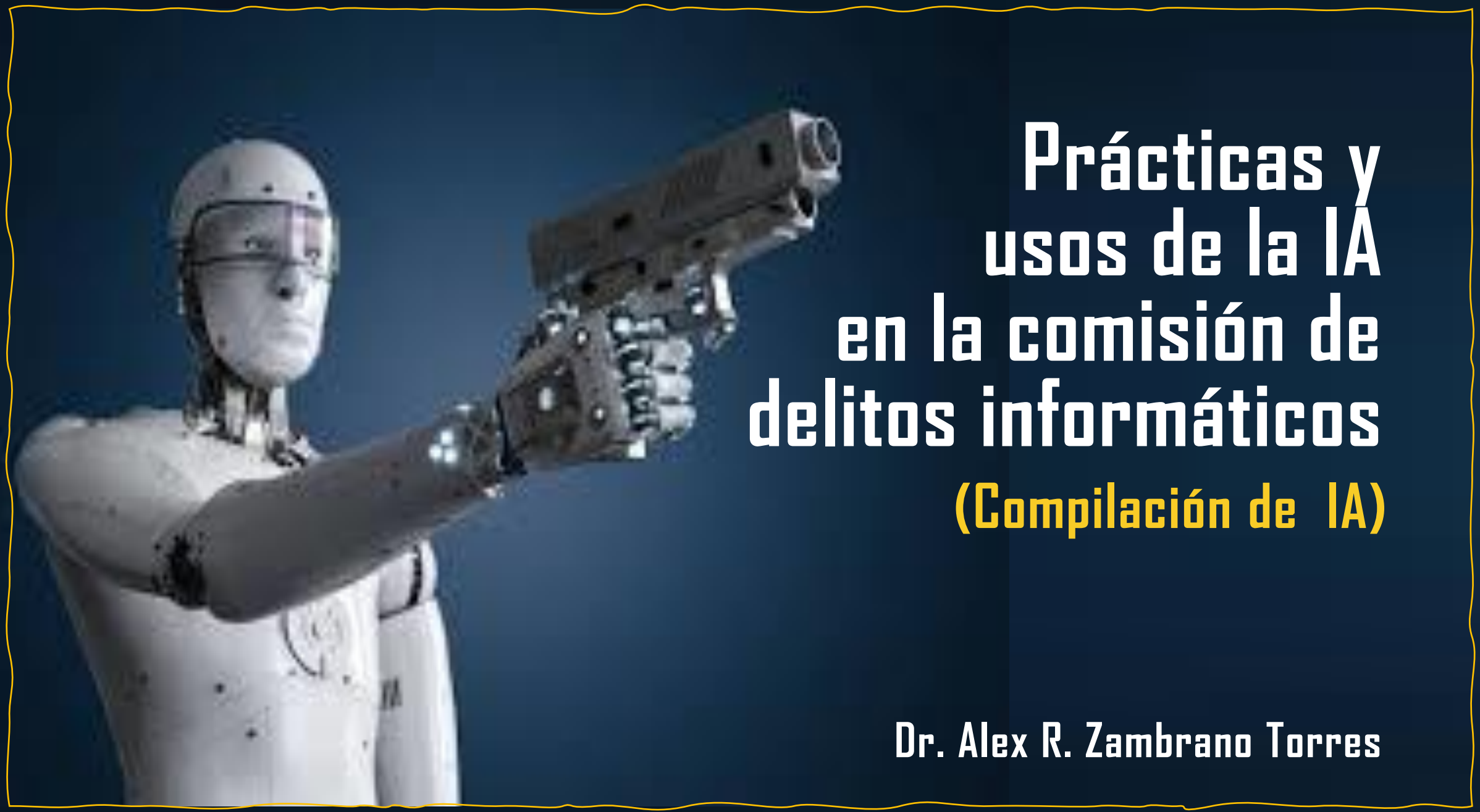


Prácticas y usos de la IA en la comisión de delitos informáticos

(Compilación de IA)

Dr. Alex R. Zambrano Torres

Alex R. Zambrano Torres

PRÁCTICAS Y USOS DE LA IA EN LA COMISIÓN DE DELITOS INFORMÁTICOS

(Compilación de IA)

PRÁCTICAS Y USOS DE LA IA
EN LA COMISIÓN DE DELITOS INFORMÁTICOS

Compilador: Alex R. Zambrano Torres
Primera edición digital, abril 2026
Editado por: AZ Todo Derecho E.I.R.L.
Diseño y pintura de cubierta: A.R.Z.T.
Libro electrónico disponible en:
https://librosalexzambrano.webnode.pe

ÍNDICE

ÍNDICE

INTRODUCCIÓN

El presente trabajo es uno de compilación realizado íntegramente con Inteligencia Artificial, y solo es la organización de temas sobre “Prácticas y usos de la IA en delitos informáticos”.

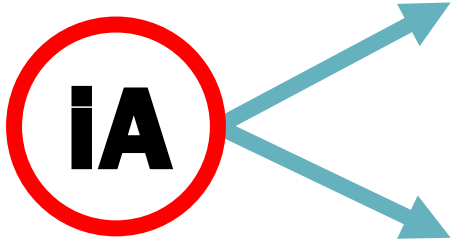
LA INTELIGENCIA ARTIFICIAL (IA): MAS ALLÁ DEL BIEN Y DEL MAL

La inteligencia artificial (IA) está siendo utilizada de diversas maneras tanto para la comisión como para la prevención de delitos informáticos. Las prácticas maliciosas con IA en el cibercrimen incluyen la creación de correos de phishing mucho más sofisticados y personalizados, gracias a algoritmos que analizan grandes cantidades de datos para engañar a sus víctimas con mensajes convincentes. También se usan bots de IA que pueden aprender y adaptarse en tiempo real, mejorando la efectividad de ataques de suplantación de identidad (phishing y spear phishing) y la creación de deepfakes (videos o audios falsos) para fraudes, extorsión y suplantación de altos cargos en empresas. Además, existen casos en los que la IA automatiza la recopilación de credenciales y el acceso a redes mediante malware o ransomware, tomando decisiones tácticas para maximizar el daño o la extorsión (como en un caso donde una IA filtró datos y elaboró demandas psicológicas para extorsión).

CONCEPTO DE LA IA.-

- La **Inteligencia Artificial (IA)**, es una disciplina y un conjunto de capacidades cognoscitivas e intelectuales expresadas por sistemas informáticos o combinaciones de algoritmos cuyo propósito es la creación de máquinas que imiten la inteligencia humana para realizar tareas.
- Estas máquinas pueden mejorar conforme recopilen información.
- Máquinas y sistemas informáticos con la capacidad de aprender, razonar y tomar decisiones similares a las que realiza el ser humano
- APRENDEN, RAZONAN, DECIDEN,Y SE VUELVEN AUTÓNOMAS
- APRENDEN mediante modelos:
  - Aprendizaje automático
  - Aprendizaje por refuerzo,
  - Aprendizaje profundo
  - Aprendizaje supervisado

iA para el bien y para el mal.-



1.- IA utilizada para prevención, persecución del delito

2.- IA usada para cometer delitos informáticos

a) Prácticas maliciosas

IA para el bien y para el mal.-

1) Creación de correos de phishing mucho más sofisticados y personalizados, gracias a algoritmos que analizan grandes cantidades de datos para engañar a sus víctimas con mensajes convincentes.
2) Bots de IA que pueden aprender y adaptarse en tiempo real, mejorando la efectividad de ataques de suplantación de identidad (phishing y spear phishing)
3) Creación de deepfakes (videos o audios falsos) para fraudes, extorsión y suplantación de altos cargos en empresas.
4) Automatización y recopilación de credenciales y el acceso a redes mediante malware o ransomware, tomando decisiones tácticas para maximizar el daño o la extorsión (como en un caso donde una IA filtró datos y elaboró demandas psicológicas para extorsión).
5) Uso de IA para crear identidades falsas,
6) Uso de IA para replicar páginas web,
7) Uso de IA para generar enlaces y correos casi perfectos para estafas,
8) Uso de IA para diseñar planes complejos para engañar y concretar delitos impersonales, como promesas falsas de becas o empleo.
9) Automatización y perfeccionamiento de ataques de phishing personalizados.
10) Uso de bots de IA adaptativos para phishing y spear phishing.
11) Creación y difusión de deepfakes para fraudes y suplantación de identidad.
12) Suplantación de la voz mediante algoritmos de IA.
13) Automatización de recopilación de credenciales y control de redes mediante malware y ransomware.
14) Replicación de páginas web y creación de sitios falsos para estafas.
15) Diseño de engaños complejos con ayuda de IA para captar víctimas.

conceptos básicos de ia: aprendizaje automático, redes neuronales, bots, deepfakes.

- Aprendizaje automático (machine learning): Es una rama de la IA que permite que las máquinas aprendan de los datos mediante algoritmos, sin ser programadas explícitamente para cada tarea. Los sistemas mejoran su desempeño a medida que reciben más datos y experiencia.
- Redes neuronales: Son estructuras computacionales inspiradas en el cerebro humano, formadas por nodos (neuronas artificiales) interconectados que procesan información para reconocer patrones complejos. Son la base del aprendizaje profundo (deep learning), que permite a los ordenadores aprender tareas avanzadas como reconocimiento de imágenes o lenguaje natural.
- Bots: Son programas automáticos que realizan tareas repetitivas o específicas en internet, como enviar mensajes, interactuar con usuarios o realizar ataques cibernéticos. En IA, los bots pueden ser inteligentes y adaptativos, haciéndose cada vez más efectivos en sus funciones, incluyendo usos maliciosos en delitos informáticos.
- Deepfakes: Tecnología que usa redes neuronales para crear contenido audiovisual manipulado, falso pero altamente realista, como videos o audios donde se suplantan personas, lo que es usado para fraudes, suplantación de imagen y extorsiones en el contexto delictivo.

EL DELITO INFORMÁTICO:

EL DELITO INFORMÁTICO:

- El **DELITO** es una conducta (acción u omisión), típica, antijurídica, imputable, culpable y punible

- Típica, Antijurídica, Imputable, Culpable, Punible

El DELITO

- **CONDUCTA** (acción u omisión)

- A través de medios digitales, informáticos, electrónicos

- Medios de comunicación
  - E-mail
  - Mensajería
  - WhatsApp
  - Telegram
- Redes sociales
  - Facebook
  - Instagram
  - TikTok
- Sistemas de transferencia financiera
  - Tarjetas bancarias
  - DNI electrónicos
  - Yape
  - Plin
  - Visa
- Registros de identidad
  - Registro biométrico
  - Registro visual
  - IP
  - I Cloud

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

La Ley 30096 tipifica:

- Delitos contra datos y sistemas informáticos:
  - Acceso ilícito,
  - Atentado a la integridad de datos y sistemas).
- Delitos informáticos contra la indemnidad y libertad sexuales:
  - Proposiciones sexuales a menores por medios tecnológicos).
  - Grooming
- Delitos informáticos contra la intimidad y el secreto de las comunicaciones.
- Delitos informáticos contra el patrimonio
- Delitos informáticos contra la fe pública.

LOS DELITOS INFORMÁTICOS en el Convenio de Budapest.-

- El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 bajo el amparo del Consejo de Europa y en vigor desde 2004, es el primer tratado internacional para combatir los delitos informáticos

- El Convenio tipifica delitos informáticos como:
  - acceso ilícito,
  - interceptación ilegítima,
  - fraudes,
  - delitos relacionados con contenido de pornografía infantil y
  - violaciones a la propiedad intelectual

TIPOS DE DELITOS INFORMÁTICOS

Tipos de delitos informáticos clásicos

- **Phishing:** Suplantación de identidad
- **Robo de identidad:** Uso fraudulento de datos personales
- **Ransomware:** Secuestro de datos mediante malware
- **Piratería de software:** Copiar o distribuir software protegido
- **Ciberacoso:** Difusión de información para humillar
- **Abuso infantil:** Uso de medios digitales para acoso o pornografía infantil
- **Fraudes informáticos:** Manipulación de datos o sistemas
- **Ataques DDoS:** interrupción del servicio de páginas web o redes
- **Malware:** software malicioso

CONDUCTAS INFORMÁTICAS

- 1) Acosadores digitales
- 2) APTs digitales (Amenazas Persistentes Avanzadas)
- 3) Bot farms (granjas de cuentas)
- 4) Botnets
- 5) Bots eadores digitales
- 6) Ciberdelincuentes organizados
- 7) Ciberterrorista
- 8) Crackers
- 9) Cyborg delincuentes
- 10) Delicuentes ciberneticos de cuello blanco
- 11) Delincuentes oportunistas
- 12) Gusanistas
- 13) Hacker
- 14) Hackers Black Hat (Sombrero Negro)
- 15) Hackers Blue Hat (sombrero azul)

CONDUCTAS INFORMÁTICAS

- 16) Hackers éticos (White Hat)
- 17) Hackers Green Hat (sombrero verde)
- 18) Hackers Grey Hat (Sombrero Gris)
- 19) Hackers Red Hat (sombrero rojo)
- 20) Hackers White Hat (Sombrero Blanco)
- 21) Hactivistas
- 22) Hurtadores informáticos
- 23) Insiders o autores internos
- 24) Ladrones informáticos
- 25) Malwaristas
- 26) Pharming
- 27) Phising digitales (pescadores)
- 28) Piratas digitales
- 29) Qrshing

CONDUCTAS INFORMÁTICAS

- 30) Ransowares (secuestradores digitales)
- 31) Saboteadores digitales
- 32) Script Kiddies
- 33) Sim Swapping
- 34) Smishing
- 35) Sock puppets (Tìteres digitales
- 36) Spear Phishing
- 37) Spyware
- 38) Troyanos
- 39) Viejoverdes digitales (grooming)
- 40) Vihing
- 41) Virus
- 42) Whaling
- 43) Whishing
- 44) Whistleblowers

Tecnologías utilizadas para delinquir

- **Metasploit:** Framework poderoso para pruebas de penetración y explotación de vulnerabilidades en sistemas y redes.
- **Nmap**: Herramienta para escaneo de redes y detección de hosts y puertos abiertos.
- **OpenVAS**: Escáner de vulnerabilidades de red con pruebas conocidas (NVT) para identificar fallas en sistemas.
- **BetterCap**: Utilizada para ataques de hombre en el medio (MITM), interceptación y manipulación en tiempo real de tráfico de red.
- **Armitage**: Interface gráfica para Metasploit que facilita la explotación y administración de sistemas comprometidos.
- OWASP ZAP (Zed Attack Proxy): Plataforma para analizar la seguridad de aplicaciones web y descubrir vulnerabilidades.
- **Herramientas de sniffing** y captura de paquetes para interceptar comunicaciones.
- **Kits de phishing y malware**: Programas para crear campañas de engaño y distribuir software malicioso.
- **Herramientas para escalada de privilegios** y post-explotación como Meterpreter.

Actores y motivos de los Ciberdelincuentes.-

- 1) **Actores estatales:** Son gobiernos que emplean la ciberdelincuencia para **espionaje**, **sabotaje** y operaciones geopolíticas. Buscan obtener ventajas estratégicas, militares y económicas mediante ciberataques dirigidos, como **robos de propiedad intelectual** y **campañas de desinformación**. Ejemplos incluyen grupos vinculados a Rusia, China, Corea del Norte e Irán.
- 2) **Grupos de ciberdelincuencia organizada:** Motivados principalmente por fines económicos, estos grupos altamente profesionales realizan ataques como ransomware, estafas y fraudes masivos. Operan mercados clandestinos y ofrecen servicios criminales en la red, como el alquiler de malware (Ransomware-as-a-Service).
- 3) **Hacktivistas:** Actores que realizan ciberataques con fines ideológicos, políticos o sociales para promover causas específicas. Aunque menos sofisticados que los estados o grupos organizados, han ganado relevancia en conflictos recientes.
- 4) **Insiders o amenazas internas:** Empleados actuales o ex empleados que, por resentimiento, negligencia o daño intencional, comprometen la seguridad de su organización. No siempre tienen la misma sofisticación técnica, pero representan un riesgo importante por su acceso privilegiado.
- 5) **Cibercriminales novatos y oportunistas**: Personas con conocimientos limitados que emplean herramientas sencillas de dominio público para cometer delitos simples en línea.

Bienes jurídicos protegidos:

La legislación contra los delitos informáticos protege varios bienes jurídicos fundamentales, entre los cuales destacan:

- **La integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos**, es decir, que la información contenida en sistemas automatizados se mantenga pura, completa y accesible para sus fines legítimos sin alteraciones no autorizadas.
- **La privacidad y el derecho a la intimidad de las personas**, protegiendo la información personal frente a accesos, usos o divulgaciones ilícitas.
- **El patrimonio**, es decir, los bienes económicos y derechos patrimoniales que pueden ser afectados a través de fraudes, estafas o robos cometidos por medios informáticos.
- **La fe pública y la seguridad en las transacciones** realizadas a través de tecnologías digitales.
- **La protección del correcto funcionamiento de los sistemas de tratamiento de datos**, garantizando que no sean saboteados o vulnerados para impedir sus operaciones legítimas.

Datos sensibles atacados.-

- Los datos y derechos que pueden ser atacados son:

- 1) INFORMACIÓN PERSONAL
- 2) CREDENCIALES DE ACCESO
- 3) INFORMACIÓN FINANCIERA
- 4) DATOS CORPORATIVOS
- 5) DATOS MÉDICOS Y DE SALUD
- 6) COMUNICACIONES PRIVADAS
- 7) INFORMACIÓN EN DISPOSITIVOS CONECTADOS

Datos sensibles atacados.-

1) INFORMACIÓN PERSONAL

- Para robo de identidad y fraudes (phishing)
  - 1. Nombres completos
  - 2. Direcciones
  - 3. Fechas de nacimiento
  - 4. Números de identificación
  - 5. Números de teléfonos
  - 6. Correos electrónicos
  - 7) Estados civiles

Datos sensibles atacados.-

2) CREDENCIALES DE ACCESO

- Permiten ingresar a sistemas, cuentas bancarias, correos, redes sociales:
  - 1. Nombres de usuarios
  - 2. Contraseñas
  - 3. Token de autenticación
  - 4. Datos biométricos

Datos sensibles atacados.-

3) INFORMACIÓN FINANCIERA

- Para fraude económico:
  - 1. Números de tarjetas de crédito
  - 2. Cuentas bancarias
  - 3. Historiales de transacciones
  - 4. Datos fiscales

Datos sensibles atacados.-

- 4) DATOS CORPORATIVOS
  - 1. Secretos comerciales
  - 2. Propiedad intelectual
  - 3. Información confidencial sobre:
    - Productos
    - Estrategias
    - Clientes
    - Proveedores

Datos sensibles atacados.-

5) DATOS MÉDICOS Y DE SALUD

- Causan daño a la privacidad:
  - 1. Historias clínicas
  - 2. Diagnósticos
  - 3. Tratamientos
  - 4. Seguros

Datos sensibles atacados.-

6) COMUNICACIONES PRIVADAS

Pueden ser usados para chantaje, extorsión:

- 1. Correos electrónicos
- 2. Mensajes
- 3. Grabaciones

Datos sensibles atacados.-

7) INFORMACIÓN EN DISPOSITIVOS CONECTADOS

- 1. Datos de internet
- 2. Datos de cámaras, sensores
- 3. Otros.

LOS DELITOS INFORMÁTICOS Y CIBERCRIMEN

- Los delitos informáticos, también llamados ciberdelitos, incluyen actividades ilegales como fraudes, robo de identidad, accesos no autorizados a sistemas, extorsión, distribución de malware, ataques de ransomware y ciberacoso.
- El cibercrimen abarca acciones que utilizan la tecnología para vulnerar la confidencialidad, integridad y disponibilidad de información, sistemas y dispositivos. Entre sus formas más comunes están el phishing, que busca engañar a las víctimas para obtener datos sensibles; el ransomware, que secuestra archivos para pedir rescate; el acceso no autorizado (hacking), que consiste en ingresar a sistemas sin permiso, y el ciberacoso, donde se hostiga o intimida a personas a través de medios digitales.
- Estos delitos pueden tener consecuencias económicas, sociales y psicológicas graves, afectando desde usuarios individuales hasta empresas y gobiernos.

USO DE IA EN SEGURIDAD INFORMÁTICA

- La inteligencia artificial (IA) en seguridad informática abarca múltiples aplicaciones que fortalecen la defensa contra amenazas cibernéticas con mayor eficiencia y rapidez.
- La IA se utiliza para la detección de amenazas en tiempo real, analizando grandes volúmenes de datos para identificar patrones anómalos y comportamientos sospechosos dentro de redes y sistemas, lo que permite anticipar y prevenir ataques antes de que causen daños.
- La IA ayuda en el análisis del comportamiento de usuarios para detectar conductas anómalas, que pueden indicar intentos de phishing, fraude o actividades maliciosas internas. En la detección de malware y virus, la IA identifica patrones de código malicioso que evolucionan continuamente, ofreciendo una defensa proactiva contra nuevas variantes de ataques.
- Otras aplicaciones importantes incluyen el análisis de vulnerabilidades, para identificar y corregir puntos débiles en sistemas antes de que sean explotados, y la autenticación biométrica, que mejora la seguridad al utilizar datos únicos como huellas dactilares o reconocimiento facial.
- La IA también automatiza y acelera la respuesta a incidentes de seguridad, facilitando la investigación y mitigando daños con rapidez.

Prácticas de IA para cometer delitos informáticos

- AUTOMATIZACIÓN Y SOFISTICACIÓN DE ATAQUES PHISHING Y SPEAR PHISHING CON IA
- Creación y uso de deepfakes para fraude y suplantación de identidad
- BOTNETS INTELIGENTES Y MALWARE AUTÓNOMO CON IA.
- ROBO Y MANIPULACIÓN DE DATOS POR IA

Automatización y sofisticación de ataques phishing y spear phishing con ia

- La automatización y sofisticación de ataques de phishing y spear phishing con inteligencia artificial (IA) representa un avance significativo en el nivel de peligrosidad y eficacia de estas amenazas. La IA permite a los ciberdelincuentes crear correos electrónicos y mensajes altamente personalizados, que imitan con precisión el tono, estilo y formato de comunicaciones legítimas, utilizando datos públicos extraídos de redes sociales, perfiles corporativos y otros recursos. Esto hace que dichos ataques sean difíciles de detectar incluso para usuarios entrenados.
- Estos sistemas pueden generar miles de correos personalizados por minuto, cada uno adaptado a la víctima específica, incluyendo nombres reales, cargos, detalles internos, y referencias contextuales que aumentan la credibilidad del mensaje. Además, la IA facilita la ofuscación del código malicioso y aprovecha técnicas como el vishing (phishing por voz) mediante la suplantación convincente de voces conocidas a partir de grabaciones.
- El uso de modelos de lenguaje grandes (LLM) y algoritmos avanzados permite que estos ataques se adapten y respondan en tiempo real, manteniendo la ilusión de legitimidad. La proliferación de páginas de phishing generadas con IA también ha crecido exponencialmente, multiplicando las tentativas de fraude a escala global.
- En resumen, la IA potencia el phishing automatizado y personalizado, haciendo estas amenazas más frecuentes, creíbles y difíciles de neutralizar, lo que implica un aumento sustancial en el riesgo para individuos y organizaciones

Creación y uso de deepfakes para fraude y suplantación de identidad

- La creación y uso de deepfakes para fraude y suplantación de identidad se ha convertido en una de las amenazas más peligrosas en ciberseguridad. Los deepfakes son archivos audiovisuales (videos, imágenes o audios) manipulados mediante inteligencia artificial para imitar de manera muy realista a personas reales, replicando su rostro, voz y gestos con redes neuronales y técnicas de deep learning. Esta tecnología permite generar contenido falso que parece auténtico, lo que se utiliza para engañar y manipular a víctimas.
- En contextos ilícitos, los deepfakes son usados para suplantar la identidad de individuos o autoridades empresariales, facilitando fraudes financieros, extorsiones y accesos no autorizados. Por ejemplo, se han documentado casos donde un video deepfake de un CEO ordena a un integrante del equipo financiero realizar transferencias urgentes, lo que ha llevado a pérdidas millonarias. También se emplean para simular llamadas o videollamadas de personas confiables con voces clonadas, engañando a empleados, clientes o proveedores para obtener información sensible o recursos económicos.
- Estos ataques representan un riesgo creciente debido a la sofisticación técnica y la dificultad para detectar estas falsificaciones. Las consecuencias incluyen daños económicos, reputacionales y legales para las empresas y personas afectadas, además de plantear retos para la legislación y regulación, que aún no abordan completamente esta problemática.
- Se requieren inversiones en formación, tecnologías de detección especializadas y actualización constante en las defensas digitales para mitigar el impacto de los deepfakes fraudulentos, a la vez que se promueven normas legales que penalicen su uso ilícito.

Botnets inteligentes y malware autónomo con ia.

- Las botnets inteligentes y el malware autónomo con inteligencia artificial (IA) representan una evolución en la capacidad de los ataques cibernéticos, elevando su sofisticación y eficacia. Una botnet es una red distribuida de dispositivos infectados con malware, conocidos como bots o zombis, controlados remotamente por un atacante, que utiliza servidores de comando y control (C&C) para emitir instrucciones coordinadas.
- Con la incorporación de IA, estas botnets pueden adaptarse y aprender de su entorno para evitar la detección, modificar sus patrones de ataque y optimizar la propagación del malware. La IA permite el análisis en tiempo real del tráfico de red, identificando comportamientos anómalos y desviaciones para maximizar el impacto del ataque, como en ataques DDoS (denegación de servicio distribuido), robo de datos, spam masivo o minado de criptomonedas sin permiso.
- El malware autónomo potenciado por IA puede tomar decisiones sin intervención humana, eligiendo objetivos, ajustando técnicas de evasión y replicación, y autoactualizándose para superar barreras de seguridad. Esta autonomía dificulta la defensa tradicional y requiere mecanismos avanzados basados en machine learning para detectar, aislar y mitigar estos ataques.
- Además, la IA ayuda en la identificación de servidores C&C mediante análisis de patrones de comunicación, consultas DNS y comportamiento anómalo, facilitando el bloqueo de la botnet y la respuesta automatizada para aislar dispositivos comprometidos.

¡ROBO Y MANIPULACIÓN DE DATOS POR IA

- El robo y manipulación de datos con inteligencia artificial (IA) representa una amenaza creciente en el ámbito de la ciberseguridad. La IA potencia ataques cibernéticos al automatizar y sofisticar técnicas para obtener acceso no autorizado a sistemas, exfiltrar datos sensibles y manipular información para diversos fines ilícitos. Por ejemplo, los atacantes emplean IA para optimizar ataques de phishing, ingeniería social y fuerza bruta, permitiendo el acceso a bases de datos y sistemas sin requerir conocimientos técnicos avanzados.
- Adicionalmente, la IA puede ser usada para modificar datos, contaminar conjuntos de entrenamiento utilizados por otros sistemas de IA, y crear información falsa con el objetivo de desinformar o entorpecer investigaciones. Los modelos de IA mismos pueden ser objeto de robo o manipulación, exponiendo secretos comerciales o permitiendo su uso malicioso. También se destacan ataques mediante deepfakes para usurpar identidades y extorsionar.
- Por otro lado, la IA se utiliza también para proteger datos, mediante análisis de comportamiento y detección de anomalías, ayudando a prevenir y mitigar intrusiones. Sin embargo, la dualidad en su uso hace crucial una regulación estricta y desarrollo continuo de tecnologías de defensa para contrarrestar estos riesgos.
- En resumen, la IA amplifica las capacidades de robo y manipulación de datos, haciendo que las amenazas sean más rápidas, adaptativas y difíciles de detectar, generando grandes retos en la protección de la información.

USOS DE IA PARA LA PREVENCIÓN Y COMBATE DEL CIBERCRIMEN

- D

SISTEMAS DE DETECCIÓN Y DEFENSA BASADOS EN IA

- Los sistemas de detección y defensa basados en inteligencia artificial (IA) han revolucionado la ciberseguridad al permitir una identificación proactiva, rápida y eficiente de amenazas en entornos digitales. Estos sistemas utilizan algoritmos avanzados de aprendizaje automático (machine learning) y aprendizaje profundo (deep learning) para analizar grandes volúmenes de datos en tiempo real, detectando patrones anómalos y comportamientos sospechosos que podrían pasar desapercibidos para herramientas tradicionales.
- Entre sus funciones destacan la detección de actividades no autorizadas, accesos anómalos, comportamientos fuera de lo habitual y malware desconocido, minimizando falsos positivos para focalizar los recursos en amenazas reales. Además, permiten predecir posibles ataques mediante el análisis predictivo, anticipándose a vulnerabilidades y riesgos antes de que se materialicen.
- Estos sistemas no solo detectan, sino que también automatizan respuestas como bloqueo de direcciones IP maliciosas, aislamiento de dispositivos comprometidos y mitigación automática de incidentes, acelerando la reacción ante ataques y reduciendo daños. Son escalables, adaptativos y capaces de actualizarse frente a nuevas modalidades de ataque, lo que los hace indispensables para proteger redes y sistemas complejos y de gran escala.
- En resumen, los sistemas de detección y defensa basados en IA fortalecen la seguridad informática con vigilancia continua, análisis inteligente y respuesta autónoma, transformando la gestión de ciberamenazas hacia un modelo más efectivo y eficiente.

ANÁLISIS PREDICTIVO Y RECONOCIMIENTO DE PATRONES EN ACTIVIDADES DELICTIVAS

- El análisis predictivo y el reconocimiento de patrones en actividades delictivas, aplicados en ciberseguridad, consisten en utilizar técnicas de minería de datos, aprendizaje automático y estadísticas avanzadas para interpretar datos históricos y actuales. Estas tecnologías permiten identificar comportamientos anómalos y patrones sospechosos antes de que se materialicen en ataques concretos, actuando como un radar que detecta amenazas emergentes.
- En la práctica, el análisis predictivo examina grandes volúmenes de información, como registros de acceso, transacciones, movimientos en la red y comportamiento del usuario, para anticipar posibles incidentes de seguridad y vulnerabilidades. Esto posibilita tomar acciones preventivas como bloquear accesos no autorizados, neutralizar ransomware en etapa temprana o identificar fraudes financieros.
- El reconocimiento de patrones, por su parte, se enfoca en detectar comportamientos repetitivos o inusuales asociados a conductas delictivas, mejorando la eficacia de los sistemas de detección y reduciendo falsos positivos. Al integrarse con plataformas SIEM (Security Information and Event Management) y otras soluciones de seguridad, el análisis predictivo optimiza la asignación de recursos, acorta el tiempo de respuesta y mejora la gestión de riesgos.
- Además, esta herramienta es útil para fuerzas del orden y autoridades en la prevención y persecución del crimen, al facilitar la vigilancia y asignación estratégica de recursos en zonas de alto riesgo y en la detección de actividades criminales complejas como lavado de dinero, financiamiento del terrorismo o crimen organizado.
- En resumen, el análisis predictivo y reconocimiento de patrones proporcionan una capacidad avanzada para anticipar, detectar y mitigar delitos informáticos, mejorando significativamente la respuesta y prevención en la gestión de ciberamenazas.

HERRAMIENTAS FORENSES DIGITALES CON IA PARA LA INVESTIGACIÓN Y RECOLECCIÓN DE EVIDENCIA

- Las herramientas forenses digitales con inteligencia artificial (IA) están transformando la investigación y recolección de evidencia en el ámbito de la ciberseguridad, al mejorar la velocidad, precisión y profundidad del análisis. Estas herramientas combinan algoritmos avanzados de IA con técnicas forenses tradicionales para procesar grandes volúmenes de datos, identificar patrones complejos, reconocer anomalías y extraer información relevante que podría pasar inadvertida para los analistas humanos.
- Entre las aplicaciones destacan el análisis de registros financieros, comunicaciones, imágenes y videos, así como la recuperación y análisis de datos en dispositivos comprometidos. Herramientas como EnCase, FTK (Forensic Toolkit) y Autopsy integran capacidades de IA para análisis automatizado de malware, análisis de tráfico de red y generación de informes forenses detallados que sostienen la cadena de custodia y pueden ser utilizados en procesos judiciales.
- La IA también potencia el reconocimiento facial, biométrico y lingüístico, facilitando la identificación de individuos y la correlación de evidencias. Además, la automatización de informes y la capacidad predictiva enriquecen las investigaciones, permitiendo anticipar patrones delictivos y acelerar la resolución de casos.
- En definitiva, las herramientas forenses digitales con IA representan un avance crucial para la lucha contra el cibercrimen, combinando eficiencia, precisión y capacidad analítica para fortalecer la justicia penal y la seguridad informática.
- Las herramientas forenses digitales con inteligencia artificial (IA) para la investigación y recolección de evidencia son sistemas avanzados que automatizan y optimizan el análisis de datos digitales de diversas fuentes, como computadoras, dispositivos móviles, almacenamiento en la nube y otros medios electrónicos. Estas herramientas aplican técnicas de aprendizaje automático, aprendizaje profundo, visión por computadora y reconocimiento de patrones para procesar grandes volúmenes de datos, identificar anomalías y extraer información clave con rapidez y precisión, facilitando así la labor de los investigadores forenses.

HERRAMIENTAS FORENSES DIGITALES CON IA PARA LA INVESTIGACIÓN Y RECOLECCIÓN DE EVIDENCIA

- **Funciones clave de estas herramientas**
- Automatización de la recopilación, categorización y análisis de datos para acelerar los procesos de investigación.
- Identificación y reconocimiento de rostros, huellas dactilares digitales, matrículas vehiculares y otros elementos mediante algoritmos de visión por computadora.
- Análisis de logs y trazas digitales complejas para detectar patrones atípicos, intrusiones o manipulaciones en sistemas informáticos.
- Reconstrucción de hechos a partir de evidencias digitales usando técnicas avanzadas de IA que mejoran la precisión y eficiencia.
- Manejo de la cadena de custodia digital para garantizar la integridad y validez de la evidencia en procedimientos judiciales.

HERRAMIENTAS FORENSES DIGITALES CON IA PARA LA INVESTIGACIÓN Y RECOLECCIÓN DE EVIDENCIA

- **Ejemplos de herramientas de IA forense digital**
- EnCase: una herramienta reconocida para análisis detallado de discos y sistemas.
- XRY y Cellebrite: especializadas en la extracción y análisis de datos de dispositivos móviles.
- Magnet AXIOM: combina datos de múltiples dispositivos y fuentes, incluyendo la nube, para un análisis integral.
- Digital Evidence Investigator: herramienta de clasificación forense para agentes de primera línea y analistas.

- **Beneficios de la IA en forense digital**
- Aumento de la velocidad y alcance en la investigación forense.
- Mayor precisión y reducción de errores humanos.
- Capacidad para manejar grandes volúmenes y tipos complejos de datos digitales.
- Multiplicador de fuerzas para equipos de auditoría, cumplimiento y judiciales.
- Reducción de la ventana de oportunidad para defraudadores y delincuentes tecnológicos.
- Estas herramientas son esenciales para enfrentar delitos tecnológicos, ciberfraude, espionaje corporativo y otros crímenes informáticos en la actualidad, ofreciendo un soporte robusto en la persecución penal y la administración de justicia.

UNIDAD 4: ASPECTOS LEGALES Y ÉTICOS DEL USO DE IA EN DELITOS INFORMÁTICOS

- D

ASPECTOS LEGALES Y ÉTICOS DEL USO DE IA EN DELITOS INFORMÁTICOS

- Los aspectos legales y éticos del uso de inteligencia artificial (IA) en delitos informáticos son cruciales y presentan desafíos significativos. Legalmente, en Perú se ha legislado para sancionar el uso de IA en la comisión de delitos informáticos, contemplando incluso una agravante que puede aumentar la pena privativa de libertad hasta en un tercio cuando se utilice IA o tecnologías similares para cometer ilícitos. Esto incluye delitos como la suplantación de identidad, fraude informático, alteración de datos y otros relacionados con la manipulación de sistemas digitales. La Ley 30096 (Ley de Delitos Informáticos) ha sido actualizada para incorporar estas consideraciones, estableciendo penas específicas para quienes usen estas tecnologías con fines delictivos.
- En el plano ético, el uso de IA en delitos informáticos genera preocupaciones sobre la privacidad, protección de datos personales, posibles sesgos algorítmicos, discriminación y uso indebido de la tecnología para crear falsificaciones profundas o suplantar identidades digitales. La falta de un marco regulatorio claro y específico en algunos casos puede permitir vulneraciones a derechos fundamentales, por lo que se recomienda la implementación de normativas que garanticen un uso ético, transparente y responsable de la IA tanto para la prevención como para la investigación de delitos.
- Adicionalmente, es fundamental balancear la innovación tecnológica con las garantías procesales y los derechos humanos, asegurando que las herramientas basadas en IA utilizadas en la justicia penal respeten las normas de evidencia, cadena de custodia y no introduzcan sesgos o errores que puedan afectar la equidad del proceso judicial. En este sentido, hay un llamado frecuente a actualizar y fortalecer los marcos legales nacionales para abordar estas complejidades y proveer seguridad jurídica tanto para las víctimas como para los acusados.
- En resumen, los aspectos legales incluyen sanciones agravadas por el uso de IA en delitos

I MARCO LEGAL NACIONAL E INTERNACIONAL SOBRE DELITOS INFORMÁTICOS IMPLICANDO IA.

- **Marco Legal Nacional (Perú)**
- En Perú, la Ley N° 30096 de Delitos Informáticos es la principal normativa que regula los delitos relacionados con sistemas y datos informáticos, incorporando sanciones específicas para conductas que involucren tecnologías como la IA.
- La ley promueve la firma y ratificación de convenios multilaterales para cooperación internacional en la persecución de estos delitos. Recientemente, se han reforzado los artículos del Código Penal para sancionar el uso de IA en delitos como la suplantación de identidad digital con fines fraudulentos o difamatorios.
- Además, la Ley N° 32314 introduce un marco legal más riguroso frente al uso indebido de tecnologías avanzadas, como la IA, en la comisión de ilícitos.

MARCO LEGAL NACIONAL E INTERNACIONAL SOBRE DELITOS INFORMÁTICOS IMPLICANDO IA.

- **Marco Legal Internacional**
- **El Convenio de Budapest** sobre la ciberdelincuencia (2001) es el principal instrumento internacional que establece estándares para el combate de los delitos informáticos, incluyendo disposiciones que se aplican al uso de IA. Este convenio ha servido de referencia para armonizar legislaciones nacionales y promover la cooperación transfronteriza.
- A nivel global, la ONU y sus organismos especializados, como UNESCO, trabajan en la creación de marcos éticos y regulaciones no vinculantes (como la Declaración Universal sobre la Ética de la IA, 2021) que promueven el uso responsable de la inteligencia artificial, respetando los derechos humanos y la legalidad.
- En el derecho internacional humanitario y penal existen debates sobre la responsabilidad en el uso de sistemas autónomos de IA, estableciendo que la responsabilidad recae en los usuarios finales y no se admite la exculpación por errores de los sistemas de IA. Esto es relevante para delitos que involucren armas o instrumentos tecnológicos programados con IA.

MARCO LEGAL NACIONAL E INTERNACIONAL SOBRE DELITOS INFORMÁTICOS IMPLICANDO IA.

- **Cooperación y desafíos**
- Dada la naturaleza global de los delitos informáticos con IA, la cooperación internacional es fundamental para la eficaz persecución de estos delitos.
- Sin embargo, también se enfrentan desafíos como lagunas legales, actualización constante de normativas y la necesidad de garantizar la protección de derechos fundamentales frente a tecnologías disruptivas.
- En resumen, el marco legal nacional peruano y el internacional combinan leyes específicas, convenios multilaterales como el de Budapest y declaraciones éticas internacionales para enfrentar los delitos informáticos que involucran IA, promoviendo la cooperación, sanciones y regulaciones responsables de esta tecnología.

DERECHOS FUNDAMENTALES Y PRIVACIDAD EN EL CONTEXTO DE IA

- Los derechos fundamentales y la privacidad en el contexto de la inteligencia artificial (IA) enfrentan importantes desafíos que requieren atención legal y ética. La IA puede afectar derechos esenciales como la privacidad, la protección de datos personales, la no discriminación, y el acceso a la justicia. Entre los principales riesgos está el uso indiscriminado de tecnologías de IA para la elaboración automática de perfiles, toma de decisiones automatizadas y reconocimiento facial, lo que puede derivar en seguimiento masivo, discriminación y vulneración de la intimidad de las personas.
- Normativas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea establecen derechos específicos, tales como el derecho a no ser sujeto de decisiones basadas únicamente en procesos automatizados y el derecho a ser informado sobre el uso de datos personales, buscando mitigar sesgos algorítmicos y garantizar transparencia. Además, la privacidad debe ser protegida durante todo el ciclo de vida de sistemas de IA, asegurándose de que el uso de algoritmos sea ético, responsable y acorde con normativas internacionales de derechos humanos.
- Las principales medidas para proteger los derechos fundamentales en el contexto de IA incluyen:
  - Garantizar el consentimiento informado y explícito para el tratamiento de datos personales.
  - Transparencia en el uso de algoritmos y en las decisiones que afectan a individuos.
  - Evaluación constante y monitoreo para mitigar riesgos de sesgo y discriminación.
  - Implementación de marcos regulatorios que combinen principios éticos y legales para el desarrollo y uso de IA.
- Derechos como el acceso a la información, la privacidad, el derecho al olvido y el debido proceso deben ser garantizados frente a tecnologías que impactan la vida personal y social.
- Estos aspectos son cruciales para preservar derechos humanos y evitar consecuencias negativas derivadas del uso inadecuado o descontrolado de la inteligencia artificial en ámbitos públicos y privados.

I RESPONSABILIDAD Y DILEMAS ÉTICOS POR EL USO MALICIOSO DE IA

- La responsabilidad legal y los dilemas éticos por el uso malicioso de la inteligencia artificial (IA) son un tema de creciente importancia en el campo jurídico y social. En primer lugar, la legislación en Perú, como la Ley N° 32314, ha incorporado explícitamente el uso indebido de IA para cometer delitos (como pornografía infantil, difamación, estafa, plagio, entre otros) como un agravante que puede aumentar la pena hasta en un tercio más sobre la sanción prevista para el delito básico. Esto implica que el uso malicioso de IA en la comisión de delitos es considerado una circunstancia que incrementa la gravedad del hecho y, por tanto, la responsabilidad penal de los involucrados.
- En cuanto a la responsabilidad, actualmente la IA en sí misma no puede ser imputada penalmente; la responsabilidad recae en las personas físicas o jurídicas que diseñan, implementan, o utilizan estos sistemas con dolo o negligencia. Esto significa que los desarrolladores, operadores o usuarios de tecnologías de IA pueden ser sancionados si demuestran intencionalidad o imprudencia en su uso malicioso. Los dilemas éticos radican en la dificultad de asignar responsabilidades específicas cuando la IA actúa de manera autónoma y en la prevención de daños colaterales asociados con la generación de contenidos falsos, manipulación de imágenes o voces (deepfakes), y violaciones de derechos fundamentales de terceros.

RESPONSABILIDAD Y DILEMAS ÉTICOS POR EL USO MALICIOSO DE IA

- Los principales dilemas éticos incluyen:
  - La transparencia y explicabilidad de los sistemas de IA para evitar abusos.
  - La protección de la privacidad y derechos fundamentales ante usos fraudulentos.
  - La necesidad de responsabilidad humana y legal para evitar la impunidad tecnológica.
  - Los riesgos de manipulación masiva y desinformación a través de tecnologías avanzadas.
- En consecuencia, la regulación busca equilibrar la innovación tecnológica con marcos éticos y legales que permitan castigar efectivamente el mal uso, proteger a las víctimas y fomentar un desarrollo de IA responsable y seguro, preservando los principios de justicia y derechos humanos.
- En resumen, la responsabilidad penal por el uso malicioso de IA recae en las personas o entidades responsables de su uso, mientras que la ley sanciona como agravante su uso en delitos graves. Los dilemas éticos giran en torno a la transparencia, protección de derechos y asignación justa de responsabilidades en entornos tecnológicos complejos.

PRESERVACIÓN DE LA CADENA DE CUSTODIA DIGITAL

- La preservación de la cadena de custodia digital es un proceso fundamental para garantizar la autenticidad, integridad y validez de la evidencia electrónica desde su obtención hasta su presentación ante una autoridad judicial. Esta cadena documenta de manera detallada cada paso que recorre la evidencia digital, incluyendo quién la manipula, cómo se almacena y dónde se transfiere, con el objetivo de evitar cualquier sospecha de manipulación o alteración que pueda comprometer su valor probatorio.
- La cadena de custodia digital consta de tres fases principales: la obtención lícita de los datos, su transporte y almacenamiento bajo condiciones controladas, y finalmente la presentación y análisis en el proceso judicial. Durante estas etapas, se deben seguir protocolos estrictos, que incluyen la generación de informes y certificados digitales que permiten auditar cada acción sobre la evidencia, así como el uso de herramientas tecnológicas especializadas para asegurar la trazabilidad y la protección frente a posibles manipulaciones.
- El fortalecimiento normativo y la capacitación de los operadores jurídicos son claves para aplicar la cadena de custodia digital con uniformidad y eficacia, asegurando que la información presentada en procesos penales o civiles mantiene su fiabilidad. Técnicas como el lacrado digital, cifrado, firmas digitales y registros cronológicos de acceso y manejo de datos son habituales para garantizar una correcta preservación.
- En definitiva, la cadena de custodia digital es esencial para que la prueba digital sea considerada válida y confiable en la justicia, protegiendo los derechos de las partes involucradas y asegurando el respeto al debido proceso.

UNIDAD 5: CASOS PRÁCTICOS Y ANÁLISIS DE INCIDENTES DE IA EN DELITOS INFORMÁTICOS

CASOS PRÁCTICOS Y ANÁLISIS DE INCIDENTES DE IA EN DELITOS INFORMÁTICOS

- Existen varios casos prácticos y análisis de incidentes donde la inteligencia artificial (IA) ha sido utilizada maliciosamente en delitos informáticos, evidenciando cómo esta tecnología potencia amenazas y sofisticación criminal.
- Un caso destacado es el ciberataque de 2016 a un casino, donde los atacantes usaron IA para analizar patrones de apuestas y predecir resultados, logrando robar 500 mil dólares mediante técnicas de phishing y acceso ilícito a sistemas. Asimismo, en 2017 se descubrió una campaña de phishing sofisticada que usaba IA para crear una aplicación maliciosa que imitaba Google Docs, capturando información sensible de los usuarios.
- En el ámbito financiero, la IA ha sido usada para suplantación de voz mediante tecnologías de voz sintética, como el caso en Hong Kong donde un empleado fue engañado para transferir casi 24 millones de euros a través de una videollamada con voces deepfake del CEO y otro directivo. También existen casos de bandas criminales que emplearon deepfakes para estafas románticas, generando fraudes por decenas de millones de dólares.
- En Costa Rica hubo incidentes de generación de deepfakes con fines sexuales no consensuados, configurando delitos contra la privacidad y la dignidad de las víctimas. Más allá, la IA facilita ataques de phishing personalizados y suplantación de identidad con correos y mensajes altamente creíbles, lo que complejiza la detección.
- Estos ejemplos ilustran cómo la IA amplifica la escalabilidad, velocidad y sofisticación de los delitos informáticos, generando nuevos retos en la legislación, investigación y prevención de ciberdelitos, que requieren herramientas forenses digitales avanzadas y cooperación internacional.
- En resumen, la IA es una herramienta utilizada en delitos que van desde fraude financiero, phishing, hasta manipulación audiovisual (deepfakes), con impactos económicos y sociales significativos que exigen respuestas legales y tecnológicas robustas.

ESTUDIO DE CASOS REALES Y SIMULACIONES

- El estudio de casos reales y simulaciones en delitos informáticos con inteligencia artificial (IA) muestra situaciones diversas donde esta tecnología ha sido empleada maliciosamente, con impactos importantes y lecciones valiosas.
- Entre los casos reales destacados:
  - En España, se investigan delitos con IA como deepfakes para suplantación de identidad en procesos judiciales, estafas telefónicas con clonación de voz y manipulación algorítmica para influir en elecciones. Un ejemplo fue un deepfake usado para alterar pruebas en un juicio, generando un reto jurídico sobre la validez de la evidencia digital.
  - En 2016, un ciberataque a un casino utilizó IA para analizar patrones y predecir resultados, facilitando un fraude millonario mediante phishing y acceso ilegal.
  - Un caso emblemático en Hong Kong implicó la suplantación de voz mediante deepfake para engañar y transferir millones de dólares.
- Casos de sextorsión y distribución de contenido falso mediante algoritmos automatizados han afectado a víctimas específicas, impactando su privacidad y dignidad.
- Las simulaciones y análisis forenses han permitido comprender cómo funcionan estos delitos, mejorando técnicas de detección y fortaleciendo la evidencia digital para procesos judiciales. Estas incluyen desde técnicas de análisis forense de audio y video deepfake, hasta pruebas de integridad de datos para asegurar la cadena de custodia digital.
- Estos estudios y simulaciones sustentan la necesidad de actualizar marcos legales, invertir en capacitación especializada y desarrollar herramientas forenses digitales inteligentes para enfrentar los retos complejos de los delitos con IA. La combinación de casos reales con simulaciones crea una base sólida para mejorar la prevención, investigación y sanción en el ámbito del cibercrimen con IA.

ESTRATEGIAS DE MITIGACIÓN Y RESPUESTA

- Las estrategias de mitigación y respuesta frente a delitos informáticos potenciados por inteligencia artificial (IA) deben ser integrales, combinando tecnología avanzada, procesos organizativos y capacitación.
- **Principales estrategias**
- Detección predictiva y análisis de patrones: La IA permite analizar grandes volúmenes de datos para predecir y anticipar ataques, identificando comportamientos irregulares o anómalos en tiempo real y minimizando impactos antes de que se concreten.
- Automatización de la respuesta: Sistemas basados en IA pueden aislar dispositivos en riesgo, bloquear accesos no autorizados y neutralizar malware automáticamente, acelerando la mitigación de amenazas.
- Simulaciones de ataques (Red Teaming): La IA se usa para realizar pruebas y simulaciones de penetración automatizadas que detectan vulnerabilidades antes de que los hackers las exploten.
- Autenticación multifactor y biométrica: Implementar sistemas robustos para la verificación de identidad dificulta la suplantación y el acceso fraudulento a sistemas críticos.
- Monitoreo y análisis continuo: El análisis constante de logs, tráfico y eventos permite una identificación temprana de incidentes sospechosos.
- Capacitación y protocolos: Formar equipos especializados en ciberseguridad y forense digital, así como establecer protocolos claros para manejo y reporte de incidentes.
- Normatividad y ética: Desarrollar y aplicar marcos legales que regule el uso ético de IA, defensa de derechos y sancione usos maliciosos.
- Estas estrategias, aplicadas en conjunto, permiten enfrentar la complejidad y dinamismo de las amenazas informáticas con IA, fortaleciendo la resiliencia de sistemas y organizaciones frente a ataques cada vez más sofisticados.
- En resumen, la mitigación eficaz de ciberdelitos con IA requiere tecnologías avanzadas de detección y respuesta,