ANÁLISIS DE LA CIBERDELINCUENCIA

DIRECCIÓN DE CIBERDELITOS
MINISTERIO DEL INTERIOR

Boletín

La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial.

Boletín de Análisis de la Ciberdelincuencia: “La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial”

Ministerio del Interior
Subsecretaría de Combate al Delito
Dirección de Ciberdelitos

Presidente de la República
MAGISTER DANIEL ROY-GILCHRIST NOBOA AZÍN

Ministra del Interior
DOCTORA MÓNICA ROSA IRENE PALENCIA NÚÑEZ

Viceministro del Interior
DOCTOR LYONEL FERNANDO CALDERÓN TELLO (E)

Subsecretario de Combate al Delito
TENIENTE CORONEL (SP) LUIS FERNANDO PÉREZ DÁVILA

Director de Ciberdelitos
MAGISTER JORGE FERNANDO ILLESCAS PEÑA

Responsables y Colaboradores

Redacción técnica del documento:
INGENIERO DIEGO TEJADA CAMPOS., Analista de Ciberdelitos
MAGISTER MARIO SIGCHA MOROCHZ., Analista de Ciberdelitos
MAGISTER GABRIEL REINOSO MARTÍNEZ., Analista de Ciberdelitos
MAGISTER CARLOS SIMBAÑA COBA., Analista de Ciberdelitos
INGENIERO CÉSAR TRELLES SEGOVIA., Analista de Ciberdelitos
Revisión
MAGISTER JORGE NÉJER GUERRERO, Especialista de Ciberdelitos
MAGISTER FREDDY GALLARDO SOSA, Especialista de Ciberdelitos
MAGISTER FERNANDO MOYA LEIMBERG, Especialista de Ciberdelitos

Redacción y compilación:
MAGISTER DUVAL MONTATIXE CAIZALUISA., Analista de Ciberdelitos

Edición y Adaptación:
MAGISTER JORGE FERNANDO ILLESCAS PEÑA, Director de Ciberdelitos

@Diciembre 2024

EL NUEVO ECUADOR Ministerio del Interior

Contenido

PRESENTACIÓN

La inteligencia artificial (IA) ha alcanzado un nivel de desarrollo y aplicación notable en la actualidad, impactando diversos sectores y transformando la vida cotidiana. A medida que la tecnología avanza, las aplicaciones de IA se vuelven cada vez más sofisticadas y omnipresentes, facilitando tareas y mejorando la eficiencia en múltiples ámbitos.

La inteligencia artificial está revolucionando tanto la forma en que se combate la delincuencia como los métodos utilizados por los delincuentes entre los más relevantes podemos robo de identidad, deepfakes, phishing automatizado. Si bien ofrece herramientas poderosas para mejorar la seguridad pública, también exige una reflexión crítica sobre su regulación y el impacto en los derechos individuales. La evolución continua de esta tecnología requerirá un enfoque equilibrado que maximice sus beneficios mientras se mitigan sus riesgos.

INTRODUCCIÓN

La inteligencia artificial es *"un campo técnico y científico dedicado al sistema de ingeniería que genera resultados como contenido, previsiones, recomendaciones o decisiones para un conjunto determinado de objetivos definidos por el ser humano"* (ISO/IEC, 22989:2022).

En las últimas décadas la inteligencia artificial (en adelante IA) ha transformado radicalmente diversos campos desde la educación, entretenimiento, salud, banca, comercio, industria entre otros, y se ha hecho más visible en estos años. La IA permite analizar el entorno y realizar acciones autónomas para optimizar procesos y mejorar la eficiencia en la toma de decisiones, basándose en algoritmos avanzados y volúmenes de datos, alcanzando objetivos específicos; influyendo cada vez más en la vida diaria y las decisiones sociales.

Sin embargo, a pesar de sus enormes ventajas, el uso de la IA ha generado inquietud tanto en lo ético como en lo legal, la capacidad de estas tecnologías para analizar grandes volúmenes de datos, tomar decisiones automatizadas y "aprender" patrones ha provocado preguntas sobre la privacidad, la seguridad y su potencial para abusos.

Entre los principales riesgos se encuentran la creación de sistemas de vigilancia cibernéticos, la manipulación de información a través de noticias falsas (fakes news), archivos multimedia manipulados por inteligencia por IA y la discriminación o sesgos a distintos grupos sociales. Por ello, la regulación y el debate ético sobre estas tecnologías son esenciales para minimizar los riesgos y garantizar su desarrollo y aplicación responsable.

El uso de la IA por parte de la delincuencia ha abierto nuevas oportunidades en el ámbito delictivo, planteando desafíos significativos para el combate a la ciberdelincuencia. Los delincuentes han aprovechado los avances en IA para automatizar ataques cibernéticos, crear malware, robar datos, incluso provocar fraude financiero hasta crear noticias falsas y algoritmos de minería ilegal de criptos, entre otras. La capacidad de estos sistemas para adaptarse y aprender de su entorno les permite operar de manera más sofisticada, burlando medidas de seguridad convencionales.

Esto obliga a los estados y autoridades a desarrollar nuevas estrategias para combatir esta creciente amenaza; la expansión de la IA en el ámbito delictivo no solo destaca la importancia de entender sus beneficios, sino también de abordar cuestiones éticas, legales y también de seguridad que surgen con su uso indebido.

Este boletín se enfoca en comprender el mal uso de la IA por parte de individuos o grupos de delincuencia y, cómo esta tecnología es utilizada para realizar actividades delictivas; exploramos el panorama "geo-ciberdelincuencial" mundial, regional y local, a través de casos, además de cómo los delincuentes utilizan diferentes técnicas y plataformas para realizar sus acciones delictivas, y entendiendo este fenómeno proponer acciones tanto en la prevención como en la respuesta.

Finalmente, se presentan estadísticas locales relacionadas con todos los ciberdelitos y delitos cometidos con el uso de tecnologías de la Información y Comunicación en el Ecuador.

Breve reseña de la evolución de Inteligencia Artificial (IA)

La historia de la IA muestra cómo la creatividad humana ha permitido avances significativos en la relación con las máquinas. Desde los planteamientos iniciales de Alan Turing en 1950 con su Test de Turing (Turing, 1950) hasta los sistemas avanzados que conocemos hoy, cada paso representa un aporte esencial en el desarrollo de la IA.

En 1956, el término "Inteligencia Artificial" marcó un hito y en los años siguientes, sistemas como ELIZA el primer chatbot conversacional en 1966 y Deep Blue que en 1997 derrotó al campeón mundial de ajedrez, demostraron las capacidades de lo que las máquinas pueden ser capaces de realizar. A este progreso se sumó IBM Watson, que en 2011 venció en el juego de trivia Jeopardy, gracias a su capacidad para procesar preguntas en lenguaje natural, buscar respuestas en grandes cantidades de datos y generar resultados en tiempo récord (Jara, s.f.). No obstante, los recursos computacionales eran aún limitados para llegar a los actuales avances de la IA.

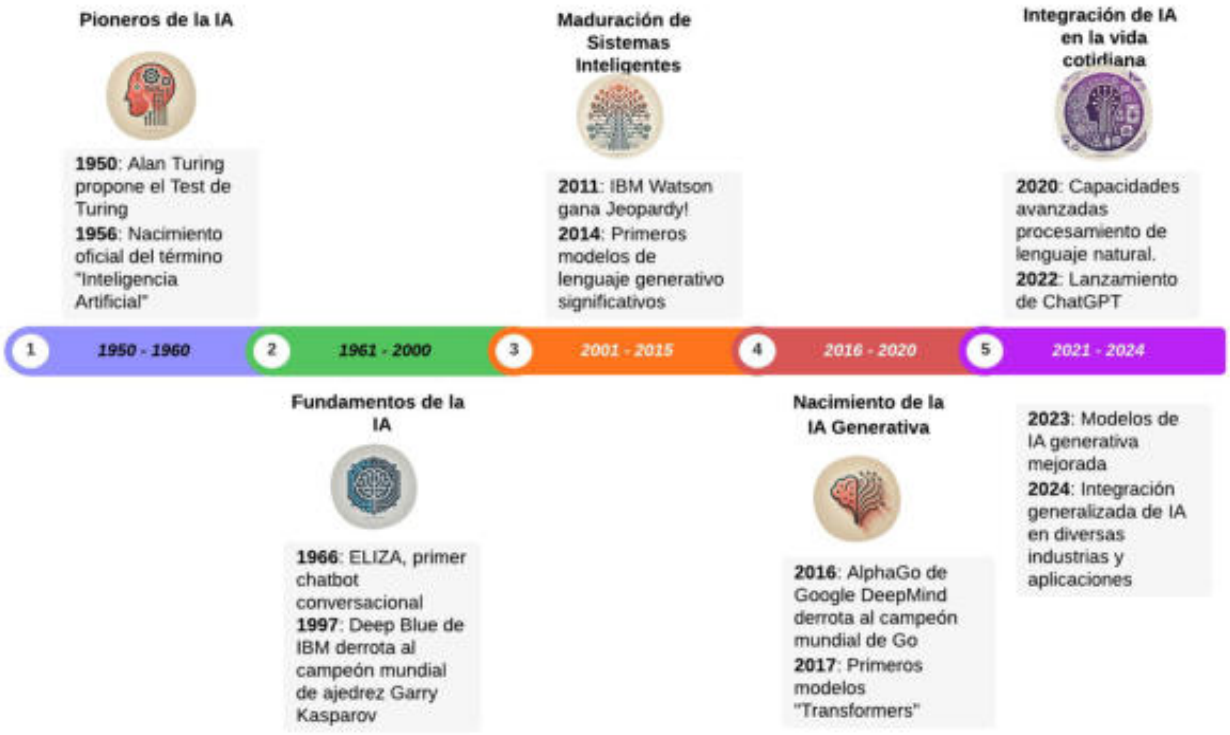
Esta limitación de recursos fue solventada mediante el uso de Unidades de Procesamiento Gráfico (GPUs). Estas tarjetas, diseñadas inicialmente para mejorar las imágenes en software gráfico y videojuegos, se convirtieron en una herramienta clave para procesar datos masivos gracias a su capacidad de realizar cálculos simultáneos en múltiples tareas pequeñas al mismo tiempo. Esto permitió a los investigadores trabajar con modelos cada vez más potentes y entrenarlos de forma más rápida y eficiente, acelerando significativamente los avances en la IA. (Mendoza, Uribe, Moncada, Morales, & Mantilla, s.f.)

A pesar de los avances alcanzados, el desarrollo de la IA enfrentaba un obstáculo significativo por la incapacidad de mantener el contexto en tareas extensas o complejas, perdiendo información crucial tras varias interacciones. En 2017, investigadores de Google abordaron y solventaron este reto desarrollando las bases teóricas para priorizar palabras clave o conceptos relevantes que permitía conservar información esencial a lo largo de las interacciones, mejorando la coherencia y la precisión

de los modelos de IA (Noam, 2020). Este logro se convirtió en la base de las capacidades avanzadas desarrolladas posteriormente por la empresa OpenAI (ChatGPT) y otras, de la manera como se conoce en la actualidad la IA con el procesamiento de lenguaje natural y su utilización en múltiples industrias.

De este modo, la IA se ha incorporado en las actividades de la vida cotidiana, ofreciendo grandes beneficios, aunque también generando desafíos en seguridad y ciberdelincuencia, ya que, como cualquier herramienta, puede usarse tanto para buenos propósitos así también para acciones indebidas.

***Imagen 1**: Evolución de la Inteligencia*



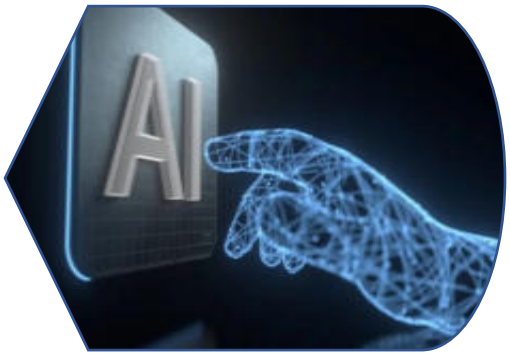
***Fuente**: Dirección de Ciberdelitos - Ministerio del Interior*

Ética y la Inteligencia Artificial

Cuando hablamos del impacto de la IA, debemos tener en cuenta el tema ético, la ética y la IA es un tema trascendental en la actualidad, la tecnología avanza rápidamente y afecta diversos aspectos de la vida humana.

La ética, entendida como la capacidad de pensar críticamente sobre los valores morales y dirigir nuestras acciones en términos de tales valores, es una capacidad humana genérica. (Churchill, 1999)

Los mismos derechos que tienen las personas fuera de línea deben protegerse también en línea, incluso durante todo el ciclo de vida de los sistemas de inteligencia artificial[2]



Algunos de los principales puntos de discusión en el tema ético incluyen:

1. **Responsabilidad:** ¿Quién es responsable cuando una IA comete un error o causa daño? Esto incluye desde los desarrolladores hasta las empresas que implementan sistemas de IA.
2. **Transparencia:** Los algoritmos de IA a menudo son complejos y opacos. Es importante garantizar que las decisiones tomadas por IA, especialmente en áreas sensibles como la salud, el derecho o las finanzas, sean comprensibles y explicables.
3. **Privacidad:** La IA puede procesar grandes cantidades de datos personales, lo que plantea preocupaciones sobre la protección de la privacidad y el uso indebido de información sensible.

4. **Discriminación:** Si las IA se entrenan con datos sesgados, pueden perpetuar o incluso amplificar las desigualdades sociales. Garantizar la equidad en los sistemas de IA es un desafío constante.
5. **Autonomía:** A medida que las IA asumen más funciones, surge el debate sobre cómo equilibrar la toma de decisiones automatizada con la autonomía humana, especialmente en decisiones que afectan la vida de las personas.
6. **Impacto en el empleo:** La automatización impulsada por IA puede reemplazar trabajos, lo que genera debates sobre la justicia social, la redistribución económica y el futuro del trabajo.

En la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), reunida en París del 9 al 24 de noviembre de 2021, en su 41ª reunión, promovió el primer marco normativo universal sobre ética de la IA – "*Recomendación Sobre la Ética de la Inteligencia Artificial",* fue adoptado por los 193 Estados miembros de la UNESCO en noviembre de 2021.

Esta recomendación aborda la ética de la IA como una reflexión normativa sistemática, basada en un marco integral, global, multicultural y evolutivo de valores, principios y acciones interdependientes, que puede guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos o desconocidos de las tecnologías de la IA en los seres humanos, las sociedades con su medio ambiente que les ofrece una base para aceptar o rechazar las tecnologías de la IA. (UNESCO, 2023)

Cuadro 1: *Recomendación Sobre la Ética de la Inteligencia Artificial*; Principios

Fuente: *Unesco*

"Los mismos derechos que tienen las personas fuera de línea deben protegerse también en línea, incluso durante todo el ciclo de vida de los sistemas de inteligencia artificial" (ONU, 2024).

INTELIGENCIA ARTIFICIAL Y LA CIBERDELINCUENCIA

La IA es vista regularmente como una tecnología de propósito general, como la electricidad, las comunicaciones o el internet; por lo que la IA tiene múltiples aplicaciones en diferentes campos, lamentablemente esta tecnología también es utilizada para el cometimiento de ciberdelitos.

En la actualidad, la inteligencia artificial (IA) está experimentando un rápido avance y la reiteración de los ataques cibernéticos continúa aumentando, por lo que es de suma importancia comprender cómo los ciberdelincuentes emplean la IA para llevar a cabo sus ataques. Se ha detectado los casos específicos relacionados con los ciberataques asociados con la Inteligencia Artificial de manera significativa, como ***malware basado en IA***, ***phishing sofisticado*** o ataques de ingeniería social mejorados por algoritmos de aprendizaje automático. (Zambrano, 2024)

De igual forma se han detectado otro tipo actividades maliciosas que implicarían la utilización de la IA para realizar ***ingeniería social***, con lo que se engaña a los usuarios para ingresar en enlaces maliciosos o compartir información confidencial. La ciberdelincuencia emplea IA para recolectar información sobre posibles víctimas, identificando perfiles específicos en redes sociales. Esto se logra mediante la correlación de imágenes y datos de los usuarios en distintas plataformas, con el objetivo de facilitar engaños más efectivos a través de la IA. (Rodríguez, s.f.)

Por ejemplo, mediante la generación de imágenes, audios o videos falsos que engañan a las personas al simular interacciones con alguien de su confianza. Existen herramientas de IA que efectúan la clonación de voz en tiempo real, con lo cual los ciberdelincuentes pueden conseguir acceso a servicios de TI o ejecutar engaños a otros individuos, con una grabación de unos pocos segundos. Aún más la ciberdelincuencia, ha llegado al punto de usar falsificaciones sofisticadas (deep fake) de

video, mediante lo cual pueden llegar a cambiar el rostro de una persona por otra, vulnerando el acceso a sistemas de tecnologías de la Información sensibles, con múltiples posibilidades de fraudes informáticos. (Rodríguez, s.f.)

Las medidas de seguridad contra la ciberdelincuencia impulsada por la inteligencia artificial requerirán esfuerzos conjuntos a nivel individual, colectivo, organizacional y social. Esto implica capacitar a las personas para reconocer nuevas amenazas y vulnerabilidades, como los *deepfakes* y los mensajes fraudulentos en redes sociales que suelen ser difíciles de detectar a simple vista. Sin embargo, con una adecuada formación y preparación, será posible identificarlos y prevenir sus efectos.

Es importante mencionar que, así como la IA, puede ser mal utilizada por la ciberdelincuencia, actualmente se cuenta con su contraparte, a través de la herramienta ***DarkGPT***, basada en inteligencia artificial y desarrollada sobre ChatGPT-4, que permite explorar la perspectiva sombría de la IA sin restricciones. Esta herramienta está diseñada específicamente para detectar e identificar datos filtrados a través de varios canales de internet, lo que permite a los expertos en ciberseguridad, investigadores y organizaciones, contar con una herramienta que posibilite la detección de violaciones de la información confidencial o activos digitales, de una persona u organización mediante la generación de alertas que serán validadas por los expertos. (Gupta, s.f.)

PANORAMA GEO CIBERDELINCUENCIAL

Enfoque Mundial

La inteligencia artificial (IA) ha revolucionado muchos aspectos de la vida cotidiana y empresarial, pero también ha sido aprovechada por ciberdelincuentes para realizar ataques más sofisticados. Un ejemplo claro es el phishing, donde se utilizan algoritmos de IA para crear correos electrónicos o sitios web falsos que imitan a la perfección entidades legítimas, aumentando la efectividad de estos ataques.

Según datos de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el phishing ha crecido un 75% en los últimos cinco años en Europa, y la inteligencia artificial ha jugado un papel importante en este incremento, ya que esta tecnología permite a los atacantes personalizar sus mensajes de phishing a través del análisis de datos personales, lo que aumenta las probabilidades de éxito (Arcos, 2024).

En el caso de España, estudios recientes indican que el 40% de las empresas han experimentado al menos un intento de ataque de phishing sofisticado en el último año. La IA facilita la personalización de estos ataques, haciendo que los correos fraudulentos sean más convincentes y difíciles de detectar (Arcos, 2024).

Un estudio reciente de la EAE Business School reveló que el 94% de los ciudadanos en España está profundamente preocupado por el impacto de la inteligencia artificial, particularmente por la creciente dificultad de diferenciar entre lo real y lo falso en internet.

Esta preocupación está justificada, debido a que las estafas online mediante la utilización de la inteligencia artificial siguen siendo el delito más prevalente en el país europeo, con un crecimiento exponencial del 509% desde 2016, en relación con datos del Sistema Estadístico de Criminalidad y Ministerio del Interior, en lo que va del 2024 (Durán, 2024).

El estudio realizado por la EAE Business School destaca que los jóvenes de entre 25 y 34 años (Millennials y Generación Z) son el grupo más afectado por las estafas en línea, sofisticadas mediante

la utilización de la inteligencia artificial, representando un 61% de los casos de fraude o intentos de fraude (Business School, 2024).

Un ejemplo reciente de un gran fraude digital involucró el uso de inteligencia artificial para manipular videos e imágenes. En este caso, se transfirieron 23 millones de euros a una empresa no identificada en Hong Kong, aparentemente bajo las órdenes del director financiero de la compañía afectada. Referenciar. (Noto, 2024)

El uso fraudulento de la IA en Australia, se ha dado en torno a la creación de noticias y vídeos deepfake, a menudo protagonizados por un famoso, para promocionar oportunidades de inversión. Según el Centro Nacional Antiestafas, estos casos costaron a los australianos más de 8 millones de dólares el 2023 (Katanich, 2024).

En Estados Unidos, el Centro de Denuncias de Delitos en Internet del FBI recibió el año pasado casi 900.000 denuncias de delitos cometidos en internet, un 22% más que el año anterior. Las pérdidas potenciales superan los 12.500 millones de dólares (Katanich, 2024).

Los daños futuros podrían ser fácilmente superiores, ya que los expertos prevén un aumento anual de 2.000 millones de dólares en fraudes de identidad mediante IA según marketwatch. (Katanich, 2024).

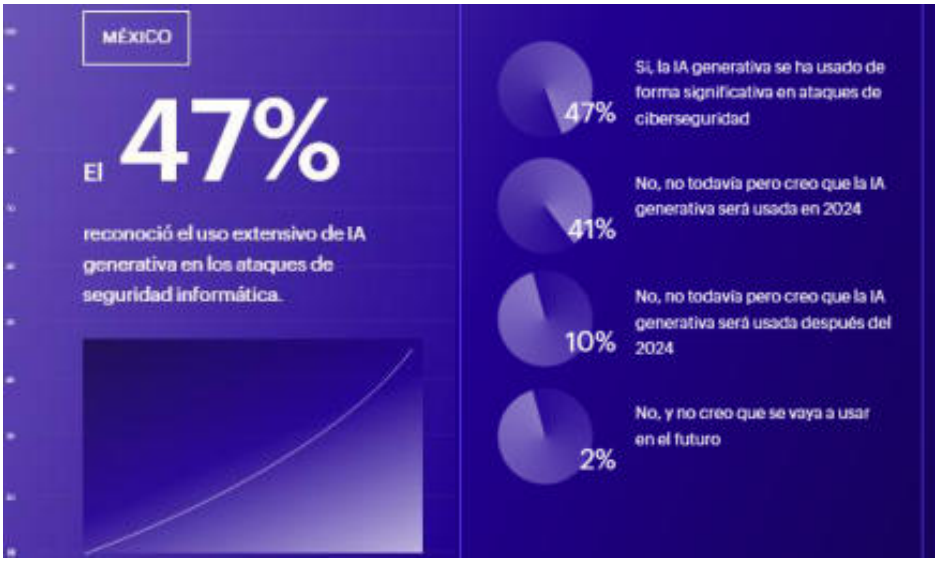
Enfoque regional: latinoamericano

Los múltiples aspectos normativos y sociales de la región, asociados con el bajo nivel de concienciación de los ciudadanos sobre los peligros que atañen a la red, establece que, *"(...) América Latina y el Caribe constituyen un destacado mercado emergente con creciente visibilidad global, pero debido al estado actual de su ciberseguridad, es una de las regiones más atacadas del mundo. La conjunción de la falta de estándares y regulaciones claras, la escasez de profesionales cualificados, la ausencia de una cultura de seguridad cibernética en los usuarios y los recursos limitados para invertir en tecnologías de seguridad convierten a la región en una zona del planeta singularmente vulnerable a las ciberamenazas.(...)*". (Arenas, 2024)

En referente al comportamiento de los ciberdelitos en Latinoamérica, su objetivo principal estaría en el sector privado desde el crecimiento del teletrabajo en 2020. En segundo lugar, se ubica el sector

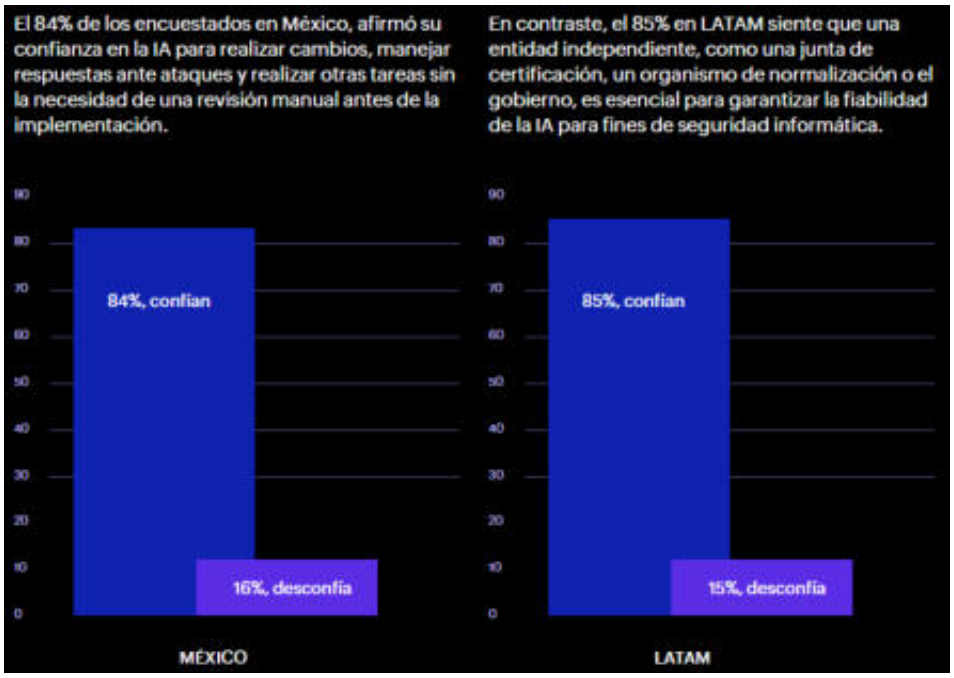
público, específicamente las entidades a cargo de la distribución de servicios y recursos nacionales, y en un margen menor las instituciones militares. (Bastutelo, s.f.)

Imagen 2: El estado de la ciberseguridad en América Latina para 2024. encuesta "Rol de la IA en la ciberseguridad"- México



Fuente: *Manage Engine*[1]

Imagen 3: El estado de la ciberseguridad en América Latina para 2024. encuesta "Rol de la IA en la ciberseguridad"- México



Fuente: *Manage Engine*

La situación de las ciberamenazas para 2024 muestra un incremento en estafas con audios y videos convincentes manipulados por inteligencia artificial. Kaspersky revela que los intentos de estafas mediante mensajes falsos aumentaron un 140% en Latinoamérica en 2024, entre julio de 2023 a julio

[1] https://www.manageengine.com/latam/encuesta/estado-de-la-ciberseguridad-2024/mexico.html

de 2024 y, en toda la región, se registraron alrededor de 397 millones de bloqueos de phishing. El estudio de los expertos de Kaspersky también destaca aspectos importantes, como el uso de audios y videos manipulados a través de Inteligencia Artificial (deepvoice y deepfake) para generar engaños convincentes, además de la utilización de direcciones de sitios web con la terminación ".ai" para embaucar a las víctimas. (Kasperky, 2024)

Enfoque local

Ecuador enfrenta una realidad digital que demanda atención ya que las amenazas cibernéticas

evolucionan con rapidez y sofisticación. Según el Reporte de la empresa Kaspersky, entre junio de 2023 y julio de 2024, se detectaron más de 1.185.000 intentos de ransomware en la región, donde Ecuador es uno de los principales objetivos junto a Brasil, México y Colombia (Kaspersky, 2024). No obstante, la identificación precisa de los delitos perpetrados con el uso de IA se ve limitada por la sofisticación de estas actividades y la necesidad de reforzar las capacidades de análisis y monitoreo de las fuerzas del orden.

En 2023, a través de medios digitales de noticias se conocieron algunos casos en donde menores de edad de distintos colegios del país usaban inteligencia artificial para realizar material de contenido sexual usando fotos de otras menores de edad, cayendo en delitos de publicación de contenido sexual infantil y de ciberacoso. Estos hechos subrayan la necesidad de fortalecer los mecanismos de prevención y respuesta ante los riesgos digitales, especialmente aquellos potenciados por IA. infoe

Frente a este panorama, Ecuador ha avanzado significativamente en el refuerzo de su capacidad de respuesta mediante la actualización de su normativa legal. De acuerdo con el Índice Global de Ciberseguridad 2024, el país ha alcanzado el nivel T2 – Avanzado, con una calificación de 17,43 sobre 20 (International Telecommunication Union (ITU), 2024). Este reconocimiento refleja un progreso tangible en marcos normativos y organizativos que buscan abordar las amenazas actuales. Asimismo, la participación activa de Ecuador en iniciativas internacionales de cooperación y desarrollo de capacidades, evidencia un compromiso por alinearse con estándares globales, fortaleciendo su infraestructura de seguridad digital, generando un entorno resiliente frente al cometimiento de delitos incluidos aquellos potenciados con IA.

CARACTERIZACIÓN DEL MAL USO DE LA IA

La IA al servicio de la delincuencia

La incorporación de la IA en actividades criminales representa un riesgo creciente y permite a las organizaciones delictivas aumentar su capacidad de adaptación y mejorar la efectividad de sus operaciones (Pascual, 2020).

La delincuencia ya no se limita a las calles; también se oculta en cualquier computadora y acecha el ciberespacio. Si internet permite a los delincuentes operar sin fronteras y acceder a un mercado de víctimas en cualquier momento y lugar, la inteligencia artificial ha amplificado esta capacidad a una escala sin precedentes.

Los grupos criminales utilizan algoritmos basados en inteligencia artificial para identificar y reclutar niños y adolescentes vulnerables en zonas desatendidas, atrayéndolos mediante redes sociales con imágenes de una vida de lujo. Además, aprovechan aplicaciones como Waze y Google Maps para optimizar rutas de tráfico ilícito de drogas, armas y personas, evitando puntos de control de seguridad.

También emplean ingeniería social automatizada para extraer datos personales de redes sociales y crear fraudes personalizados mediante técnicas de phishing, como correos electrónicos con enlaces o archivos maliciosos. A su vez, el uso de inteligencia artificial les permite perfeccionar estos ataques, haciendo que los correos electrónicos sean más realistas y convincentes (Newton, 2024).

La creación de malware también se beneficia de la inteligencia artificial, permitiendo explotar rápidamente vulnerabilidades de software de “día cero” y desarrollar ataques cibernéticos más eficaces. Paralelamente, en la deep web existen “servicios para delincuencia”, un mercado de herramientas ilícitas que permite a los ciberdelincuentes menos experimentados realizar ataques avanzados. Finalmente, los delincuentes utilizan deepfakes para crear audios y videos falsos con los

que suplantan identidades, extorsionan o incluso simulan secuestros, engañando a las familias de migrantes desaparecidos y exigiendo rescates sin necesidad de un secuestro físico (Orgaz, 2024).

Implicaciones y desafíos

Actualmente la (IA) se ha difundido notablemente en la sociedad, ya que estas tecnologías pueden ayudar en el proceso de toma de decisiones y así establecer políticas más igualitarias y eficientes que permitan mejorar los empleos, servicios de salud, calidad educativa, etc. (Pombo, 2023). No obstante, estas tecnologías conllevan implicaciones y desafíos que se detallan a continuación.

Implicaciones

La utilización de la inteligencia artificial (IA) en los mecanismos de toma de decisiones, implica riesgos potenciales, debido a las implicaciones directas o indirectas en la implementación de estas tecnologías. Lo cual genera aspectos positivos o ventajas como: *Automatización eficiente, Aumento de la precisión, Mejora de la productividad, Personalización y experiencia del cliente, Avances en la atención médica, Automatización de procesos, Potencia las tareas creativas, Reduce el error humano, Reducción del tiempo de análisis de datos, Mantenimiento predictivo, Mejora en la toma de decisiones, Control y optimización de procesos productivos y líneas de producción, Aumento de la productividad y calidad en la producción*. Así como también se pueden destacar Aspectos negativos o desventajas como: *Desplazamiento laboral*, *Sesgo y discriminación*, *Privacidad y seguridad*, *Dependencia de la IA*, *Manipulación y desinformación*, *Armas autónomas*, *Disponibilidad de datos*, *Falta de profesionales cualificados, Costo y el tiempo de implementación* (Rentería R. , 2023).

Desafíos

La (IA) se ha convertido en una herramienta fundamental en el desarrollo de las actividades cotidianas de las entidades públicas o privadas, transformando la forma de operación, toma de decisiones y la forma en la que se relacionan con usuarios o clientes. No obstante, a medida que la IA sigue evolucionando, surgen desafíos que deben abordarse para aprovechar al máximo su potencial. La IA presenta múltiples desafíos, que deben ser tomados muy en cuenta y tratados con la criticidad que corresponde, entre los que se destacan: la *Arquitectura de información, la Implementación, la Ética y responsabilidad, la Interoperabilidad de sistemas, la Ciberseguridad, la Escasez de talento en IA., la Regulación y cumplimiento, Aceptación y Adopción Cultural* (Rentería R. , 2023)

Imagen 4: *Desafíos de la inteligencia artificial*

Fuente: (Kaira., 2023).

La (IA) brinda grandes oportunidades a las organizaciones, al igual que presenta grandes desafíos que deben ser examinados minuciosamente. La solución de los desafíos presentados requerirá de acciones multidisciplinarias de áreas especializadas en tecnología, ética, regulación y cultura organizacional. Una opción que permita superar los desafíos que conlleva el uso de la Inteligencia Artificial es la iniciativa ***fAIr LAC+ (IA justa y responsable),*** "*que es una alianza entre los sectores público y privado, la sociedad civil y la academia, para incidir tanto en la política pública como en el ecosistema emprendedor en la promoción del* ***uso responsable y ético de la IA".*** (FAIRLAC, s.f.). Cuenta con 5 instrumentos del tipo abierto y disponibles para los líderes de los proyectos que emplean IA y el personal a cargo del desarrollo de la solución (equipo técnico), que deseen cumplir con principios éticos y disminución de riesgos. Estos instrumentos son: *Autoevaluación ética para sistemas desarrollados, Autoevaluación para el ecosistema emprendedor, Manual para quien esté dirigiendo desde una entidad pública, un proyecto que use sistemas de soporte de decisión, Manual para el equipo técnico, Guía de auditoría algorítmica*. (FAIRLAC, s.f.)

Conductas delictivas

La inteligencia artificial (IA) ha transformado diversos ámbitos, incluyendo la comisión de conductas delictivas. Su capacidad para aprender y tomar decisiones autónomas ha facilitado la ejecución de delitos cometidos a través del uso de las tecnologías de la Información y Comunicación. Las conductas delictivas constituyen el núcleo del derecho penal, al representar aquellas acciones u omisiones realizadas por el sujeto activo (titular de la conducta típica, antijurídica y culpable que constituye el núcleo de la infracción penal.) que vulneran bienes jurídicos protegidos por la ley. Estas

conductas son tipificadas en los ordenamientos jurídicos para delimitar las acciones que serán sancionadas penalmente, bajo los principios de legalidad, culpabilidad y proporcionalidad.

Una conducta delictiva es la acción u omisión típica antijurídica y culpable que atenta contra bienes jurídicos relevantes para la sociedad, como la vida, la integridad física, la propiedad o el orden público. Para que una conducta sea considerada delictiva, debe reunir los siguientes elementos:

- **Típica**: Debe estar descrita en la ley penal (principio de legalidad).
- **Antijurídica**: Contraria al ordenamiento jurídico.
- **Culpable**: Debe ser imputable al autor, con dolo o culpa.

Es así, que se debe considerar que las conductas delictivas se las puede clasificar en función de su forma de ejecución, elementos subjetivos, forma de comisión y resultado:

a) Por la forma de ejecución

- Acción: Cuando el delito se comete mediante un comportamiento positivo, es decir, realizando un acto prohibido por la ley. Ejemplo: un homicidio.
- Omisión: Cuando el delito se comete al no realizar una conducta exigida por la ley, habiendo un deber jurídico de actuar. Ejemplo: un médico que, estando de turno, se niega a atender a un paciente en estado de emergencia, resultando en su fallecimiento.

b) Por el elemento subjetivo

- Dolosas: La conducta se realiza con intención de infringir la ley, es decir, con conocimiento y voluntad. Ejemplo: el robo.
- Culposas: La conducta es producto de imprudencia, negligencia o impericia, sin intención de causar el daño. Ejemplo: un accidente de tránsito con resultado de muerte.
- Preterintencionales: Se excede el resultado querido inicialmente. Ejemplo: una agresión que, sin intención, causa la muerte de la víctima.

c) Por la forma de comisión

- Simples: Una sola acción configura el delito. Ejemplo: hurto.
- Complejos: Requieren varias acciones para su consumación. Ejemplo: el secuestro.

d) Por el resultado

- De resultado: Exige un cambio en el mundo exterior para consumarse, como los delitos contra la vida.
- De mera actividad: Basta con la acción para que se configuren, sin importar el resultado. Ejemplo: portación ilegal de armas

Una vez que se ha contemplado la clasificación de la “Conducta Delictiva”, es necesario abordar el tema de “Autoría”, partiendo de la siguiente premisa “no toda persona que intervenga en la

comisión de un ciberdelito será su autor". Ello es así porque el Código Orgánico Integral Penal diferencia en sus artículos 42 y 43, Autores (modalidades) y Cómplices.

> ***Art. 42.- Autores**. - Responderán como autoras las personas que incurran en alguna de las siguientes modalidades:*
> ***1. Autoría directa:***
> *a) Quienes cometan la infracción de una manera directa e inmediata.*
> *b) Quienes no impidan o procuren impedir que se evite su ejecución teniendo el deber jurídico de hacerlo.*
> ***2. Autoría mediata:***
> *a) Quienes instiguen o aconsejen a otra persona para que cometa una infracción, cuando se demuestre que tal acción ha determinado su comisión.*
> *b) Quienes ordenen la comisión de la infracción valiéndose de otra u otras personas, imputables o no, mediante precio, dádiva, promesa, ofrecimiento, orden o cualquier otro medio fraudulento, directo o indirecto.*
> *c) Quienes, por violencia física, abuso de autoridad, amenaza u otro medio coercitivo, obliguen a un tercero a cometer la infracción, aunque no pueda calificarse como irresistible la fuerza empleada con dicho fin.*
> *d) Quienes ejerzan un poder de mando en la organización delictiva.*
> ***3. Coautoría:** Quienes coadyuven a la ejecución, de un modo principal, practicando deliberada e intencionalmente algún acto sin el cual no habría podido perpetrarse la infracción.*
>
> ***Art. 43.- Cómplices. -** Responderán como cómplices las personas que, en forma dolosa, faciliten o cooperen con actos secundarios, anteriores o simultáneos a la ejecución de una infracción penal, de tal forma que aun sin esos actos, la infracción se habría cometido. No cabe complicidad en las infracciones culposas.*
> *Si de las circunstancias de la infracción resulta que la persona acusada de complicidad, coopera en un acto menos grave que el cometido por la autora o el autor, la pena se aplicará solamente en razón del acto que pretendió ejecutar.*
> *El cómplice será sancionado con una pena equivalente de un tercio a la mitad de aquella prevista para la o el autor.*

El **artículo 42 del Código Orgánico Integral Penal** clasifica los tipos de autoría en la comisión de infracciones penales, distinguiendo entre **autoría directa, mediata y coautoría**. Esta clasificación tiene como objetivo precisar la participación de los sujetos en la ejecución de un delito, estableciendo diferentes grados de responsabilidad.

1. **Autoría Directa**

   a) Ejecución directa e inmediata: Esta modalidad abarca a quienes materializan el hecho típico, es decir, ejecutan directamente el comportamiento que configura el delito. Por ejemplo, una persona que dispara un arma para causar una lesión cumple con esta modalidad.

   b) Omisión con deber jurídico: Involucra a quienes, teniendo la obligación jurídica de impedir el delito (por su cargo o relación), no lo hacen. Por ejemplo, un guardia de seguridad que deliberadamente no actúa para evitar un robo.

La autoría directa presupone una vinculación inmediata con el acto, ya sea por acción u omisión. En el caso de la omisión, la doctrina penal exige que el sujeto tenga un deber específico y legalmente establecido de actuar.

2. Autoría mediata

a) Instigación: Se refiere a quien persuade o convence a otra persona para cometer un delito, siempre que se demuestre que su influencia fue determinante. Por ejemplo, incitar a alguien a realizar un hurto.

b) Comisión indirecta mediante terceros: Este caso contempla a quien utiliza a otras personas (imputables o no) para cometer el delito, valiéndose de medios como pagos, promesas, amenazas o engaños. Un ejemplo es un líder criminal que organiza un asalto utilizando subordinados.

c) Violencia o coacción: Quienes obligan a terceros a actuar delictivamente mediante violencia, abuso de autoridad o amenazas, incluso si esta fuerza no es irresistible, son responsables como autores mediatos.

d) Poder de mando: Aquellas personas que, dentro de una estructura delictiva, tienen capacidad de ordenar y controlar la comisión de delitos.

La autoría mediata se centra en el control indirecto del acto delictivo, ya sea a través de la manipulación psicológica, la coerción o el uso de una estructura jerárquica para ejecutar actos ilícitos.

3. Coautoría

La coautoría implica una colaboración activa y esencial en la ejecución del delito, realizando actos fundamentales que, sin ellos, la infracción no se habría llevado a cabo. Un ejemplo es cuando dos personas participan activamente en un robo, una vigilando y la otra ejecutando el hurto.

En la coautoría, la responsabilidad recae sobre aquellos que contribuyen significativamente a la materialización del hecho delictivo, compartiendo tanto la decisión como la ejecución.

El artículo 43 del Código Orgánico Integral Penal regula la figura del cómplice, estableciendo los parámetros de responsabilidad penal para quienes, sin ser autores, participan en la comisión de un delito facilitando su ejecución de manera secundaria.

1. Concepto de complicidad

La complicidad se define como la participación accesoria en la comisión de un delito. Los cómplices no ejecutan directamente el delito (como los autores), pero su cooperación dolosa contribuye a que este se materialice. La cooperación puede ser:

Anterior: Actos realizados antes de la ejecución, como proporcionar armas o información.

Simultánea: Actos realizados en el momento de la ejecución, como vigilar para que el autor no sea descubierto.

Desde la perspectiva de la teoría del delito, los cómplices no tienen el "dominio del hecho" (característica de los autores), pero su colaboración tiene relevancia penal porque incrementa las posibilidades de éxito del acto delictivo.

2. Elementos de la complicidad

Acto doloso: La complicidad requiere intención (dolo) en la cooperación, es decir, el cómplice debe conocer y querer participar en el delito, aun de manera accesoria.

Carácter secundario de la cooperación: El acto del cómplice no es indispensable para la comisión del delito, ya que este se habría ejecutado igualmente. Por ejemplo, un conductor que transporta al autor después de un robo no es indispensable para el acto mismo.

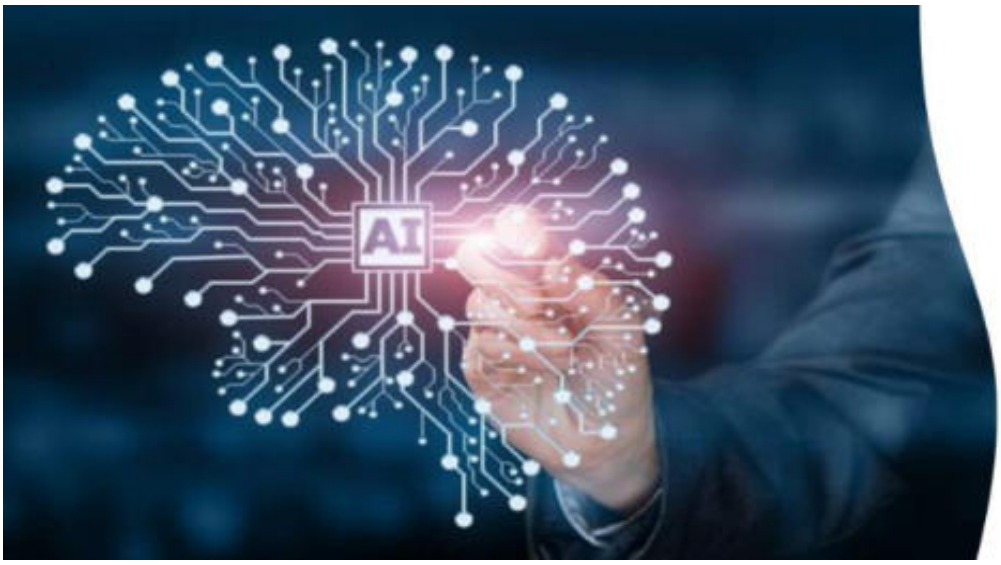
3. Principio de proporcionalidad

El artículo aclara que, si el cómplice coopera en un acto menos grave que el cometido por el autor, será sancionado únicamente por la gravedad de su contribución. Por ejemplo: Si el cómplice coopera para un robo simple, pero el autor comete un robo agravado, el cómplice será sancionado solo por el robo simple.

La figura del cómplice está arraigada en la teoría general del delito y la clasificación de partícipes:

- **Dominio del hecho**: Según Roxin y la teoría del dominio del hecho, el autor tiene control sobre la ejecución del delito, mientras que el cómplice carece de ese control.
- **Dolo y accesoriedad:** La complicidad depende de un acto principal, y su sanción es accesoria porque el acto del cómplice no configura un delito independiente

La teoría sostiene que es autor del delito quien tiene el dominio o control sobre su realización, es decir, quien decide y ejecuta el acto principal de manera directa o indirecta. A diferencia de un partícipe (como un cómplice), el autor es quien posee el control del hecho, ya sea porque lo realiza personalmente o porque tiene capacidad para determinar cómo, cuándo y por quién se ejecutará.



Prevención

La creciente amenaza de la ciberdelincuencia potenciada por la IA requiere una evolución en los métodos de seguridad digital, que involucra a las instituciones públicas y privadas, así como también a los ciudadanos, en la creación de un entorno digital seguro. En diciembre de 2024, la Organización International de Policía Criminal - INTERPOL presentó una campaña de concientización para prevenir delitos que se han vuelto más sofisticados y automatizados con el uso de la IA, como ataques de phishing personalizados y ransomware avanzado (INTERPOL, 2024).

Cada actor, desde su ámbito de acción, debe orientar sus esfuerzos hacia objetivos que converjan en el fortalecimiento de la seguridad digital. Las instituciones públicas tienen el papel de articular normativas y promover su implementación y cumplimiento efectivos, mientras que el sector privado complementa estos esfuerzos mediante la actualización de sistemas, la adopción de tecnologías y prácticas seguras que refuercen tanto sus operaciones como la confianza de los ciudadanos. Entre estos esfuerzos, destaca la necesidad de proteger a niñas, niños y adolescentes, quienes son especialmente vulnerables en el entorno digital. La protección frente al riesgo de ser víctimas de abuso sexual infantil, requiere un enfoque basado en la comunicación, colaboración y supervisión de los padres o tutores, junto con el compromiso de las fuerzas del orden para prevenir estos delitos, así como identificar y sancionar a los responsables.

La colaboración y el aprendizaje son fundamentales para enfrentar los desafíos de la ciberdelincuencia. Como se menciona en el Microsoft Digital Defense Report 2024, el intercambio de conocimientos entre los actores relevantes, fortalecen la comprensión sobre la seguridad digital y aumentan la resiliencia de las organizaciones frente a las amenazas (Burt, 2024).

ESTADÍSTICAS DE DELITOS COMETIDOS CON EL USO DE LAS TICs

Cifras de detenidos

A continuación, se presentan las cifras relacionadas con los delitos cometidos con el uso de las TICs, cuyas fuentes son la Fiscalía General del Estado, la Unidad Nacional de Ciberdelitos de la Policía Nacional y el Consejo de la Judicatura.

Estadísticas de los detenidos y aprendidos por delitos cometidos con el uso de las TICs en Ecuador

Actualmente no se contemplan estadísticas exclusivamente referentes a delitos cometidos a través del uso de las tecnologías digitales, pero podemos destacar el número de detenciones por ciberdelitos y delitos cometidos con el uso de las TICs, proporcionados por la Policía Nacional.

A continuación, se presenta un cuadro de progresión de detenidos por delitos cometidos a través del uso de las tecnologías digitales desde el 2020 hasta abril de 2024

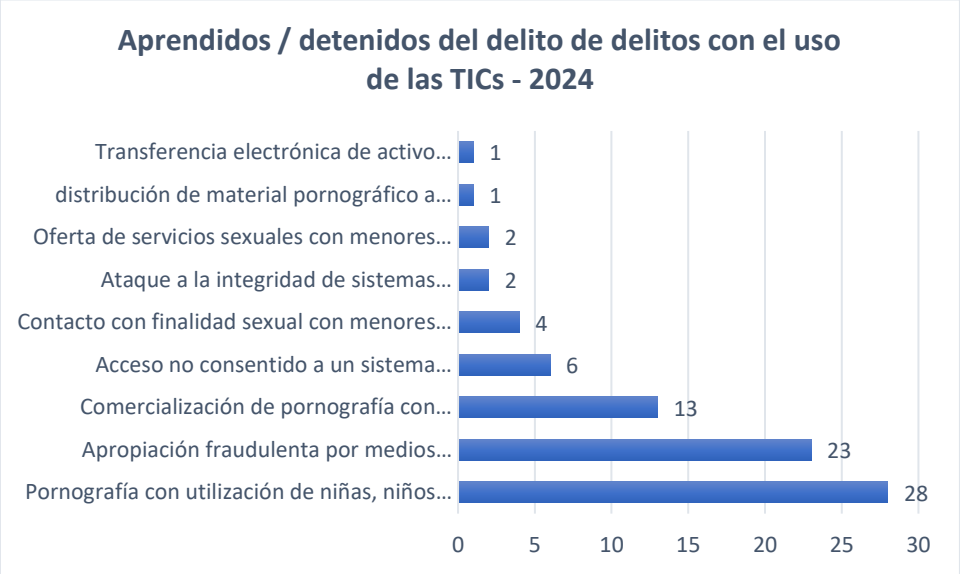
__Tabla 1:__ Detenidos por delitos con el uso de las TICs

Aprendidos / detenidos del delito de delitos con el uso de las TICs	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	Total
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	0	0	0	2	2	0	0	0	2	0	1	**7**
Apropiación fraudulenta por medios electrónicos	1	1	5	2	1	1	1	4	2	5	1	**24**
Ataque a la integridad de sistemas informáticos	0	0	1	0	0	0	1	0	0	0	0	**2**
Comercialización de pornografía con utilización de niñas, niños o adolescentes	1	0	1	1	3	4	1	1	0	1	0	**13**

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1	1	0	1	0	0	0	0	1	0	0	**4**
Distribución de material pornográfico a niñas, niños y dolescentesadolescentes	0	0	0	0	0	1	0	0	0	0	0	**1**
Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	0	1	0	0	0	0	1	0	0	0	0	**2**
Pornografía con utilización de niñas, niños o adolescentes	1	3	2	5	0	6	3	0	5	3	0	**28**
Transferencia electrónica de activo patrimonial	0	0	1	0	0	0	0	0	0	0	0	**1**
Total	**4**	**6**	**10**	**11**	**6**	**12**	**7**	**5**	**10**	**9**	**2**	**82**

Fuente: *C4i2- Policía Nacional*

Gráfico 1: *Detenidos/ aprendidos por delitos con el uso de las TICs*



Fuente: *C4i2- Policía Nacional*

Estadísticas de los ciberdelitos cometidos en Ecuador

Fiscalía General del Estado

Una vez que se ha realizado un análisis a los datos estadísticos de las noticias del delito (NND) proporcionados por Dirección de Estadísticas y Sistemas de la Información de la Fiscalía General del Estado relacionado a los Delitos con el uso de las TICs, comprendido en el periodo desde el año 2020 hasta octubre del 2024 se tiene el siguiente resultado:

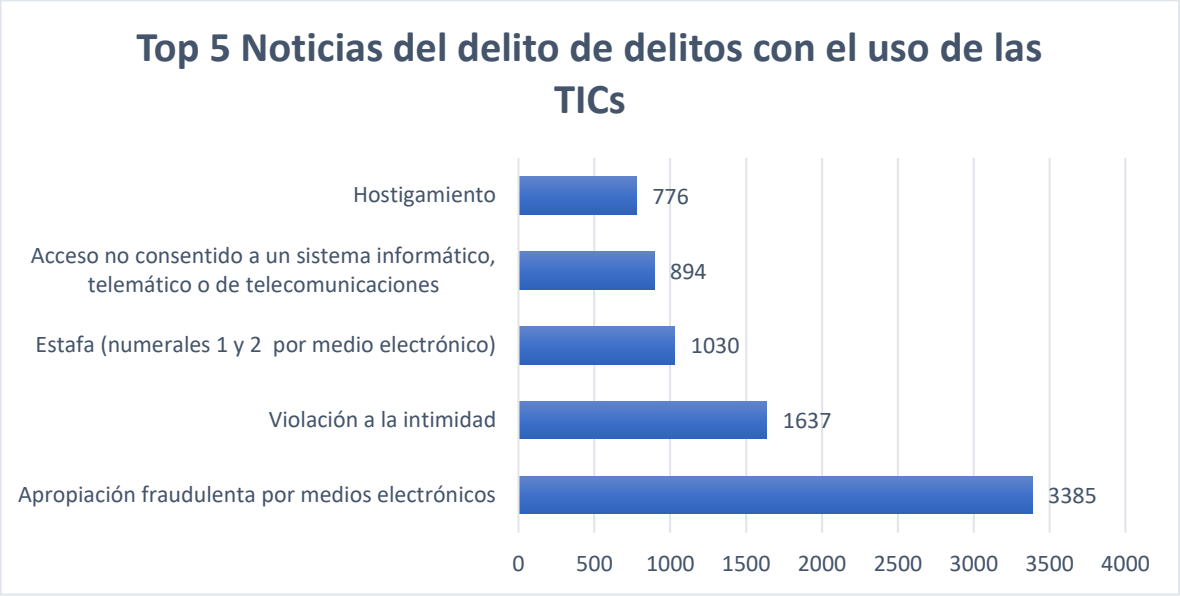
Tabla 2: Denuncias de Delitos con el uso de las TICs durante el año 2024.

Noticias del delito de delitos con el uso de las TICs	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	Nov	Total
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	62	63	65	67	110	75	73	81	119	99	80	**894**
Acoso sexual (inciso 2 - Ciberacoso sexual)	10	5	5	6	8	12	9	6	8	12	5	**86**
Actos lesivos a los derechos de autor	0	0	0	0	1	1	0	0	0	0	0	**2**
Apropiación fraudulenta por medios electrónicos	277	286	312	359	326	332	312	305	326	280	270	**3385**
Ataque a la integridad de sistemas informáticos	16	21	18	27	30	26	14	21	36	23	12	**244**
Comercialización de pornografía con utilización de niñas, niños o adolescentes	1	4	3	1	2	3	2	2	3	2	2	**25**
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	8	16	18	12	18	9	10	7	5	5	8	**116**
Delitos contra la información pública reservada legalmente	0	0	0	0	0	1	0	1	3	0	0	**5**
Distribución de material pornográfico a niñas, niños y adolescentes	0	2	3	4	1	0	1	0	0	2	0	**13**
Estafa (numerales 1 y 2 por medio electrónico)	90	103	102	82	94	81	98	127	77	92	84	**1030**
Falsificación Informática	6	13	16	8	9	6	12	11	7	11	6	**105**
Hostigamiento	60	92	74	70	65	61	95	59	66	62	72	**776**
Interceptación ilegal de datos	8	3	10	7	12	6	5	6	5	3	2	**67**
Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.	1	1	0	3	0	1	1	2	0	0	0	**9**
Pornografía con utilización de niñas, niños o adolescentes	6	12	13	10	17	14	7	13	16	4	6	**118**
Reprogramación o modificación de información de equipos terminales móviles	0	0	0	2	0	0	0	2	0	0	0	**4**
Revelación ilegal de base de datos	5	3	3	5	4	4	6	4	1	3	5	**43**
Terrorismo (numeral 1)	11	0	2	0	0	1	0	0	0	0	0	**14**
Transferencia electrónica de activo patrimonial	11	18	23	9	21	13	13	10	10	16	7	**151**

Violación a la intimidad	138	179	131	153	167	152	170	145	145	138	119	**1637**
Total	**710**	**821**	**798**	**825**	**885**	**798**	**828**	**802**	**827**	**752**	**678**	**8724**

Fuente: *Fiscalía General del Estado.*

Gráfico 2: *Top de delitos con el uso de las TICs 2024*



Fuente: *Fiscalía General del Estado.*

Policía Nacional

Las estadísticas remitidas por la Unidad Nacional de Ciberdelito de la Policía Nacional, corresponden a las delegaciones remitidas por la autoridad competente.

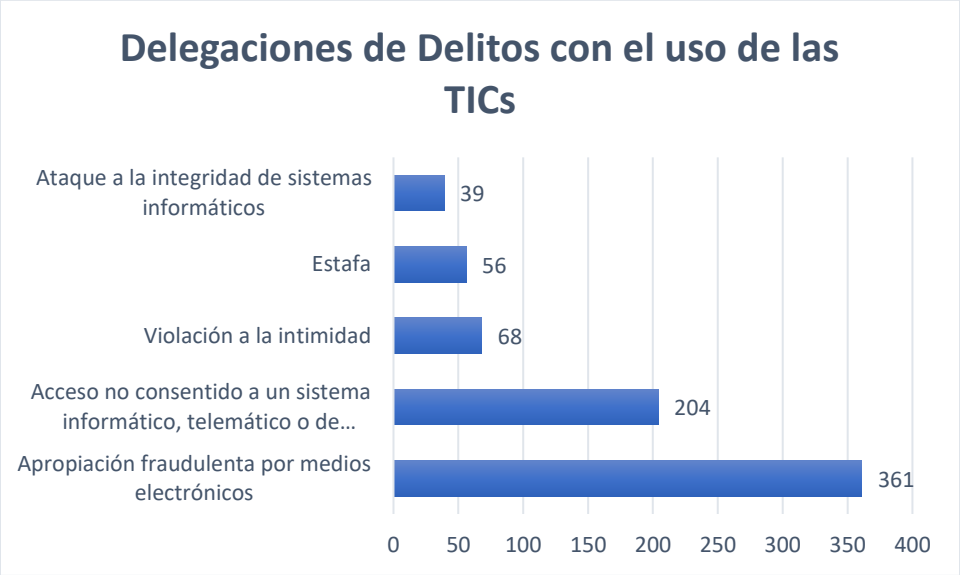
Tabla 3: Delegaciones de Delitos con el uso de las TICs durante el año 2024

Delegaciones de Delitos con el uso de las TICs	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	Nov	Total
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	11	19	16	17	15	19	22	13	11	39	22	**204**
Acoso sexual	2	3	2	0	1	0	2	0	0	3	0	**13**
Apropiación fraudulenta por medios electrónicos	31	23	28	39	39	26	41	41	25	48	20	**361**
Ataque a la integridad de sistemas informáticos	5	2	4	2	3	3	7	1	2	7	3	**39**
Comercialización de pornografía con utilización de niñas, niños o adolescentes	4	1	2	1	0	0	1	0	0	0	0	**9**
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	2	0	2	1	0	1	0	0	0	0	0	**6**
Distribución de material pornográfico a niñas, niños y adolescentes	1	0	0	0	0	0	0	0	0	0	0	**1**
Estafa	6	7	6	9	11	4	5	3	0	5	0	**56**

Hostigamiento	0	0	0	0	0	0	0	0	0	1	1	**2**
Interceptación ilegal de datos	0	0	0	1	1	0	0	3	1	1	0	**7**
Pornografía con utilización de niñas, niños o adolescentes	4	3	5	4	1	4	3	3	3	1	2	**33**
Revelación ilegal de base de datos	0	0	0	1	3	0	1	1	0	0	0	**6**
Terrorismo	4	1	1	1	1	0	0	1	0	0	0	**9**
Transferencia electrónica de activo patrimonial	2	1	2	0	1	6	3	0	3	1	1	**20**
Violación a la intimidad	4	8	10	5	11	6	5	3	3	7	6	**68**
Total	**76**	**68**	**78**	**81**	**87**	**69**	**90**	**69**	**48**	**113**	**55**	**834**

Fuente: *Unidad Nacional de Ciberdelito de la Policía Nacional.*

Gráfico 3*: Top 5 de delegaciones de delitos con el uso de las TICs*



Fuente: *Unidad Nacional de Ciberdelito de la Policía Nacional*

Consejo de la judicatura

La información estadística proporcionados por el consejo de la judicatura reflejan las causas ingresadas y resueltas que se presentan ante el sistema judicial del país, ya sea por delitos remitidos por la Fiscalía o por contravenciones tramitadas directamente en las Unidades Judiciales.

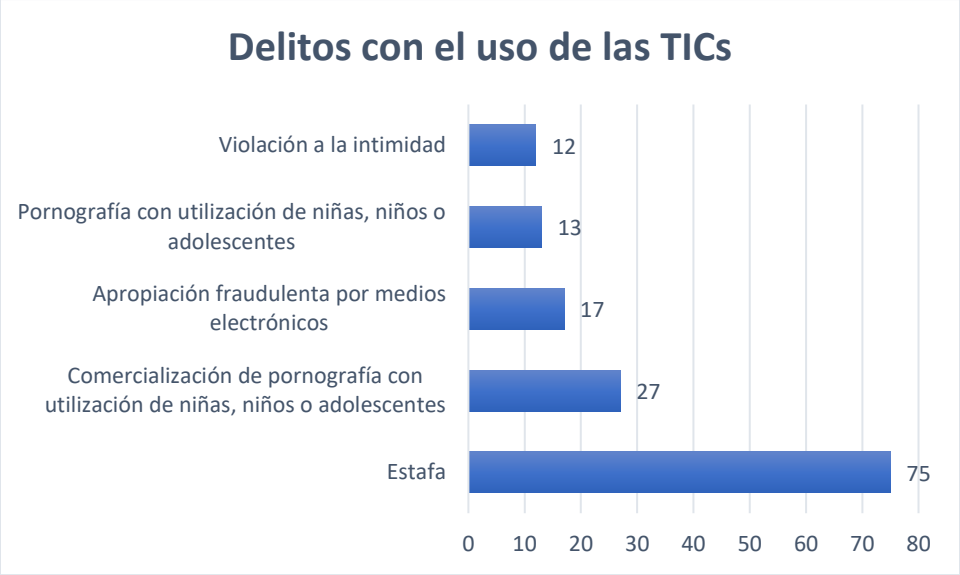
Tabla 4: *Causas ingresadas y resueltas de la función judicial con el uso de las TICs*

Delitos con el uso de las TICs	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	Total
Pornografía con utilización de niñas, niños o adolescentes	0	2	4	2	2	0	2	1	0	0	0	**13**
Comercialización de pornografía con utilización de niñas, niños o adolescentes	4	1	0	6	2	5	6	2	1	0	0	**27**
Acoso sexual	2	1	0	0	3	1	0	0	0	0	1	**8**

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1	3	1	0	1	1	1	1	1	0	0	**10**
Violación a la intimidad	1	3	2	0	0	0	2	2	2	0	0	**12**
Estafa	12	16	6	11	4	8	4	4	6	2	2	**75**
Apropiación fraudulenta por medios electrónicos	1	5	2	3	1	1	0	2	2	0	0	**17**
Transferencia electrónica de activo patrimonial	0	1	0	0	0	0	0	0	0	0	0	**1**
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	1	0	0	0	1	0	0	0	0	0	0	**2**
Terrorismo	1	0	0	0	3	0	0	0	0	0	0	**4**
Total	**23**	**32**	**15**	**22**	**17**	**16**	**15**	**12**	**12**	**2**	**3**	**169**

Fuente: *Consejo de la Judicatura*

Gráfico 4*: causas ingresadas y resueltas del Consejo de la Judicatura de delitos con el uso de las TICs*



Fuente: *Consejo de la Judicatura*

CONCLUSIONES Y PROYECCIONES

Conclusiones

- Crecimiento de la Ciberdelincuencia: La integración de la inteligencia artificial en el ámbito delictivo ha llevado a un aumento significativo en la sofisticación y efectividad de los ciberataques. Delincuentes utilizan herramientas de IA para personalizar y optimizar sus ataques, lo que dificulta su detección y prevención.

- Desafíos Éticos y Legales: La rápida evolución de la IA plantea serios desafíos éticos y legales. Es fundamental establecer un marco que regule el uso de estas tecnologías para evitar su explotación en actividades delictivas.
- Impacto Social: Los ciberdelitos no solo afectan a las instituciones financieras, sino que también tienen un impacto negativo en la confianza pública y en la seguridad de los ciudadanos. Las estafas en línea han crecido, afectando especialmente a grupos vulnerables como los jóvenes.
- Necesidad de Concienciación: Existe una falta de conocimiento general sobre los riesgos asociados con la IA y la ciberdelincuencia. La educación y la concienciación son esenciales para empoderar a los usuarios y protegerlos de posibles fraudes.Proyecciones
- Se prevé un crecimiento sostenido en el uso de inteligencia artificial por parte de ciberdelincuentes para automatizar ataques, como phishing personalizado y malware autónomo, lo que aumentará la cantidad y efectividad de los incidentes.
- Tecnologías como los deepfakes y la clonación de voz evolucionarán, permitiendo nuevas formas de extorsión, fraudes y manipulación de sistemas de verificación biométrica.
- Los ataques dirigidos a infraestructuras esenciales, como redes eléctricas, sistemas de transporte y hospitales, serán más comunes debido a la capacidad de la IA para identificar y explotar vulnerabilidades.

Proyecciones

- Aumento de la Sophisticación de los Ataques: Se espera que los ciberdelincuentes continúen perfeccionando sus técnicas, utilizando IA para desarrollar ataques más personalizados y difíciles de detectar. Esto incluye el uso de algoritmos avanzados para crear correos electrónicos y sitios web fraudulentos que imiten a entidades legítimas, lo que incrementará el riesgo de fraudes en línea.
- Incremento en la Frecuencia de Ciberdelitos: Las estadísticas indican un crecimiento exponencial en los delitos cibernéticos. Por ejemplo, el phishing ha aumentado un 75% en Europa en los últimos cinco años, y se prevé que esta tendencia continúe a medida que los delincuentes adopten nuevas tecnologías y técnicas basadas en IA.
- Desarrollo de Herramientas de IA para Ciberdelincuentes: La creación de herramientas como DarkGPT muestra cómo la IA puede ser utilizada tanto para fines maliciosos como para mejorar las capacidades defensivas. Se anticipa que los delincuentes desarrollen más software basado en IA que les permita llevar a cabo ataques con mayor eficacia.
- Impacto Social y Económico: A medida que las estafas online se vuelven más comunes, especialmente entre los jóvenes, se proyecta un aumento en la preocupación pública sobre la

seguridad digital. Esto podría llevar a un mayor escrutinio regulatorio y a la implementación de medidas más estrictas para proteger a los consumidores.

- Evolución de las Estrategias de Seguridad: Las autoridades y organizaciones deberán adaptarse continuamente a las nuevas amenazas cibernéticas. Se prevé que se desarrollen nuevas estrategias y tecnologías para combatir el uso indebido de la IA en delitos cibernéticos, incluyendo la capacitación continua para reconocer y responder a estos ataques.
- Regulación y Ética: A medida que la tecnología avanza, también lo hará la necesidad de establecer marcos regulatorios claros para el uso ético de la IA. Esto incluirá debates sobre responsabilidad, transparencia y protección de datos personales, lo cual será crucial para mitigar los riesgos asociados con su uso indebido.

BIBLIOGRAFÍA

Arcos, D. (septiembre de 2024). *Inteligencia artificial y delitos informáticos: ¿Cómo afecta el cibercrimen?* Obtenido de https://tecfuturo.es/inteligencia-artificial-y-delitos-informaticos/

Arenas, J. (12 de Junio de 2024). Obtenido de https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/panoramica-de-la-ciberseguridad-en-latinoamerica-una-coyuntura-singular_2

Bastutelo, G. (s.f.). *CiberLatam*. Obtenido de https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/panoramica-de-la-ciberseguridad-en-latinoamerica-una-coyuntura-singular_20240612.html

Burt, H.-B. &. (2024). *Microsoft Digital Defense Report 2024.* Obtenido de https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Business School, E. (diciembre de 2024). *Los Millennials y la Generación Z son quienes sufren más estafas en la red*. Obtenido de https://www.eae.es/actualidad/noticias/los-millennials-y-la-generacion-z-son-quienes-sufren-mas-estafas-en-la-red

Churchill, L. R. (1999). Are We Professionals? A Critical Look at the Social Role of Bioethicists. *Daedalus*, 253-274.

Durán, I. (octubre de 2024). *Crisis con la IA en España, el 94 % de la población está preocupada y confunde lo real de lo falso.* Obtenido de https://www.infobae.com/tecno/2024/10/17/crisis-con-la-ia-en-espana-el-94-de-la-poblacion-esta-preocupada-y-confunde-lo-real-de-lo-falso/

(2024).*Evolución de la IA.* Ministerio del Interior.

FAIRLAC, H. |. (s.f.). *FAIRLAC. (n.d.-b)*. Obtenido de https://fairlac.iadb.org/

Gupta, V. (s.f.). *DarkGPT — AI OSINT tool powered by ChatGPT-4 to detect leaked databases. Medium*. Obtenido de https://bevijaygupta.medium.com/darkgpt-ai-osint-tool-powered-by-chatgpt-4-to-detect-leaked-databases-be0b7d53f200

IBM. (s.f.). *¿Qué es el ransomware como servicio (RaaS)?* Obtenido de https://www.ibm.com/es-es/topics/ransomware-as-a-service

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024 (5th Edition)*. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

INTERPOL. (Diciembre de 2024). *La campaña Think Twice invita a pensárselo dos veces para no dejarse engañar por las estafas en línea*. Obtenido de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Una-campana-de-INTERPOL-alerta-sobre-la-ciberdelincuencia-y-otros-delitos-financieros

Jara, L. M. (s.f.). *Inteligencia artificial y derecho. Un abordaje preliminar.* Obtenido de https://repositorio.unlz.edu.ar/handle/123456789/500

Kaira. (19 de Octubre de 2023). *8 retos que enfrentará tu empresa para implementar IA y cómo resolverlos. Canvia.* . Obtenido de https://canvia.com/retos-inteligencia-artificial/

Kasperky. (2024). *las estafas mediante mensajes falsos en América Latina, revela Kaspersky*. Obtenido de https://latam.kaspersky.com/about/press-releases/aumentan-en-140-las-estafas-mediante-mensajes-falsos-en-america-latina-revela-kaspersky

Kaspersky. (Octubre de 2024). *América Latina registra un aumento del 2.8% en los intentos de ataque de ransomware*. Obtenido de https://latam.kaspersky.com/about/press-releases/america-latina-registra-un-aumento-del-28-en-los-intentos-de-ataque-de-ransomware

Katanich, D. (abril de 2024). *Así actúan los estafadores para robar dinero mediante la Inteligencia Artificial*. Obtenido de https://es.euronews.com/business/2024/04/16/asi-actuan-los-estafadores-para-robar-dinero-mediante-la-inteligencia-artificial

Mendoza, F., Uribe, A., Moncada, O., Morales, D., & Mantilla, L. (s.f.). *Implementacion de las GPUs para un futuro inteligente.* Obtenido de http://wiki.sc3.uis.edu.co/images/8/8c/Siete.pdf

Newton, C. (26 de agosto de 2024). *Cuatro formas en que la IA está influyendo en el crimen organizado en América Latina*. Obtenido de https://insightcrime.org/news/four-ways-ai-is-shaping-organized-crime-in-latin-america/

Noam, S. (2020). *GLU Variants Improve Transformer.* Obtenido de https://arxiv.org/pdf/1706.03762v7

Noto, G. (mayo de 2024). *Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'*. Obtenido de https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/

ONU, N. (21 de marzo de 2024). *La Asamblea General adopta una resolución histórica sobre la IA*. Obtenido de https://news.un.org/es/story/2024/03/1528511

Orgaz, C. (4 de octubre de 2024). *6 maneras en que grupos criminales de América Latina usan la inteligencia artificial para delinquir*. Obtenido de https://www.bbc.com/mundo/articles/crej5gwllvlo#:~:text=Los%20delincuentes%20tambi%C3%A9n%20est%C3%A1n%20utilizando,y%20se%20acaba%20de%20publicar.

Pascual, D. S.-R. (2020). ¿INTELIGENCIA ARTIFICIAL AL SERVICIO DE LA CRIMINALIDAD ORGANIZADA ¿MITO O REALIDAD?

Pombo, C. (22 de Noviembre de 2023). *Los riesgos de la inteligencia artificial y algunas soluciones. Abierto Al Público.* Obtenido de https://blogs.iadb.org/conocimiento-abierto/es/riesgos-inteligencia-artificial/

Rentería, R. (junio de 2023). *El impacto de la inteligencia artificial: ¿revolución o riesgo? Gaceta UDG.* Obtenido de https://www.gaceta.udg.mx/el-impacto-de-la-inteligencia-artificial-revolucion-o-riesgo/

Rentería, R. H. (junio de 2023). *El impacto de la inteligencia artificial: ¿revolución o riesgo? Gaceta UDG.* Obtenido de https://www.gaceta.udg.mx/el-impacto-de-la-inteligencia-artificial-revolucion-o-riesgo/

Rodríguez, I. (s.f.). *auditool.org*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/la-inteligencia-artificial-y-el-cibercrimen

Sum and Substance Ltd. (2024). *Identity Fraud Report 2024*. Obtenido de https://sumsub.com/files/sumsub_identity_fraud_report_2024.pdf

Turing, A. (Octubre de 1950). *Computing machinery and intelligence.* Obtenido de https://doi.org/10.1093/mind/LIX.236.433

UNESCO. (30 de agosto de 2023). *Recomendación sobre la ética de la inteligencia artificial*. Obtenido de https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

Verdugo, S., & Ochoa, A. (2022). *Acciones para combatir el impacto del crimen en el ciberespacio*. Obtenido de https://www.ceeol.com/search/article-detail?id=1079009

Zambrano, A. (2024). *Impacto de la inteligencia artificial en los ciberataques.* Obtenido de https://revistas.itsup.edu.ec/index.php/sinapsis/article/view/895/2080