ENTHEC

qondar

Inteligencia Artificial:
El reto para la seguridad de las personas

qondar

PAG.

Índice

INTRODUCCIÓN

La irrupción de la inteligencia artificial ha revolucionado múltiples sectores ofreciendo beneficios significativos que nadie pone en duda. Sin embargo, como ocurre con cada nueva tecnología, su desarrollo también ha dado lugar a nuevas amenazas y vulnerabilidades.

Los ciberdelincuentes están utilizando IA para llevar a cabo ataques más sofisticados y difíciles de detectar. Junto con el peligro que esto supone para las organizaciones, la utilización de la IA para llevar a cabo ciberataques también pone en riesgo la privacidad, la seguridad y el bienestar de las personas.

En este contexto, la ciberseguridad se convierte en un componente esencial para garantizar que los avances en IA no se traduzcan en mayores riesgos para la sociedad. En el punto de evolución tecnológica que nos encontramos y antes de que se produzca la inflexión que cambiará nuestra forma de estar en el mundo, es preciso que los gobiernos, organizaciones y usuarios individuales asuman las implicaciones de la IA en la ciberseguridad y aprendan a adoptar medidas proactivas para mitigar estos riesgos.

En este documento analizamos los desafíos y riesgos que la inteligencia artificial plantea en la seguridad de las personas y la forma de enfrentarlos. A medida que la IA avanza y se integra en todos los aspectos de nuestra vida cotidiana, es crucial entender cómo estas tecnologías pueden ser explotadas por ciberdelincuentes y qué medidas proactivas se pueden ya tomar para evitarlo e impedir que su evolución impacte negativamente en la seguridad personal de todos.

qondar

ESTADO DE LA INTELIGENCIA ARTIFICIAL:

La IA se ha integrado en numerosos sectores, transformando la manera en que operan las industrias y organizaciones y mejorando la eficiencia y la productividad. Desde sus inicios en la década de 1950, la IA ha evolucionado significativamente, pasando de simples programas de reglas a sistemas avanzados de aprendizaje automático y redes neuronales profundas..

Aplicaciones ACTUALES

Asistentes virtuales

Tecnologías que utilizan IA para comprender y responder a comandos de voz, facilitando la interacción entre humanos y máquinas.

Automatización industrial

Robots y sistemas de análisis y producción automatizados impulsados por IA están revolucionando la manufactura, optimizando procesos y desarrollando prototipos.

Sistemas de recomendación

Utilizados en plataformas como y redes sociales para sugerir y mostrar contenido basado en los intereses y las preferencias del usuario.

Conducción autónoma

Vehículos con sistemas de conducción autónoma integrados, que no necesitan la presencia o dirección de un conductor humano.

Procesamiento del lenguaje natural

Herramientas capaces de generar texto y conversación similares a los desarrollados por los humanos y realizar labores asociadas, como las traducciones automáticas.

Medicina personalizada

La inteligencia artificial analiza datos médicos, emite diagnósticos y ofrece tratamientos altamente personalizados.

Aplicaciones FUTURAS

Súperinteligencia

Máquinas capaces de realizar operaciones y tomar de forma autónoma decisiones complejas inalcanzables para el ser humano.

Automatización avanzada

Máquinas capaces de llevar a cabo tareas y operaciones de alta complejidad en sectores industriales como la manufactura y la logística.

Robots sociales

Androides integrados en la sociedad capaces de interactuar, relacionarse y convivir con humanos, de manera empática y social, realizando labores de acompañamiento.

Educación avanzada

Sistemas personalizados de aprendizaje que analizarán las características y el contexto de cada estudiante para crear una ruta con métodos y contenidos adaptados.

Salud y bienestar

La inteligencia artificial servirá para implantar un sistema de salud altamente preventivo, en el que las enfermedades se diagnosticarán en su fase potencial, para ser evitadas o minimizadas al máximo, y las necesidades para lograr bienestar mental y corporal se identificarán y cubrirán de forma temprana.

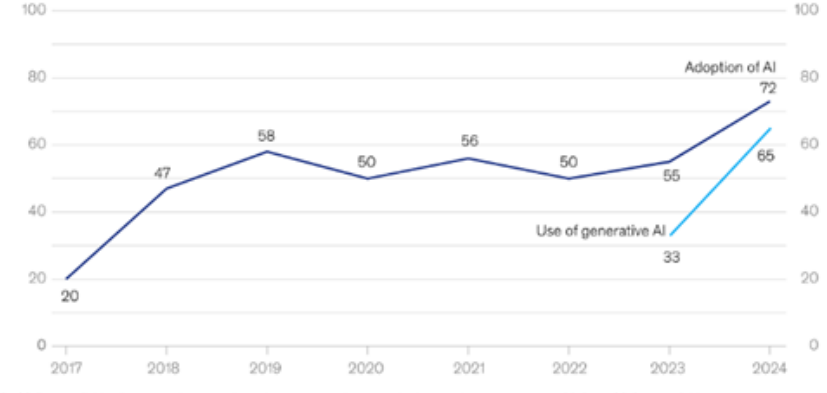
DATOS

En 2023, la IA superó el rendimiento humano en varias tareas intelectuales, como la clasificación de imágenes y el razonamiento visual. Además, el uso de modelos de aprendizaje automático por parte de la industria superó al de la academia, con 51 modelos producidos por la industria en comparación con solo 15 de la academia.
Stanford University 2024 AI Index Report

En 2024, el 65% de las organizaciones utilizan regularmente IA generativa, casi el doble del porcentaje del año anterior.
The state of AI in early 2024: Gen AI adoption spikes and starts to generate value (McKinsey, 2024)

AI adoption worldwide has increased dramatically in the past year, after years of little meaningful change.

Organizations that have adopted AI in at least 1 business function,[1] % of respondents



[1]In 2017, the definition for AI adoption was using AI in a core part of the organization's business or at scale. In 2018 and 2019, the definition was embedding at least 1 AI capability in business processes or products. Since 2020, the definition has been that the organization has adopted AI in at least 1 function.
Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

qondar

RIESGOS DE LA INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD DE LAS PERSONAS

La rápida evolución prevista de la inteligencia artificial plantea desafíos importantes en términos de seguridad y privacidad de las personas, que deben ser abordados para garantizar el desarrollo y uso seguros y éticos de la tecnología.

RIESGOS

PRIVACIDAD

La inteligencia artificial tiene la capacidad de procesar grandes cantidades de datos personales. Los sistemas de IA recopilan, almacenan y analizan información personal sensible, lo que deriva en la filtración y exposición de datos privados si no se custodian adecuadamente.

SEGURIDAD

Como cualquier tecnología, los sistemas de IA son vulnerables a ataques cibernéticos, lo que permite a actores malintencionados tomar el control de estos sistemas para causar daños físicos o digitales. Por ejemplo, un ataque a un sistema de conducción autónoma podría resultar en accidentes de tráfico.

SESGOS

La IA puede perpetuar y amplificar sesgos existentes en los datos de entrenamiento, con un impacto significativo en la vida de las personas. En el peor de los escenarios, esos sesgos pueden ser introducidos en el desarrollo de la IA con una intencionalidad maliciosa contra u grupo de personas determinado.

OPACIDAD

La falta de transparencia en su desarrollo hace que sea difícil detectar y corregir errores o sesgos, intencionados o no, en los sistemas de IA. La falta de supervisión humana y sus consecuentes construcciones morales aumenta el riesgo de que los sistemas de IA perjudiquen a individuos o grupos de personas.

MANIPULACIÓN

La inteligencia artificial puede ser utilizada para crear y difundir información falsa o manipulada. Esta capacidad de la IA para generar desinformación puede tener consecuencias graves para personas de relevancia social o patrimonial.

Todos los [CROs] encuestados coincidieron en que el desarrollo de la IA estaba superando su capacidad para gestionar sus posibles riesgos éticos y sociales, y el 43% dijo que el desarrollo de nuevas tecnologías de IA debería detenerse o ralentizarse hasta que se comprendiera mejor su impacto potencial.
Chief Risk Officer Outlook (World Economic Forum, 2023)

En un sistema basado en IA, la fase de recogida y preprocesamiento de datos es vulnerable a ataques de suplantación de sensores y a ataques de escalado, respectivamente, mientras que las fases de entrenamiento e inferencia del modelo están sujetas a ataques de envenenamiento y a ataques adversarios.
Artificial Intelligence Security: Threats and Countermeasures (Associaton for Computing Machinery, 2021)

NUEVAS FORMAS DE CIBERDELINCUENCIA

La utilización de las nuevas tecnologías, destacando entre todas la inteligencia artificial, es la causa de la sofisticación que han experimentado las técnicas de ciberataques estos últimos tiempos y, también, de su creciente número de éxitos y de la dificultad de enfrentarse a ellos con los medios tradicionales de protección.

CIBERATAQUES IMPULSADOS POR INTELIGENCIA ARTIFICIAL

Los ciberataques impulsados por IA son cada vez más numerosos, sofisticados y difíciles de detectar. Los atacantes utilizan algoritmos de aprendizaje automático para analizar patrones de comportamiento y encontrar vulnerabilidades en los sistemas de seguridad. Estos ataques pueden adaptarse en tiempo real, lo que los hace extremadamente peligrosos y efectivos.

PHISHING Y FRAUDES AUTOMATIZADOS

Con la ayuda de la IA, estos ataques se han vuelto más convincentes y difíciles de identificar. Los sistemas de IA son capaces de generar correos electrónicos y mensajes de texto personalizados que imitan a la perfección la comunicación legítima de empresas y personas. Además, los fraudes automatizados pueden llevarse a cabo a gran escala, afectando a miles de personas en cuestión de minutos. La capacidad de la IA para analizar grandes volúmenes de datos permite a los atacantes identificar y explotar las debilidades de sus víctimas con mayor precisión.

MALWARE Y RANSOMWARE AVANZADOS

Los programas maliciosos ahora pueden evadir las medidas de seguridad tradicionales mediante técnicas de camuflaje y autoaprendizaje. El ransomware, en particular, se ha vuelto más sofisticado, con la capacidad de cifrar datos de manera más efectiva y exigir rescates más altos. Los atacantes también utilizan IA para identificar los objetivos más lucrativos y planificar ataques altamente dirigidos.

NUEVAS FORMAS DE CIBERDELINCUENCIA

qondar

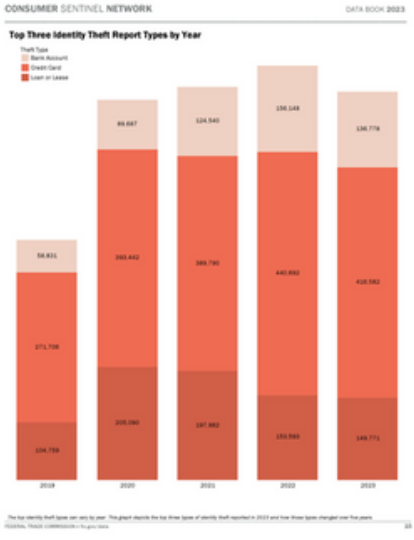
CASOS DE ESTUDIO

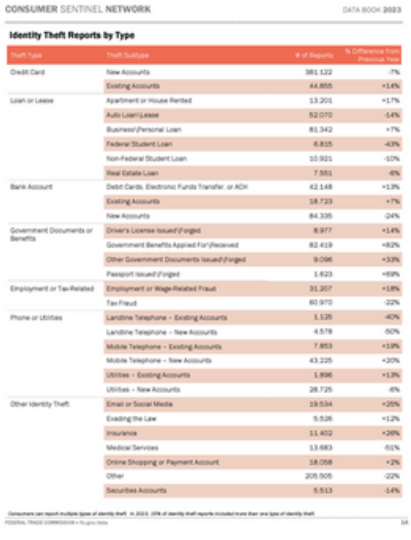
La inteligencia artificial está detrás de una gran cantidad de ciberataques de éxito que han trascendido por su enorme impacto negativo, tanto en organizaciones como en personas. Respecto a estas, los ciberataques impulsados por IA han tenido consecuencias significativas, tanto a nivel financiero como emocional.

DEEP FAKES Y ROBO DE IDENTIDAD

La manipulación de imágenes, vídeos y archivos de audio mediante IA ha creado una nueva amenaza conocida como deepfakes. Estos se han utilizado para suplantar identidades y cometer fraudes, generando pérdidas significativas.

La Comisión Federal de Comercio de EEUU (FTC) señala que en 2023, recibió más de 1 millón de denuncias de robo de identidad a través del sitio web de la FTC habilitado para ello.
Consumer Sentinel Network Data Book 2023





CLONACIÓN DE VOZ Y DE IMAGEN:

Los ciberdelincuentes han utilizado IA para clonar voces y engañar a personas, haciéndoles creer que están hablando con alguien de confianza.

Un empleado de una compañía financiera hongkonesa transfirió recientemente 23,7 millones de euros a lo que él creía que era la filial de su empresa en el Reino Unido. Los estafadores usaron la tecnología deepfake para hacerse pasar por el director financiero y otros colegas en una videoconferencia.
CNN 04/02/2024

CASOS DE ESTUDIO

ANÁLISIS DEL IMPACTO

FINANCIERO

El objetivo último de la mayoría de los ciberataques es el enriquecimiento ilícito. La utilización de la IA por parte de los ciberdelicuentes está provocando que las pérdidas patrimoniales personales por este tipo de delitos sea cada año mayor. La cantidad de números de cuentas bancarias y tarjetas de crédito en venta en foros ilegales debido a brechas de seguridad en los datos de compañías financieras no deja de crecer cada año.

PERSONAL

Tras un ataque que haya utilizado la IA para suplantar la identidad de una persona o actuar en su nombre, la reputación personal puede verse gravemente afectada, así como sus relaciones profesionales y personales. Para las personas de relevancia social profesional o patrimonial, está claro que la reputación es un activo valioso, pero también lo es para cualquier persona dentro de su entorno de actuación.

EMOCIONAL

Ser víctima de un ciberataque del tipo deep fake lleva aparejado un impacto emocional profundo, tanto si el suplantado es uno mismo, como si ha sido el engañado por una suplantación realizada a través de IA. El éxito de este tipo de ataques genera estrés y ansiedad en las víctimas y es presumible que, en un futuro cercano, existan terapias especializadas en superar este trance.

Comprender y asumir los nuevos tiempos, la evolución de los ciberataques, las nuevas técnicas utilizadas y los nuevos delitos, así como la realidad de ser objetivo de ellos es fundamental para la protección de la integridad y el patrimonio individual. La educación y la concienciación son imprescindibles para prevenir ciberataques, pero también lo es asumir que es necesaria la **protección personal online,** igual que se lleva a cabo offline, protegiendo propiedades, información y activos del alcance ajeno.

CASOS DE ESTUDIO

qondar

MEDIDAS DE PROTECCIÓN Y MITIGACIÓN

La inteligencia artificial ha transformado tanto la defensa como los ataques en el ámbito de la ciberseguridad. Para proteger a las personas de las amenazas basadas en IA, es esencial implementar estrategias avanzadas y contar con tecnologías emergentes y regulaciones específicas.

ESTRATEGIAS

Detección y prevención de amenazas en tiempo real: Utilizar sistemas de IA que analicen el tráfico de red y los comportamientos en tiempo real para identificar y neutralizar las amenazas antes de que causen daño.

Automatización de la respuesta a incidentes: Implementar soluciones de IA que puedan responder automáticamente a incidentes de seguridad, minimizando el tiempo de reacción y reduciendo el impacto de los ataques.

Análisis predictivo y proactivo: Emplear IA para predecir posibles ataques basándose en patrones históricos y comportamientos sospechosos, permitiendo una preparación y defensa proactiva.

TECNOLOGÍAS EMERGENTES

Blockchain: Ofrece una forma segura y transparente de almacenar y transferir datos, protegiendo la integridad y privacidad de la información personal.

Edge Computing: Permite procesar datos más cerca de su origen, reduciendo la exposición a posibles ataques durante la transmisión y mejorando la privacidad.

IA y automatización: Facilitan la detección en tiempo real de filtraciones, exposiciones y usos ilegítimos de información y activos digitales.

REGULACIONES

Reglamento General de Protección de Datos (RGPD): Este reglamento europeo establece directrices claras sobre cómo deben manejarse y protegerse los datos personales, garantizando los derechos de los individuos.

Ley de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD): En España, esta ley complementa el RGPD y proporciona un marco legal para la protección de datos personales, asegurando que las personas tengan control sobre su información.

Políticas de ciberseguridad nacionales: Los gobiernos deben desarrollar y actualizar continuamente sus políticas de ciberseguridad para abordar las amenazas emergentes y proteger a los ciudadanos de posibles ataques.

MEDIDAS DE PROTECCIÓN Y MITIGACIÓN

qondar

EL FUTURO DE LA SEGURIDAD ONLINE DE LAS PERSONAS

A corto plazo, será cada vez más necesario que las personas aprendan a protegerse frente a las nuevas amenazas que, para su seguridad personal, conllevan las últimas tecnologías. A medio plazo, las soluciones y herramientas de protección personal online serán tan rutinarias como hoy lo son los antivirus.

TENDENCIAS Y PREDICCIONES

CIBERATAQUES MÁS SOFISTICADOS

Los ciberdelincuentes también están aprovechando la IA para llevar a cabo ataques más sofisticados. Los ataques de phishing automatizados altamente dirigidos, los chatbots maliciosos y el uso de la IA para crear deep fakes difíciles de detectar se volverán técnicas de ataque más comunes.

SEGURIDAD PERSONAL MÓVIL

La seguridad móvil es ya una prioridad una prioridad. En unos años, la IA se utilizará de forma generalizada para proteger estos dispositivos y detectar amenazas en tiempo real.

AUMENTO DE LA IA EN LA CIBERSEGURIDAD

Aunque las soluciones de ciberseguridad más evolucionadas ya la incorporan, la IA se utilizará cada vez más de forma habitual para detectar vulnerabilidades y prevenir ciberataques en tiempo real. La información sobre filtraciones, exposiciones y actividades sospechosas que puedan suponer una amenaza para una persona determinada se recibirá en tiempo real para que se proteja con efectividad frente a ellas. Los sistemas de protección persona online serán herramientas de uso habitual y automatizado.

CIBERATAQUES ALTAMENTE DIRIGIDOS

Se observa ya una tendencia a que los ciberataques apunten directamente a las personas, el eslabón más débil de la cadena de la ciberseguridad, en lugar de apuntar a las organizaciones. De esta forma, las personas con puestos relevantes en las organizaciones están convirtiéndose a la vez en objetivo, para atacar su patrimonio y reputación personales, y medio, para alcanzar a la organización que dirigen o representan.

EL FUTURO DE LA SEGURIDAD ONLINE

DESAFÍOS

Privacidad de la información:

La recopilación y el análisis de grandes volúmenes de datos personales plantean preocupaciones sobre la privacidad de estos. Pero la irrupción de la IA en el contexto de la ciberseguridad pone en jaque no solo los datos recopilados por las organizaciones y administraciones sino la propia información personal expuesta públicamente por los individuos.

Sesgos en los algoritmos:

Los algoritmos de IA están diseñados por seres humanos y contienen sesgos, introducidos voluntaria o involuntariamente, que pueden afectar negativamente a ciertos grupos de personas y a su seguridad. Desarrollar habilidades profesionales para detectar y neutralizar esos sesgos y saberse proteger frente a ellos serán también actividades habituales en un futuro cercano.

Ciberseguridad:

La IA puede ser utilizada tanto para proteger como para atacar. Los sistemas de IA deben ser robustos y capaces de defenderse contra ataques sofisticados y, también, contra su uso para fines ilícitos.

OPORTUNIDADES

Mejor detección de amenazas:

La IA ya forma parte de las soluciones de ciberseguridad más evolucionadas, utilizándose para la localización de vulnerabilidades, el análisis de datos y la eliminación de los errores y falsos positivos.

Ciberseguridad automatizada:

La automatización permite que la detección de amenazas, la emisión de alarmas y la prevención de ataques sean continuas y en tiempo real, mejorando la eficiencia de las soluciones de ciberseguridad.

Normalización de la protección individual online:

La normalización actual de la protección de información, redes y sistemas de las organizaciones se extenderá a la protección individual online de las personas, con soluciones de uso particular para el control de la información personal expuesta y las actividades online que puedan suponer una amenaza para una persona determinada.

EL FUTURO DE LA SEGURIDAD ONLINE

qondar

Qondar Personal Watchbots es la plataforma desarrollada por Enthec que proporciona a las personas información en tiempo real sobre su identidad, datos personales y activos digitales y las actividades en curso relacionadas con ellos, para que puedan controlar su seguridad online.

Qondar proporciona información relacionada con la persona protegida sobre:

- Móvil: Personal y profesional
- Email: Personal y profesional
- Tarjeta de crédito
- Cuenta bancaria
- Wallet: Bitcoin, Ethereum
- Documentación: DNI, pasaporte, carnet de conducir, tarjeta sanitaria

FUNCIONALIDADES

- Búsqueda de información personal en filtraciones.
- Búsqueda de información del wallet.
- Búsqueda de información de la cuenta bancaria.
- Rastreo de la documentación personal.

BENEFICIOS PARA LA PERSONA PROTEGIDA

- Protección del patrimonio personal
- Protección de las comunicaciones personales y profesionales
- Protección de la reputación
- Protección frente a amenazas activas que impliquen riesgos personales o patrimoniales
- Protección frente a la suplantación de identidad digital

BENEFICIOS PARA LA ORGANIZACIÓN

- Protección frente al fraude del CEO, BEC y técnicas de ingeniería social.
- Protección de la información confidencial y sensible corporativa.
- Protección de las operaciones corporativas de alto nivel
- Protección financiera.

ENTHEC©

#WeAlreadyKnow

ENTHEC©

@enthec

@enthecsolutions

qondar