temas y procesamiento de texto, útil para la creación de modelos de vectores de palabras y recuperación de información.
- IBM Watson Natural Language Understanding: Plataforma basada en la nube que ofrece análisis semántico, extracción de entidades y análisis de sentimientos, integrándose con diversas aplicaciones y entornos de desarrollo.
- TextBlob: Biblioteca sencilla de procesamiento de lenguaje natural en Python que facilita tareas como análisis de sentimientos, clasificación de texto y extracción de frases clave.

1.11.1.4 SISTEMAS DETECTORES DE INTRUSOS (IDS)

En las empresas, los Sistemas Detectores de Intrusos (IDS)[23] son esenciales para la ciberseguridad. Monitorean el tráfico de red en tiempo real, identificando patrones anómalos y posibles amenazas. Proporcionan alertas inmediatas ante intrusiones, permitiendo respuestas rápidas para mitigar riesgos. Se utilizan para proteger sistemas críticos y recursos sensibles, integrándose con sistemas de prevención para acciones automáticas. Su capacidad de análisis forense y actualización

[23] Thakkar, A. y Lohiya, R. Una revisión del avance en los conjuntos de datos de detección de intrusiones. {En línea}. 2020. {05 de abril de 2024}. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050920311121

constante de firmas fortalece la postura de seguridad. En la estrategia de seguridad empresarial, los IDS sirven como una capa vital, complementando otros sistemas y contribuyendo a la defensa integral contra amenazas cibernéticas.

Los IDS pueden ser basados en red o en host, supervisando la actividad en tiempo real y generando alertas o bloqueando el acceso ante posibles amenazas. Algunos IDS avanzados incorporan inteligencia artificial y machine learning para adaptarse a nuevas amenazas. Su función es esencial en la detección temprana de intrusiones y la protección proactiva de sistemas y datos contra ciberataques.

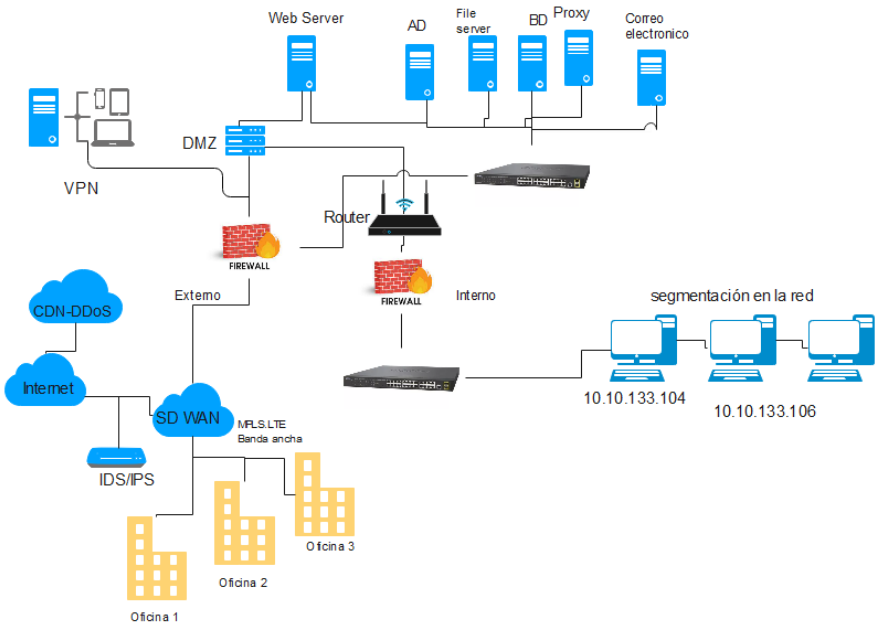
¿Dónde instalar un IDS en la red?

Uno de los lugares más comunes para implementar un IDS es cerca de un firewall. Dependiendo del tráfico a monitorear, se coloca antes o detrás del firewall para monitorear el tráfico sospechoso proveniente del interior o del exterior de la red. Cuando se coloca en interiores, el IDS debe ubicarse cerca de la DMZ. Sin embargo, la mejor práctica es utilizar defensa en capas, implementando un IDS delante del firewall en la red y un IDS detrás del firewall.

Tener una IDS (Sistema de Detección de Intrusiones) permite identificar y responder a las actividades maliciosas, puede identificar alertas en tiempo real, Web Application Firewall (WAF) en la red es una medida importante para proteger los sistemas y aplicaciones web contra amenazas y ataques específicos dirigidos a través de la capa de aplicación.

EDR es adecuado ya que nos ofrece soluciones de seguridad en los dispositivos finales (endpoints), como computadoras portátiles, estaciones de trabajo y servidores, la implementación, DMZ es un segmento de red separado que actúa como un amortiguador entre una red interna y la Internet pública. Se utiliza para aislar y proteger los recursos internos de amenazas externas colocando servidores y dispositivos a los que se debe acceder desde Internet. (ver Figura 10)

Figura 10.Estructura de una red segura



Fuente: propia

¿Como funciona una IDS?

Funciona monitoreando continuamente el tráfico de red o eventos en sistemas, utilizando técnicas como análisis de comportamiento, firmas de ataques conocidos y detección de anomalías. Analiza patrones de tráfico en busca de comportamientos inusuales o firmas específicas de ataques. Cuando se identifica una actividad sospechosa, el IDS genera alertas para notificar a los administradores de seguridad. Puede actuar en tiempo real, bloqueando o mitigando amenazas. Algunos IDS utilizan inteligencia artificial y machine learning para adaptarse a nuevas amenazas. Su función es esencial para la detección temprana y la respuesta efectiva a intrusiones.

1.12.1 EVOLUCIÓN DE LAS TÁCTICAS Y TÉCNICAS DE RANSOMWARE EN LOS ÚLTIMOS AÑOS ENTRE 2020 Y 2023

Los ataques de ransomware han sido una amenaza importante en el panorama cibernético durante varios años, y sus tácticas y técnicas han evolucionado rápidamente entre 2020 y 2023. Durante este período, los grupos de ransomware se han vuelto más sofisticados y han utilizado nuevos métodos para obtener acceso inicial a las víctimas, y empleando tácticas de extorsión más elaboradas.

Desde 2019[24], en menos de cinco años, el ransomware se ha convertido en una industria de miles de millones de dólares, una industria lucrativa no solo para los ciberdelincuentes como los afiliados de ransomware como servicio (RaaS), los intermediarios de acceso y los distribuidores de datos oscuros, sino también para todo un ecosistema de negociadores de ransomware, aseguradoras cibernéticas, respondedores de DFIR y proveedores de SaaS de filtrado de correo electrónico.

Para obtener acceso inicial a las víctimas, los grupos de ransomware han empleado varios métodos, incluidas amenazas internas, ataques de phishing y compra de acceso inicial a intermediarios. El número de corredores de acceso inicial ha aumentado significativamente en los últimos años, con más de 2.500 puestos que ofrecen acceso inicial en 2022, un aumento del 112 % en comparación con 2021.

Desde 2021, muchas filtraciones de creadores y códigos fuente de ransomware observadas han permitido a grupos con poca o ninguna experiencia crear o modificar su ransomware. Las filtraciones de código, incluidas Babuk, Conti, Lockbit3.0 y Chaos, han permitido que nuevos grupos produzcan ataques más frecuentes, cambiando así el panorama de amenazas. Sin embargo, los investigadores han observado que los grupos que utilizan estos constructores filtrados tienden a solicitar un pago de rescate más bajo. Esto puede indicar que

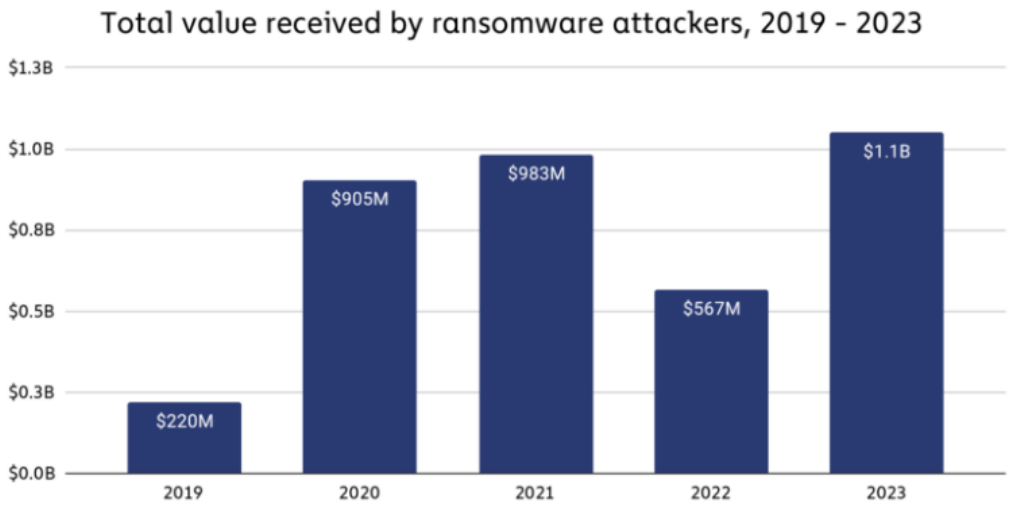
[24] Team, C. Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. {En línea}. 2024. {24 de mayo de 2024}. Disponible en: https://www.chainalysis.com/blog/ransomware-2024/

estos grupos están tratando de evitar la atención mientras prueban sus nuevas variantes.

Los factores globales y geopolíticos también han influido en la evolución de los ataques de ransomware. La pandemia de COVID-19, por ejemplo, convirtió al sector de la salud en un objetivo atractivo, mientras que las tensiones y sanciones geopolíticas han provocado un aumento de los ataques de ransomware patrocinados por el Estado.

Los pagos de ransomware en 2023 superaron la marca de los mil millones de dólares, la cifra más alta jamás observada (ver Figura 11). Aunque en 2022 se produjo una disminución en el volumen de pagos de ransomware, la línea de tendencia general de 2019 a 2023 indica que el ransomware es un problema en aumento. Tenga en cuenta que esta cifra no refleja el impacto económico de la pérdida de productividad y los costos de reparación asociados con los ataques.

Figura 11.Pagos de ransomware 2019 al 2023



Fuente: Team, C. (2024, 29 febrero). Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. Chainalysis. https://www.chainalysis.com/blog/ransomware-2024/

1.12.1.2 TECNICAS DEL RANSOMWARE

Una de las principales técnicas[25] utilizadas durante este período es el modelo Ransomware-as-a-Service (RaaS). RaaS es un servicio basado en suscripción que permite a los ciberdelincuentes menos capacitados utilizar herramientas de ransomware desarrolladas previamente para llevar a cabo ataques, lo que genera un aumento en el volumen general de ataques de ransomware.

El método de doble extorsión, en el que los atacantes no sólo cifran los datos de la víctima, sino que también los roban, amenazando con hacerlos públicos a menos que se pague un rescate. Esta estrategia ha sido empleada por varios grupos de ransomware, como REvil, Maze y DoppelPaymer, para obligar a las víctimas a pagar el rescate, aumentando el impacto financiero del ataque.

La explotación del Protocolo de escritorio remoto (RDP) ha sido una técnica común para obtener acceso inicial a una red de destino. Los atacantes utilizan ataques de fuerza bruta o explotan vulnerabilidades en RDP para obtener acceso al sistema de la víctima e implementar el ransomware.

El uso de ataques de ransomware sin archivos también se ha vuelto cada vez más popular. En estos ataques, los ciberdelincuentes aprovechan las vulnerabilidades del software o de los sistemas operativos para inyectar código malicioso sin escribir un archivo en el disco. Este enfoque dificulta que el software antivirus detecte y bloquee el ransomware, lo que permite a los atacantes cifrar los archivos de la víctima más fácilmente.

Las etapas de un ataque típico de ransomware incluyen:

[25] Frenz, Christopher M. & Díaz, Christian L. Guía Contra Ataques Ransomware. {En línea}. 2019. {20 febrero del 2024}. Disponible en: https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf

Etapa 1: los atacantes de ransomware obtienen su ingreso inicial a una organización a través de varios métodos, como correos electrónicos de phishing, explotación de vulnerabilidades de software o uso de credenciales comprometidas. Después de obtener acceso, realizan reconocimientos dentro de la red para escalar privilegios y moverse lateralmente entre dispositivos.

Etapa 2: esta etapa implica que el actor de la amenaza transfiera sin autorización los datos de una organización a sus servidores antes de que se active el ransomware. Este proceso, conocido como exfiltración de datos, prepara para más extorsiones. Los atacantes amenazan con hacer públicos los datos robados si no se paga el rescate, aprovechando posibles multas regulatorias y daños a la reputación como puntos de presión adicionales para obligar al pago.

Etapas 3 y 4: el actor de la amenaza lleva a cabo un ataque DDoS (denegación de servicio distribuido) para dañar la reputación pública de la organización objetivo o intenta extorsionar a terceros afectados por la filtración de datos. Estas técnicas pueden usarse por separado o juntas para maximizar la presión sobre la organización víctima.

Los grupos de ciberdelincuentes (ver Tabla 2) son redes organizadas de personas que participan en actividades ilegales en línea, como piratería informática, robo de identidad, filtraciones de datos y ataques de ransomware. A menudo utilizan técnicas y herramientas avanzadas para explotar vulnerabilidades y causar daños financieros y de reputación.

Tabla 2.Grupos de ciberdelincuencia

Grupos	**Descripción**
Agentes de acceso	Los agentes de acceso se centran en encontrar organizaciones con vulnerabilidades, comprometer redes y buscar la forma más fácil de acceder a ellas. Una vez

	identificados, venden estos prospectos como un paquete a grupos de ciberdelincuentes.
Desarrolladores	Los desarrolladores crean herramientas de ransomware como servicio (RaaS) para alquilarlas a otros malos actores.
Testaferros	Después de comprar la información de acceso y adquirir herramientas RaaS, un tercer grupo (el testaferro) ingresará a la red, robará o cifrará datos, ejecutará la carga útil del ransomware y exigirá el rescate.

Fuente: propia

A continuación (ver Tabla 3) Implica acceso inicial, reconocimiento, escalada de privilegios, movimiento lateral, cifrado de datos, demanda de rescate y pago. Los ciberdelincuentes aprovechan las vulnerabilidades para obtener acceso, aumentar privilegios, moverse lateralmente y cifrar datos, exigiendo un pago por descifrarlos.

Tabla 3.Cadena de ataque del ransomware

Infección	Cuando un usuario final hace clic en un enlace o archivo adjunto creado en un mensaje de correo electrónico por uno de estos actores de amenazas, se ejecuta y configura un mecanismo de persistencia.
Comando y Control	llama al servidor de comando y control del atacante, proporciona información sobre la computadora de la víctima y descarga la clave de cifrado.
Cifrado	utiliza la clave para cifrar tanto el disco duro de la víctima como todo el almacenamiento de datos accesible en la red.
Extorsión	El atacante exige un pago para que la víctima proporcione la clave de descifrado necesaria para

	recuperar los archivos. Si no paga a tiempo, corre el riesgo de perder sus archivos para siempre.
Pago	Los pagos de ransomware, que normalmente se realizan utilizando criptomonedas como Bitcoin, son difíciles, pero no imposibles, de rastrear. La mayoría de las transacciones, pero no todas, se completan con éxito.

Fuente: propia

1.12.1.3 TÁCTICAS DE RANSOMWARE

Hay una proliferación[26] de nuevos grupos de ransomware, muchos de los cuales han aprovechado las filtraciones de código y de constructores para crear o modificar su ransomware.

Linux sigue siendo el sistema operativo más popular para dispositivos integrados, restringidos y de Internet de las cosas utilizados por sectores de infraestructura críticos como la manufactura y la energía. Además, los ataques a sistemas Linux aumentaron un 75 % en 2022 y probablemente seguirán aumentando en la segunda mitad de 2023.

Phishing y de ingeniería social engañan a los usuarios para que revelen sus credenciales de inicio de sesión o descarguen malware. Los atacantes suelen utilizar correos electrónicos, mensajes de texto o publicaciones en redes sociales ingeniosamente elaborados para atraer a las víctimas a divulgar información confidencial.

[26] Sharma, P., Kapoor, S. y Sharma, R. Detección, prevención y protección de ransomware en dispositivos IoT mediante técnicas de aprendizaje automático basadas en un enfoque de análisis dinámico. {En línea}. 2022. {22 de mayo de 2024}. Disponible en: https://doi.org/10.1007/s13198-022-01793-0

¿Cómo seguirá evolucionando el ransomware?

Los ataques de ransomware[27] seguirán evolucionando y serán más sofisticados, avanzados y dirigidos. Los actores de amenazas están dominando una nueva técnica en la que los atacantes explotan las vulnerabilidades en la cadena de suministro para lanzar grandes campañas de extorsión.

Con el desarrollo de la inteligencia artificial (IA) y modelos de IA como ChatGPT, los grupos de ransomware probablemente seguirán la tendencia y utilizarán herramientas de IA como chatbots, malware desarrollado con IA, procesos automatizados y algoritmos de aprendizaje automático. Es probable que la IA ayude a los grupos a desarrollar técnicas más avanzadas y sofisticadas para evadir la prevención y orientación actuales del ransomware. Podemos esperar que todo tipo de actores de amenazas de ransomware aprovechen la IA para ayudarlos a completar ataques exitosos.

A finales del tercer trimestre, el recuento de víctimas de ransomware de 2023 ya superó lo observado durante todo 2021 o 2022. Si las cosas continúan en la trayectoria actual, este podría ser el primer año con más de 4000 víctimas de ransomware publicadas en sitios de filtraciones, según la aseguradora cibernética Corvus.

Los ciberdelincuentes han aprendido que no sólo las empresas son objetivos lucrativos para los ataques de ransomware, sino que también infraestructuras importantes como hospitales e instalaciones industriales se ven afectadas por el ransomware. Y esas perturbaciones pueden tener grandes consecuencias para las personas.

[27] Grobler, Ronan. Defending Against AI-Based Cyber Attacks: A Comprehensive Guide for Startups. {En línea}. 2023. {29 de mayo de 2024}. Disponible en: https://scytale.ai/resources/defending-against-ai-based-cyber-attacks/

El sector educativo también se ha convertido en un objetivo cada vez más popular para las campañas de ransomware. Las escuelas y universidades se volvieron dependientes del aprendizaje remoto debido a la pandemia de coronavirus, y los ciberdelincuentes se dieron cuenta.

¿Cómo evoluciona la respuesta ante la amenaza del ransomware en las empresas?

Las organizaciones también han adoptado un enfoque más proactivo para protegerse de los ataques de ransomware. Esto incluye implementar controles de acceso sólidos, invertir en herramientas avanzadas de detección de amenazas y actualizar y aplicar parches a los sistemas periódicamente. Además, se ha hecho hincapié en los programas de educación y concientización de los empleados para ayudar a prevenir ataques de phishing e ingeniería social.

Un avance notable es la mayor colaboración entre los sectores público y privado. Los organismos encargados de hacer cumplir la ley y las empresas de ciberseguridad han unido fuerzas para interrumpir las operaciones de ransomware y detener a los perpetradores.

Esto puede incluir el uso de tecnologías avanzadas de detección y respuesta a amenazas, la implementación de controles de acceso sólidos y la revisión y actualización periódica de políticas y procedimientos de seguridad.

1.13.1 SOLUCIONES TECNOLÓGICAS QUE FORTALECEN A LAS ORGANIZACIONES CONTRA ATAQUES DE RANSOMWARE, IA Y IOT

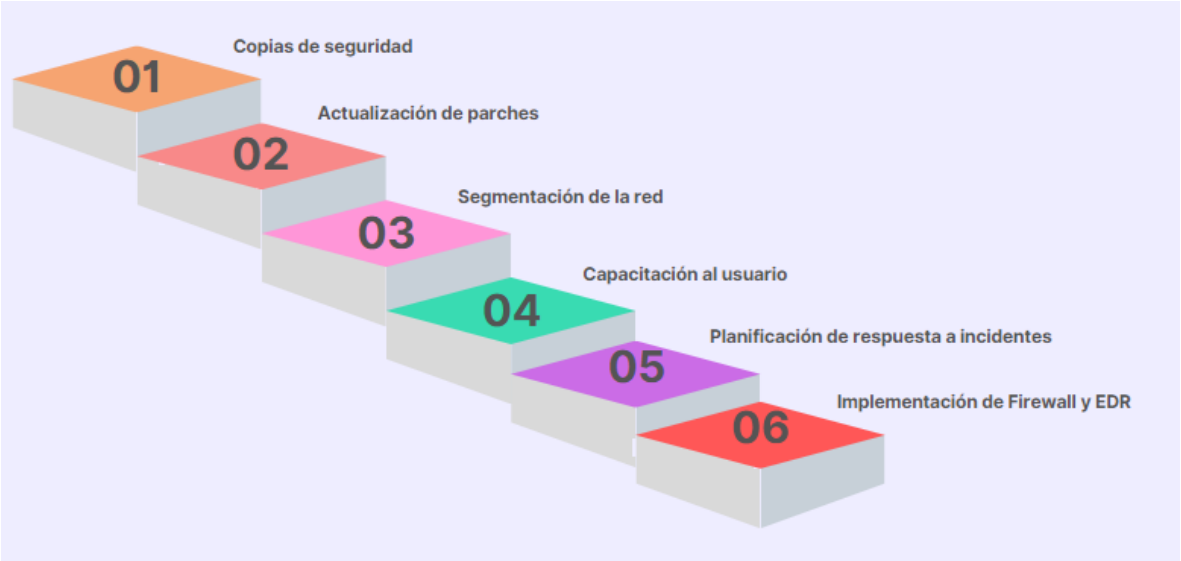
Los ataques de ransomware pueden provocar importantes tiempos de inactividad, pérdida de datos y costos financieros, por lo que es esencial que las organizaciones tomen medidas proactivas para prevenir y mitigar estos ataques.

Es importante contar con una solución de seguridad sólida que pueda detectar y prevenir ataques de ransomware. Uno de esos programas está desarrollado con la alta tecnología de Sophos[28], que puede contrarrestar el ransomware evasivo que se disfraza de ejecutables, archivos PDF y documentos de Microsoft Office.

Las estrategias[29] de prevención y mitigación tienen como objetivo reducir la probabilidad de un ataque de ransomware mediante la implementación de medidas técnicas, educación de los usuarios y planificación de respuesta a incidentes. Las medidas técnicas incluyen actualizaciones periódicas de software, segmentación de red, firewalls y seguridad de terminales. La educación de los usuarios implica capacitar a los empleados para que reconozcan y eviten los correos electrónicos de phishing y otras tácticas de ingeniería social comúnmente utilizadas por los atacantes de ransomware. La planificación de la respuesta a incidentes implica establecer líneas claras de comunicación y procedimientos de respuesta con anticipación para que todos los usuarios comprendan qué hacer si ocurre un ataque (Ver Figura 12).

[29] Ransomware: una guía de aproximación para el empresario. (2021). Empresas | INCIBE. Recuperado de https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario

Figura 12.Estrategias de prevención y mitigación de ataques de ransomware



Fuente: una guía de aproximación para el empresario. (2021). Empresas | INCIBE. Recuperado 20 de abril de 2021, de https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario

- **Copias de seguridad periódicas**: realizar copias de seguridad periódicas de los datos críticos es esencial para la prevención y mitigación del ransomware.
- **Actualizaciones de los sistemas:** mantener el software actualizado es otra estrategia fundamental para la prevención de ataques.
- **Segmentación de la red:** implementar la segmentación de la red ayuda a limitar la propagación del ransomware en caso de un ataque.
- **Cortafuego o Firewall:** ayuda a prevenir ataques de ransomware al bloquear la entrada de paquetes de datos sospechosos al sistema.
- **Planificación de respuesta a incidentes:** contar con un plan claro de respuesta a incidentes es esencial para la mitigación las organizaciones deben establecer líneas claras de comunicación y procedimientos de respuesta antes de un ataque.

- **Capacitación en concientización sobre seguridad:** Proporcionar conocimientos básicos de ciberseguridad a los empleados puede afectar en gran medida e incluso prevenir los ataques en su origen.

Uno de los principales riesgos de seguridad para los sistemas de IA[30] es la posibilidad de que los adversarios comprometan la integridad de sus procesos de toma de decisiones de manera que no tomen decisiones de la manera que sus diseñadores esperarían o desearían. Una forma de lograrlo sería que los adversarios tomaran directamente el control de un sistema de IA para poder decidir qué resultados genera el sistema y qué decisiones toma. Alternativamente, un atacante podría intentar influir en esas decisiones de manera más sutil e indirecta entregando entradas maliciosas o datos de entrenamiento a un modelo de IA.

Sin embargo, los ciberataques basados en IA son una preocupación creciente para las organizaciones y gobiernos de todo el mundo. Estos ataques pueden incluir el uso de IA para automatizar ataques de phishing, generar deepfakes o explotar vulnerabilidades en los sistemas de IA. Para protegerse contra los ciberataques basados en IA, las organizaciones pueden implementar detección basada en aprendizaje automático, inteligencia sobre amenazas basada en IA y automatización de seguridad basada en IA.

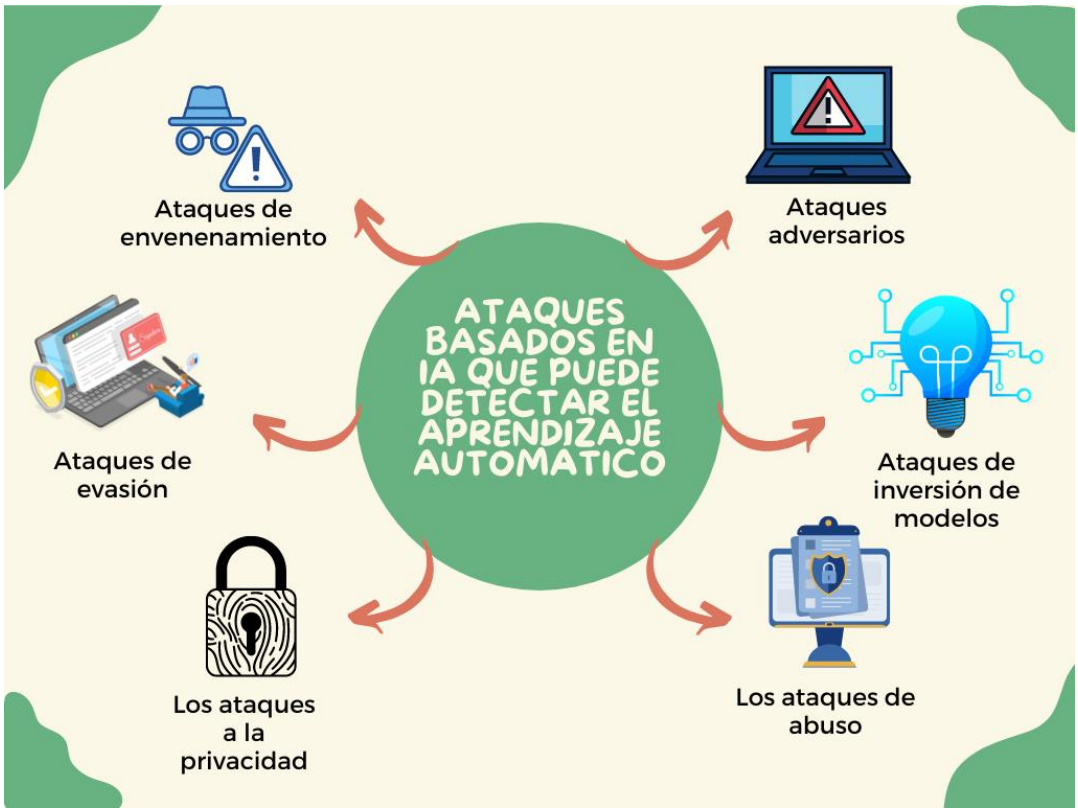
Los sistemas de inteligencia artificial han permeado la sociedad moderna, trabajando en capacidades que van desde conducir vehículos hasta ayudar a los médicos a diagnosticar enfermedades e interactuar con los clientes como chatbots en línea.

[30] García-Qismondo, M. Á. M., & Vivarelli, M. La convergencia de la Inteligencia Artificial y las Habilidades Digitales: un espacio necesario para la Educación Digital y la Educación 4.0. En: JLIS.it. 15, n.º 1 (2024); Pag. 1-15. Disponible en: https://www.jlis.it/index.php/jlis/article/view/566/531

Como hablamos anteriormente el aprendizaje automático[31] puede ayudar a detectar ataques basados en IA analizando rápidamente grandes volúmenes de datos e identificando patrones que pueden indicar un ataque.

Los algoritmos de aprendizaje automático pueden detectar estos y otros tipos de ataques basados en IA (ver Figura 13)

Figura 13. Ataques IA que el aprendizaje automático detecta



Fuente: NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems (2024) NIST. https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-system

[31] NIST. Identifica tipos de ciberataques que manipulan el comportamiento de los sistemas de IA. {En línea}. 2024. {22 de mayo de 2024}. Disponible en: https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

- **Ataques adversarios**: estos ataques implican realizar pequeñas modificaciones cuidadosamente elegidas en los datos de entrada, como imágenes o audio, para provocar que los sistemas de inteligencia artificial se comporten mal o hagan predicciones incorrectas.
- **Ataques de envenenamiento**: los adversarios introducen datos o códigos maliciosos en conjuntos de datos o modelos de entrenamiento de IA para manipular su comportamiento.
- **Ataques de evasión**: estos ataques implican que los adversarios modifiquen su comportamiento para evadir la detección de los sistemas de seguridad basados en IA.
- **Ataques de inversión de modelos**: en estos ataques, los adversarios intentan aplicar ingeniería inversa a los modelos de IA para extraer información o datos confidenciales.
- **Ataques a la privacidad**: son intentos de obtener información confidencial sobre la IA o los datos con los que fue entrenada para poder hacer un mal uso de ella.
- **Ataques de abuso**: intentan proporcionar a la IA información incorrecta de una fuente legítima pero comprometida para reutilizar el uso previsto del sistema de IA.

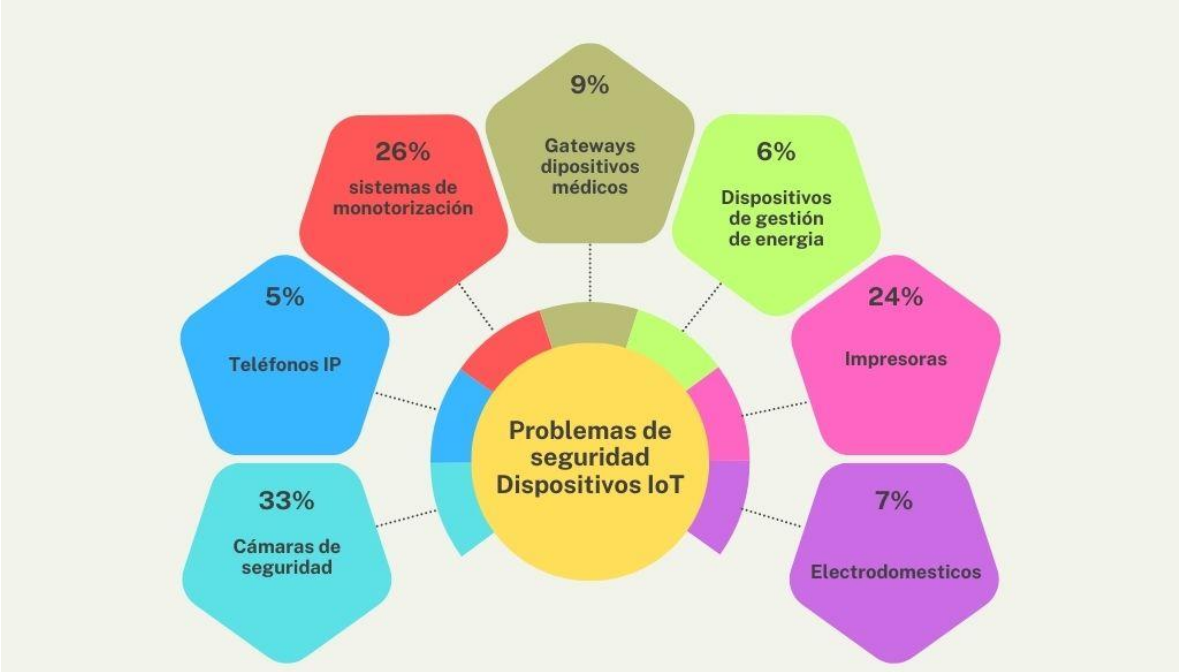
Los ataques de IoT[32] utilizan estos dispositivos como puerta de entrada para acceder a la red. Los ciberdelincuentes se aprovechan de que los usuarios, incluidos los empleados de las organizaciones, no piensan en proteger sus dispositivos de la misma manera que piensan en proteger sus computadoras. Desafortunadamente, nuestras redes son tan fuerte. Los ciberdelincuentes pueden explotar incluso un dispositivo IoT desprotegido para obtener acceso a una red y robar los datos.

[32] Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., Patrono, L. Internet de las cosas (IoT): oportunidades, problemas y desafíos hacia un futuro inteligente y sostenible. {En línea}. 2020. {01 de abril de 2024}. Disponible en: https://dialnet.unirioja.es/descarga/articulo/8914181.pdf

El análisis y la creación de perfiles de dispositivos inteligentes permiten al equipo de seguridad de TI ver los dispositivos IoT conectados, su perfil de riesgo y el comportamiento de la red en interacción con otros dispositivos de red.

Los problemas[33] de seguridad de IoT incluyen exposición remota, falta de previsión de la industria, limitaciones de recursos, contraseñas predeterminadas débiles, múltiples dispositivos conectados y falta de cifrado. Estos desafíos aumentan el riesgo de ataques cibernéticos, violaciones de datos y otras amenazas a la seguridad (Ver Figura 14).

Figura 14.Problemas de seguridad en los diferentes dispositivos IoT



Fuente: Smartekh, G. (s. f.). ¿Conoces el estado de la seguridad IoT en las empresas? https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf

[33] Smartek, G. ¿Conoces el estado de la seguridad IoT en las empresas? {En línea}. 2021. {20 mayo de 2024}. Disponible en: https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf

Debido a la vulnerabilidad de los dispositivos IoT, los ciberdelincuentes pueden usarlos fácilmente como parte de lo que se llama una " botnet ", que permite el ataque DDoS. Se puede ordenar a los dispositivos IoT pirateados que ayuden a inundar las redes junto con otros dispositivos pirateados. Cuantos más dispositivos IoT desprotegidos haya, más grandes serán las botnets.

A continuación, proporcionamos una descripción general de los tipos de malware de IoT con fines específicos:

- Botnets DDoS: Para el malware DDoS, el tipo de dispositivo objetivo es irrelevante, ya que cada dispositivo es capaz de cumplir el objetivo del atacante: enviar solicitudes a través de la Web.

- Mineros: Los atacantes intentaron utilizar dispositivos IoT para la minería de Bitcoin durante las campañas de Mirai, a pesar de su baja potencia de procesamiento. La práctica no se ha generalizado debido a su relativa ineficiencia.

- Cambiador de DNS: Cualquier enrutador que todavía utilice las credenciales de acceso predeterminadas, como admin:admin, podría estar infectado. En dicho dispositivo, la configuración se modificaría para que utilice el servidor DNS de los operadores.

Para fortalecer a las organizaciones[34] contra los ataques de IoT, se pueden emplear varias soluciones tecnológicas. En primer lugar, implementar protocolos de

[34] Echeverría, A., Cevallos, C., Ortiz-Garcés, I., & Andrade, RO Modelo de ciberseguridad basado en el endurecimiento para la implementación segura del Internet de las cosas. {En línea}. 2021. {09 de febrero del 2024}. Disponible en: https://doi.org/10.3390/app11073260

seguridad y métodos de cifrados sólidos puede evitar el acceso no autorizado a dispositivos y datos de IoT. Esto incluye el uso de protocolos de comunicación seguros, como HTTPS y TLS, para proteger los datos en tránsito. Además, cifrar datos en reposo y en tránsito puede evitar que los piratas informáticos intercepten y exploten información confidencial, implementar planes de respuesta a incidentes y recuperación ante desastres puede ayudar a las organizaciones a responder de forma rápida y eficaz en caso de un ataque ,esto incluye tener un plan integral de respuesta a incidentes, realizar simulacros y ejercicios regulares y contar con un plan de recuperación ante desastres para minimizar el tiempo de inactividad y la pérdida de datos.

La seguridad de los dispositivos IoT es crucial para proteger los activos más valiosos de una organización, es importante mantener la productividad mientras se prioriza la seguridad.

A medida que los dispositivos IoT se vuelven cada vez más frecuentes en el mundo empresarial, también lo hacen los riesgos y amenazas que plantean. A continuación, se muestran algunas medidas[35] que pueden ayudar a reducir el riesgo de ataques de IoT:

1. Implementar medidas sólidas de control de acceso

Una de las formas más efectivas de reducir el riesgo de ataques de IoT es implementar fuertes medidas de control de acceso.

2. Mantener el software y el firmware actualizados

[35] Trevino, A., & Trevino, A. Cómo evitar los ataques del Internet de las cosas (IoT). {En línea}. 2023. {21 abril de 2024}. Disponible en: https://www.keepersecurity.com/blog/es/2023/07/11/how-to-prevent-internet-of-things-iot-attacks/

Otra medida importante es mantener actualizado el software y el firmware. Esto ayuda a garantizar que se parcheen las vulnerabilidades conocidas y reduce el riesgo de ataque.

3. Utilizar cifrado

El cifrado es una medida crítica para proteger los datos transmitidos hacia y desde dispositivos IoT.

4. Implementar la segmentación de la red

La segmentación de red es la práctica de dividir una red en segmentos más pequeños y aislados. Esto ayuda a reducir el riesgo de ataque al limitar el alcance de cualquier posible infracción.

5. Realizar auditorías de seguridad periódicas

Las auditorías de seguridad periódicas pueden ayudar a identificar posibles vulnerabilidades y debilidades en el sistema de IoT.

6. Capacitar a los empleados

Por último, brindar capacitación a los empleados sobre las mejores prácticas de seguridad de IoT puede ayudar a reducir el riesgo de ataques.

CONCLUSIONES

La proliferación de dispositivos de Internet de las cosas (IoT) ha propiciado avances significativos en nuestra vida diaria y en los procesos industriales. Sin embargo, este rápido crecimiento también ha introducido una serie de desafíos de seguridad que deben abordarse de manera efectiva. Una de las principales dificultades con la seguridad es la diversidad de tecnologías y estándares utilizados, lo que crea complejidad para garantizar la seguridad en toda la red, muchos dispositivos de IoT tienen recursos limitados, como potencia de procesamiento y memoria, lo que dificulta la implementación de medidas de seguridad sólidas. La falta de conciencia y educación en seguridad también es un desafío importante en el panorama de los usuarios y organizaciones no son plenamente conscientes de los riesgos asociados con los dispositivos.

Para mitigar estos riesgos, es esencial comprender los problemas de seguridad comunes como contraseñas débiles, falta de actualizaciones de firmware y comunicación no cifrada. La implementación de mejores prácticas, como autenticación sólida, actualizaciones periódicas y cifrado, puede ayudar a reducir las vulnerabilidades y los riesgos asociados con los dispositivos de IoT.

La Inteligencia Artificial (IA) está impactando significativamente la ciberseguridad al mejorar las defensas, predecir amenazas y brindar soluciones efectivas. La capacidad para procesar y analizar grandes volúmenes de datos a altas velocidades la convierte en una herramienta vital para anticipar e identificar amenazas cibernéticas. Los dos tipos principales de IA utilizados en ciberseguridad son el aprendizaje automático y el aprendizaje profundo, ayudan a categorizar ataques, priorizar respuestas y predecir ataques futuros en función de patrones de comportamiento. Sin embargo, el uso de la IA en la ciberseguridad también presenta desafíos, como garantizar la confiabilidad de los datos e interpretar los resultados, a pesar de estos desafíos, el potencial para transformar la ciberseguridad es enorme

y ofrece capacidades avanzadas de detección y respuesta que pueden proteger sistemas y datos de maneras sin precedentes.

En los últimos años, los ataques de ransomware se han vuelto cada vez más sofisticados y destructivos, y los ciberdelincuentes desarrollan constantemente nuevas tácticas y técnicas para explotar vulnerabilidades y evadir la detección. A partir de 2020, han aumentado en frecuencia y gravedad y se han dirigido a diversas industrias, incluidas la atención médica, las finanzas y la infraestructura crítica.

Una de las tendencias más importantes en los ataques de ransomware es el uso de tácticas de doble extorsión, donde los atacantes no sólo cifran los datos de la víctima, sino que también los roban y amenazan con divulgarlos públicamente a menos que se pague un rescate. Este enfoque hace que sean más dañinos y costosos para las víctimas, ya que enfrentan no solo la pérdida de acceso a sus datos sino también el riesgo de daños a su reputación y multas regulatorias.

Para combatir estas amenazas, las organizaciones deben implementar medidas sólidas de ciberseguridad, incluidas actualizaciones periódicas de software, autenticación multifactor y capacitación de los empleados. Además, las organizaciones deben contar con un plan integral de respuesta a incidentes para minimizar el impacto de un ataque de ransomware y garantizar la continuidad del negocio.

RECOMENDACIONES

Para las empresas, una de las aplicaciones más valiosas del metaverso será cerrar la brecha entre los mundos real y virtual. Utilizando datos de sensores de IoT, será posible construir gemelos digitales cada vez más realistas de muchos sistemas diferentes, desde instalaciones de fabricación hasta centros comerciales.

Para garantizar la seguridad de los dispositivos de IoT, las organizaciones deben implementar medidas sólidas de control de acceso, como autenticación multifactor y políticas de gestión de acceso. Actualizar periódicamente el firmware y el software de los dispositivos también es fundamental para garantizar que estén protegidos contra vulnerabilidades conocidas. Se debe utilizar el cifrado para proteger los datos transmitidos entre los dispositivos de IoT y la nube, y la segmentación de la red puede ayudar a limitar la propagación de un posible ataque. Las herramientas de administración de dispositivos se pueden utilizar para monitorear y administrar dispositivos IoT, y las auditorías de seguridad periódicas pueden ayudar a identificar y abordar posibles riesgos de seguridad.

La IA puede automatizar tareas rutinarias, reduciendo costos y minimizando el error humano tiene un impacto significativo en la ciberseguridad al mejorar las capacidades de detección, prevención y respuesta a amenazas. Las técnicas de inteligencia artificial, como el aprendizaje automático y el aprendizaje profundo, pueden analizar grandes cantidades de datos, identificar patrones y detectar anomalías, lo que permite a los equipos de ciberseguridad detectar amenazas con mayor rapidez y precisión. Los sistemas impulsados por IA también pueden predecir y prevenir ataques cibernéticos mediante la identificación de actividades potencialmente maliciosas y actores de amenazas.

Para prevenir y mitigar el impacto de los ataques de ransomware, es fundamental implementar mejores prácticas y medidas de seguridad. Esto incluye actualizar el

software periódicamente y utilizar contraseñas seguras y únicas, así como implementar controles de acceso y autenticación multifactor. Además, es importante realizar copias de seguridad periódicas de los datos críticos y garantizar que las copias de seguridad estén aisladas de la red para evitar el cifrado por ransomware. Los empleados deben estar capacitados para reconocer y evitar correos electrónicos de phishing y otras tácticas de ingeniería social comúnmente utilizadas por los atacantes de ransomware. La segmentación de la red y el uso de sistemas de prevención y detección de intrusiones también pueden ayudar a limitar la propagación dentro de una red.

BIBLIOGRAFÍA

ALBORS, J. Tendencias 2021: ¿Qué nos depara un futuro incierto en materia de ciberseguridad? {En línea}. {10 febrero de 2024}. Disponible en: https://blogs.protegerse.com/2020/12/04/tendencias-2021-que-nos-depara-un-futuro-incierto-en-materia-de-ciberseguridad

ALRFAI, Mm, ALQUDAH, H., LUTFI, A., AL-KOFAHI, M., ALRAWAD, M. y ALMAIAH, MA La influencia de la inteligencia artificial en la eficiencia de los AIS: efecto moderador de la ciberseguridad. {En línea}. 2023. {29 enero del 2024}. Disponible en: https://www.researchgate.net/publication/373139284_The_influence_of_artificial_intelligence_on_the_AISs_efficiency_Moderating_effect_of_the_cyber_security

AMIRUDDIN, A., RATNA, AAP y SARI, RF Revisión sistemática de la seguridad de Internet de las cosas. {En línea}. 2019. {28 enero del 2024}. Disponible en: https://www.researchgate.net/publication/358022729_Systematic_Literature_Review_of_Internet_of_Things_IoT_Security

BUSSELEN, M. Por qué el ciberdelito sigue siendo un desafío empresarial preocupante en un mundo bloqueado por COVID. {En línea}. 2020. {02 febrero del 2024}. Disponible en: https://www.crowdstrike.com/blog/why-cybercrime-remains-a-worryingbusiness-challenge-in-a-covid-lockdown-world

CHUQUILLA, A., GUARDA, T., & NINAHUALPA Quiña, G. Ransomware WannaCry: La seguridad es de todos. {En línea}. 2019. {28 enero del 2024}. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=8760749

CONGRESO DE COLOMBIA. Ley 1273 de 2009. {En línea}. 2009. {10 febrero del 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CENTRO NACIONAL DE CIBERSEGURIDAD. Mitigar ataques de malware y ransomware. {En línea}. 2020. {13 de febrero de 2024}. Disponible en: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

DANG, LM, PIRAN, MJ, HAN, D., MIN, K., & MOON, H. Una encuesta sobre Internet de las cosas y computación en la nube para la atención médica. En: Electronics. Vol. 8, No. 7 (2019); 768p.

DUQUE, AR Tendencias en Ciberseguridad en Latinoamérica. {En línea}. 2022, 6 de julio. {15 febrero del 2024}. Disponible en:

https://revistaempresarial.com/tecnologia/seguridad-informatica/tendencias-en-ciberseguridad-en-latinoamerica/

EBERT, C. y LOURIDAS, P. IA generativa para profesionales de software. Es: Software IEEE. vol. 40, N° 4 (Jul.-ago. 2023). 30-38p. doi: 10.1109/MS.2023.3265877. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=10176168

ECHEVERRÍA, A., CEVALLOS, C., ORTIZ-GARCÉS, I., & Andrade, RO Modelo de ciberseguridad basado en el endurecimiento para la implementación segura del Internet de las cosas. {En línea}. 2021. {09 de febrero del 2024}. Disponible en: https://doi.org/10.3390/app11073260

FRENZ, Christopher M. & DÍAZ, Christian L. Guía Contra Ataques Ransomware. {En línea}. 2019. {20 febrero del 2024}. Disponible en: https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf

GARCÍA-QISMONDO, M. Á. M., & VIVARELLI, M. La convergencia de la Inteligencia Artificial y las Habilidades Digitales: un espacio necesario para la Educación Digital y la Educación 4.0. En: JLIS.it. 15, n.º 1 (2024); 1-15p. Disponible en: https://www.jlis.it/index.php/jlis/article/view/566/531

GOMEZ, MA & SHANDLER, R. Confianza en riesgo: el efecto de la proximidad a los ciberataques. {En línea}. 2024. {Fecha de consulta: [fecha de consulta]}. Disponible en: https://academic-oup-com.bibliotecavirtual.unad.edu.co/jogss/article/9/2/ogae002/7627110

GÓMEZ, WOA La inteligencia artificial y su incidencia en la educación: Transformando el aprendizaje para el siglo XXI. En: Revista Internacional de Pedagogía e Innovación Educativa. 3, n.º 2 (2023); 217-229p. Disponible en: https://editic.net/ripie/index.php/ripie/article/view/133/114

INCIBE. Ciberseguridad en la identidad digital y la reputación online. Guía de recomendaciones para empresas. {En línea}. 2023. {02 de febrero del 2024}. Disponible en: https://www.incibe.es/empresas/guias/guia-ciberseguridad-identidad-online

INTERNET DE LAS COSAS (IoT): oportunidades, problemas y desafíos hacia un futuro inteligente y sostenible (2020) Revista de Producción Más Limpia, 274, art. No. 122877 https://dialnet.unirioja.es/descarga/articulo/8914181.pdf

KARIM, S., AFZAL, M., IQBAL, W. y ABRI, DA Conjunto de datos de evaluación de detección de intrusiones y amenazas persistentes avanzadas (APT) para sistemas

Linux. {En línea}. 2024. {01 de marzo del 2024}. Disponible en: https://www.sciencedirect.com/science/article/pii/S2352340924002592?pes=vor

KOUICEM, DE, BOUABDALLAH, A., & LAKHLEF, H. Seguridad de Internet de las cosas: una encuesta de arriba hacia abajo. En: Computer Networks . 141 (2018); 199-221p. Disponible en: https://www.researchgate.net/publication/323912995_Internet_of_Things_Security_a_top-down_survey

MAAS, M. Combinación del aprendizaje automático y la gestión de recursos basada en la vida útil para la asignación de memoria y más. {En línea}. 2024, 18 de marzo. {Fecha de consulta: 22 octubre 2024}. Disponible en: https://cacm.acm.org/research/combining-machine-learning-and-lifetime-based-resource-management-for-memory-allocation-and-beyond/en

MORENO, J., RODRÍGUEZ, C., & LEGUIAS, I. Revisión sobre propagación de ransomware en sistemas operativos Windows. En: I+D Tecnológico. 16 (2020); N° 1; 39-45p.

NIST. Identifica tipos de ciberataques que manipulan el comportamiento de los sistemas de IA. {En línea}. 2024. {22 de mayo de 2024}. Disponible en: https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

NIŽETIĆ, S., ŠOLIĆ, P., LÓPEZ-DE-IPIÑA, D., PATRONO, L. Internet de las cosas (IoT): oportunidades, problemas y desafíos hacia un futuro inteligente y sostenible. {En línea}. 2020. {01 de abril de 2024}. Disponible en: https://dialnet.unirioja.es/descarga/articulo/8914181.pdf

ORTIZ-GARCÉS, I., CADENA, C., NEGRETTE, G. Implementación de un Modelo de Ciberseguridad de una Arquitectura de Sensores de Monitoreo IoT en la Niebla. {En línea}. 2023. {02 abril de 2024}. Disponible en: https://www.proquest.com/openview/0d6c5600ad7df199fb0eb45d60a7d415/1.pdf?pq-origsite=gscholar&cbl=1006393

OSORIO-SIERRA, A., MATEUS-HERNÁNDEZ, MJ, & VARGAS-MONTOYA, HF Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. {En línea}. 2020. {Fecha de consulta: 22 de octubre de 2024}. Disponible en: https://doi.org/10.18273/revuin.v19n3-2020013

PUAT, HAM y ABD RAHMAN, NA Ransomware como servicio y concienciación pública. {En línea}. 2020. {12 mayo de 2024}. Disponible en: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=92GovCkAAAAJ&citation_for_view=92GovCkAAAAJ:u-x6o8ySG0sC

RANSOMWARE: una guía de aproximación para el empresario. (2021). Empresas | INCIBE. Recuperado de https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario

SAMTANI, S., KANTARCIOĞLU, M., CHEN, H. Pioneros en la inteligencia artificial para la disciplina de ciberseguridad. {En línea}. 2020. {09 mayo de 2024}. Disponible en: https://dl.acm.org/doi/pdf/10.1145/3430360

SHARMA, P., KAPOOR, S. y SHARMA, R. Detección, prevención y protección de ransomware en dispositivos IoT mediante técnicas de aprendizaje automático basadas en un enfoque de análisis dinámico. {En línea}. 2022. {22 de mayo de 2024}. Disponible en: https://doi.org/10.1007/s13198-022-01793-0

SMARTEK, G. ¿Conoces el estado de la seguridad IoT en las empresas? {En línea}. 2021. {20 mayo de 2024}. Disponible en: https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf

TREVINO, A. Cómo evitar los ataques del Internet de las cosas (IoT). {En línea}. 2023. {21 abril de 2024}. Disponible en: https://www.keepersecurity.com/blog/es/2023/07/11/how-to-prevent-internet-of-things-iot-attacks/

THAKKAR, A. y LOHIYA, R. Una revisión del avance en los conjuntos de datos de detección de intrusiones. {En línea}. 2020. {05 de abril de 2024}. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050920311121

UE (2020): “La estrategia de ciberseguridad de la UE para la década digital”, ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

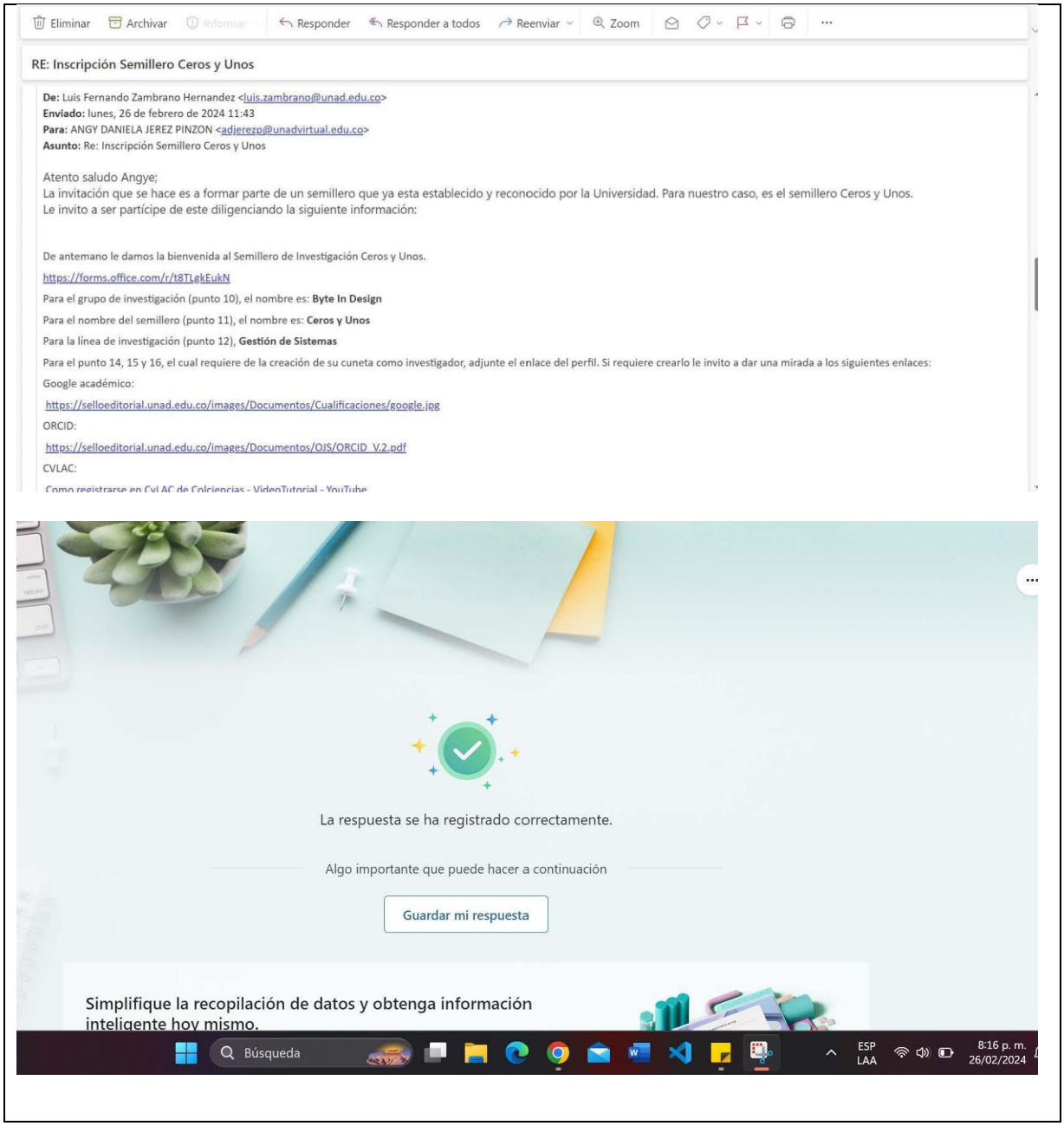
WANG, X., ZHAO, Y. y POURPANAH, F. Avances recientes en el aprendizaje profundo. {En línea}. 2020. {25 de mayo de 2024}. Disponible en: https://link.springer.com/article/10.1007/s13042-020-01096-5.

WIAFE, I., KORANTENG, FN, OBENG, EN, ASSYNE, N., WIAFE, A. y Gulliver, SR Inteligencia artificial para la ciberseguridad: un mapeo sistemático de la literatura. {En línea}. 2020. {26 de mayo de 2024}. Disponible en: https://ieeexplore.ieee.org/ielx7/6287639/8948470/09152956.pdf

ZARINA, IK, ILDAR, RB y Elina, LS Inteligencia artificial y problemas para garantizar la seguridad cibernética. {En línea}. 2019. {24 marzo de 2024}. Disponible en: https://www.cybercrimejournal.com/pdf/KhisamovaetalVol13Issue2IJCC2019.pdf

ANEXOS

Anexo A Inscripción semillero ceros y unos



Anexo B Interacción con el asesor del proyecto