TRABAJO FIN DE GRADO – GRADO EN CRIMINOLOGÍA

El papel de la Inteligencia Artificial en la prevención y lucha contra los ciberdelitos

Autor del TFG:

Valery Masi Legidos

Tutor del TFG:

Dr. Julián Pinazo Dallenbach

UNIVERSIDAD EUROPEA DE VALENCIA

2023/2024

Valery Masi Legidos

El papel de la Inteligencia Artificial en la prevención y lucha contra los ciberdelitos

UNIVERSIDAD EUROPEA

Facultad de Ciencias Sociales

Grado en Criminología

Tutor: Dr. Julián Pinazo Dallenbach

Valencia, a 22 de mayo de 2024

DEDICATORIA

A mamá y papá, por sus sacrificios para siempre darnos lo mejor.

A la yaya, por el apoyo constante durante todo este proceso.

A los pininos, por los consejos y los debates.

Este trabajo final está dedicado con mucho amor a ustedes, por estar a mi lado (incluso en la distancia), brindándome todo su apoyo y cariño en cada paso. Sin ustedes esto no hubiera sido posible.

AGRADECIMIENTOS

Gracias a Alex y Max, por ser siempre mi soporte.

A Maricel, por sus consejos.

Y un agradecimiento especial a todos aquellos que han mostrado interés y han colaborado en mi proyecto.

Resumen

El avance del mundo digital supone un beneficio para la sociedad, sin embargo este avance ha causado que los delitos cibernéticos creen una amenaza cada vez mayor para los usuarios de este mundo. Por esta razón los profesionales de la ciberseguridad han de implementar medidas eficaces para proteger la seguridad de los ciudadanos. La Inteligencia Artificial es una herramienta con gran potencial para reforzar estas medidas, siendo capaz de detectar amenazas. El presente trabajo investiga cómo es utilizada la Inteligencia Artificial para prevenir y luchar contra los ciberdelitos, mediante el estudio de la bibliografía, en particular artículos científicos, libros, artículos de prensa y reportes anuales, al igual que un análisis de las regulaciones que distintos países la han dado a esta herramienta. Por último se realizó un análisis cualitativo, por medio de entrevistas, a profesionales de la materia quienes han proporcionado una visión concreta y profunda sobre las medidas utilizadas con la ayuda de la Inteligencia Artificial para prevenir y mitigar los daños causados por los ataques cibernéticos. Este trabajo analiza el papel crucial de la Inteligencia Artificial en la prevención y lucha contra ciberdelitos, demostrando su eficacia en la automatización de procesos y la detección temprana de amenazas.

Palabras clave: Inteligencia Artificial, ciberseguridad, prevención, lucha, criminología.

Abstract

The advancement of the digital world has brought many benefits to our society; however, these progress has caused cybercrime to create an ever-increasing threat to its users. For this reason, cybersecurity professionals have to implement effective measures to protect the security of citizens. Artificial Intelligence is a tool with great potential to reinforce these measures, being able to detect threats. This paper investigates how Artificial Intelligence is used to prevent and fight against cybercrime, through the study of the literature, in particular scientific articles, books, press articles and annual reports, as well as an analysis of the regulations that different countries have given to this tool. Finally, a qualitative analysis was carried out by means of interviews with professionals in the field who have provided a concrete and in-depth vision of the measures used with the help of Artificial Intelligence to prevent and mitigate the damage caused by cyber-attacks. This work analyzes the crucial role of Artificial Intelligence in the prevention and fight against cybercrime, demonstrating its effectiveness in the automation of processes and the early detection of threats.

Keywords: Artificial Intelligence, cybersecurity, prevention, combating, criminology.

ÍNDICE GENERAL

CONTENIDOS PÁGINA

ÍNDICE DE FIGURAS

CONTENIDOS PÁGINA

ÍNDICE DE TABLAS

CONTENIDOS PÁGINA

ÍNDICE DE SIGLAS Y ABREVIATURAS

Sigla	Inglés	Español
O.D.S	Sustainable Development Goals.	Objetivos de Desarrollo Sostenible.
CP	Penal Code.	Código Penal.
INCIBE	National Institute of Cybersecurity.	Instituto Nacional de Ciberseguridad.
EEUU	United States of America.	Estados Unidos de América.

1 INTRODUCCIÓN

1.1. Problema de Investigación

El informe de Riesgos Globales de 2023 del Foro Económico Mundial sostiene que los ciberataques se encuentran entre las primeras cinco probabilidades de riesgo grave a nivel global (World Economic Forum, 2023). En otro informe realizado por la compañía IBM (2023), se resalta que el coste de la filtración de datos alcanzó un máximo nivel durante el 2023, registrando un total de 4.45 millones de dólares, siendo un aumento de 2.3% sobre el año anterior.

Sin embargo, se demostró que aquellas compañías que utilizaban procesos de seguridad automatizados por Inteligencia Artificial reportaron una pérdida de 1.76 millones menos que aquellas que no utilizaban estos sistemas (IBM Security, 2023a). Los sistemas de Inteligencia Artificial fueron desarrollados para simular y crear estructuras que fueran capaces de funcionar sin la necesidad de ayuda humana.

Actualmente, con el crecimiento de la tecnología, la Inteligencia Artificial ha sido capaz de crecer y evolucionar para poder ser utilizada en el ámbito de la seguridad. Los ataques a compañías han demostrado ser cada vez más peligrosos, ya que los agresores han encontrado nuevas maneras de aumentar su conocimiento y habilidad en las tecnologías. El uso de algoritmos y de máquinas basadas en el aprendizaje, como la Inteligencia Artificial, provocan una dificultad en los agresores, ya que estos impiden que se utilice el mismo método repetidas veces (Ansari et al., 2022).

El presente trabajo busca investigar los diferentes usos que la Inteligencia Artificial propone para la prevención y detección de los delitos cibernéticos. Es de relevante importancia una investigación en esta área, ya que cada día, la tecnología se vuelve parte de la vida de los seres humanos en mayor escala, por lo tanto, la necesidad de utilizar sus herramientas para el beneficio y seguridad de la sociedad se vuelve fundamental en el ámbito criminológico.

1.2. Pregunta de Investigación

Una vez determinado el problema de investigación, se plantea la siguiente pregunta como base de investigación. ¿Cómo puede ser utilizada la Inteligencia Artificial para prevenir y luchar de los

ciberdelitos? Además, se plantea entender cuál será el efecto del uso de esta herramienta en la profesión de la criminología, evaluando los factores positivos y negativos que posee.

1.3. Objetivos

1.3.1. Objetivo General

El objetivo general del presente Trabajo de Fin de Grado es investigar y analizar las distintas funciones que la Inteligencia Artificial podrá tener en la prevención de los ciberdelitos, al igual que sus funciones con relación a la lucha de estos.

1.3.2. Objetivos Específicos

Como objetivos específicos se proponen:

- Estudiar las competencias con las que la Inteligencia Artificial permite ser utilizada en la actualidad.
- Analizar los distintos problemas que puede conllevar la mala utilización de la Inteligencia Artificial.
- Explorar el futuro de la profesión de Criminología con la llegada de la Inteligencia Artificial, específicamente el papel de esta profesión en la prevención y lucha contra los ciberdelitos.
- Entender cómo la llegada de las nuevas tecnologías ha afectado la evolución de los ciberdelitos.

1.4. Justificación: relevancia y contribución científica al conocimiento académico

El mundo digital ha sufrido una evolución significativa en los últimos años, específicamente con la llegada de la Inteligencia Artificial. Una herramienta tecnológica que ha revolucionado el funcionamiento ya conocido de la tecnología es un mecanismo que busca crear máquinas artificialmente cognitivas que se desenvuelvan de manera inteligente, al igual que, estas tengan la capacidad de adaptarse y prevenir nuevas situaciones (Broadhurst et al., 2019).

El crecimiento de la tecnología y de la Inteligencia Artificial ha sido beneficioso en múltiples áreas y aspectos, sin embargo, esta evolución tecnológica, ha generado una nueva ola de delitos, conocidos como *ciberdelitos*. Los delitos en línea o ciberdelitos son aquellos que se producen en

el ámbito digital, donde el autor utiliza sus conocimientos sobre el ciberespacio para realizarlos (Bossler & Berenblum, 2019).

Estos delitos han mostrado ser una amenaza cada vez mayor para la sociedad, los ciberdelincuentes aprovechan, cada vez más, las oportunidades que el crecimiento de la tecnología les proporciona, beneficiándose de las vulnerabilidades que la sociedad presenta frente a esta evolución (Monteith et al., 2021).

La Inteligencia Artificial ha aportado grandes beneficios a la sociedad en la última década, y, se predice que cada día irá teniendo más repercusión, tanto positiva como negativa en nuestras vidas. Desde el punto de vista criminológico, permitirá ser utilizado para estrategias de reconocimiento facial, uso de drones de vigilancia, crear mapas geográficos de delitos, etc. De la misma manera, un uso no adecuado de esta tecnología podría llegar a limitar los derechos y libertades de los seres humanos (Velasco, 2022).

El presente trabajo busca identificar y analizar el uso de la Inteligencia Artificial en el ámbito de los ciberdelitos, identificando su uso para la prevención e investigación de estos. Entender estos factores es de relevante importancia ya que permitirá que los profesionales de la criminología conozcan las ventajas y desventajas de las herramientas, llegando a utilizarlas para poder prevenir y conocer el delito de mejor manera.

1.5. Plan de Investigación

Para la realización de este trabajo de fin de grado será necesario realizar un plan de investigación. En este se tratarán todos los puntos a mencionar a lo largo del estudio, en primer lugar, se realizará un marco teórico donde se tratarán los fundamentos teóricos y jurídicos. Una vez se tenga un conocimiento de estos fundamentos, se procederá al proceso de investigación, en el cual se realizarán una serie de entrevistas a profesionales en materia de ciberseguridad, para obtener su perspectiva sobre esa temática.

Posteriormente se realizará un análisis de los resultados en base al fundamento teórico ya mencionado, para poder llegar a una conclusión sobre el rol de la Inteligencia Artificial en la prevención y lucha contra los ciberdelitos.

2 FUNDAMENTACIÓN TEÓRICA

2.1. Marco Teórico

Para el buen desarrollo y entendimiento del presente Trabajo de Fin de Grado, resulta necesario conocer la fundamentación teórica respecto al tema, ya que investigaciones previas sobre esta temática aportan una contextualización importante a esta investigación. De la misma manera, se realizará un breve análisis del marco jurídico actual sobre la regulación de la Inteligencia Artificial.

2.1.1. Definiciones

El siguiente apartado proporciona las definiciones claves que el lector ha de conocer para comprender de manera adecuada los objetivos que el trabajo busca alcanzar.

2.1.1.1. Tecnología

Se considera que la tecnología es una herramienta aplicable que permite a los humanos realizar procedimientos de manera más eficaz, tanto en tiempo, como en velocidad (Volti, 2017). Sin embargo, este término carece de una definición exacta por ser un término muy amplio. Por un lado, la Real Academia Española, define la tecnología como el "conjunto de teorías y técnicas que permiten el aprovechamiento práctico del conocimiento científico" (RAE, 2020). Esta definición proporciona un punto de partida clave para el entendimiento amplio de la tecnología.

Aunque, por otro lado, distintos autores han resaltado la dificultad de determinar un concepto único para este término. El autor Rudi Volti (2017), en su publicación *Society and Technology*, proporciona una serie de características a considerar, a la hora de delimitar este concepto. Se expone las características de la tecnología y cómo esta requiere una red compleja de material, herramientas, agentes y consumidores, ya que sin esta red, la tecnología no se podría desarrollar y utilizar.

De la misma manera, se requieren múltiples agentes con habilidades determinadas que puedan ser utilizadas en conjunto para crear una estructura organizada. Siendo así la tecnología el resultado de una combinación de dispositivos, habilidades y estructuras que se presentan como un sistema. Resultando, su concepto, como "un sistema creado por humanos que utiliza el

conocimiento y organización que produce objetos y técnicas con el fin de obtener resultados específicos" (Volti, 2017, p 19).

Dentro de este sistema tan amplio, se encuentran distintos subtipos de la tecnología, entre estos, es importante resaltar la *tecnología de la información.* Un término que ha recibido múltiples definiciones a lo largo de su evolución. En 1995 se definió este término como un conjunto de soluciones de software y hardware que crean y permiten un soporte en la gestión, operaciones y estrategias de las organizaciones (Thong & Yap, 1995, como es citado en Onn & Sorooshian, 2013).

Sin embargo, de manera más reciente, se define este término como el conjunto de hardware, software y redes que permiten la conexión con el internet (Sin Tan et al., 2009). Se considera que este tipo de tecnología ha sido una de las herramientas más eficientes utilizadas a nivel organizacional, ya que abarca una gama amplia de medios y dispositivos que permiten la vinculación de los sistemas información con las personas (Dewett & Jones, 2001). Dentro de este subtipo, se encuentran áreas específicas que se mencionan más adelante como la seguridad de sistemas o ciberseguridad y la Inteligencia Artificial.

2.1.1.2. Ciberespacio

El espacio digital o el *ciberespacio*, es un ambiente complejo, y es el resultado de la interacción que tienen los seres humanos con los servicios de internet y softwares creados, utilizados por medio de la tecnología informática (ISO/IEC 27002, 2005). El Instituto Nacional de Estándar y Tecnología define el ciberespacio como el dominio global dentro del entorno de la información, está conformado por una red independiente de infraestructuras de sistemas de información (National Institute of Standar and Technology, 2024).

Para entender el término ciberespacio de mejor manera, es importante resaltar que el término *ciber* proviene del concepto de *cibernética*, que fue definido por primera vez en 1948 por el autor Norbert Wiener, quien lo clasificó como el estudio del control y la comunicación del animal y la máquina (Marinescu, 2017). Esta definición explica la idea de cómo los humanos pueden interactuar con las máquinas para proporcionar un entorno alternativo, brindando así la base del concepto del ciberespacio.

Entendiendo este concepto, el ciberespacio es el conjunto de dispositivos tecnológicos conectados por una red electrónica que permite que la información se transmita y se utilice (Clark, 2010). El ciberespacio será una red que permite el tráfico de la información, y se caracteriza por distintos grados de accesos, navegación y actividad. Uno de los grados o puntos de acceso para el ciberespacio es el Internet, el cual consiste en conexiones físicas entre computadores alrededor del mundo utilizando protocolos que permiten que estén conectadas entre sí (Folsom, 2007).

2.1.1.3. Seguridad y ciberseguridad

A lo largo de este Trabajo de Fin de Grado, se buscará estudiar cómo los ciberdelitos pueden ser prevenidos y detectados por la Inteligencia Artificial. Cuando se habla de ciberdelitos y su prevención y detección, se hace referencia al ámbito de la seguridad de sistemas o ciberseguridad, ya que este término abarca la seguridad que ocurre dentro del ciberespacio.

La seguridad implica una estabilidad que sea predecible para los individuos, para así, poder perseguir los objetivos sin ningún daño o temor. De manera más tradicional, el diccionario Oxford, define el término seguridad como el "estado libre de peligro o amenaza" (Oxford Dictionary, 2022). Al relacionar la seguridad con el mundo cibernético, se puede entender esta como aquella tecnología de seguridad que es aplicada para la protección de bienes que se encuentren en el ciberespacio (Brooks, 2009).

La ciberseguridad se entiende como el conjunto de herramientas, políticas de la seguridad que se enfocan en la gestión de riesgos y mejores prácticas tecnológicas para proteger el entorno cibernético, al igual que a las organizaciones y los usuarios activos de este entorno (von Solms & van Niekerk, 2013). La ciberseguridad es mayormente utilizada en organizaciones con el objetivo de garantizar una continuidad y minimizar los daños cuando se encuentre con un impacto de incidentes de seguridad. Esto se debe a que se esfuerza en garantizar el mantenimiento de las propiedades de seguridad para la organización y los usuarios (von Solms & van Niekerk, 2013).

Resulta importante también, el concepto que propone la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, en su estándar ISO/IEC 27002; en el cual explica la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27002, 2005).

La ciberseguridad, por su amplio campo de aplicación, se divide en dos componentes esenciales: defensivo y ofensivo. El uso del componente o práctica, dependerá de múltiples factores como el entorno y sistema operativo utilizado (Schatz et al., 2017). La seguridad ofensiva u *Offsec* hace referencia a las estrategias proactivas que se utilizan en el ámbito de seguridad, normalmente por actores maliciosos, sin embargo, en este caso, serán utilizados por los agentes de seguridad para fortalecer la seguridad del sistema. Este tipo de práctica incluye los conocidos *equipos rojos*, que realizan pruebas de penetración para evaluar las vulnerabilidades de sistemas (IBM Security, 2024d).

Por otro lado, la seguridad defensiva es la práctica de estrategias contrarias. Son estrategias reactivas centradas en la prevención y detección de ataques malignos, serán una respuesta a estos. Es la práctica más tradicional para proteger las redes y requiere un gran conocimiento del sistema a proteger (Aiyanyo et al., 2020).

2.1.1.4. Inteligencia Artificial

Al igual que los términos que se han estudiado anteriormente, no existe una definición estándar del concepto de Inteligencia Artificial. Sin embargo, por el gran interés académico que ha recibido en los últimos años, múltiples autores han intentado proporcionar una definición que se adapte a este. La Inteligencia Artificial ha sido descrita mediante el enfoque otorgado al concepto de inteligencia humana, de la misma manera, se hace referencia a cómo las máquinas se comportan como humanos y son capaces de realizar acciones que requieren inteligencia (European Commission. Joint Research Centre, 2020).

Un reporte realizado por la Comisión Europea introduce la Inteligencia Artificial como un término genérico que hace referencia a las máquinas y algoritmos capaces de observar el ambiente y aprender de estos en base a la experiencia ganada anteriormente, tomando así las decisiones adecuadas (European Commission. Joint Research Centre, 2018).

Otra definición, más completa, explica cómo la Inteligencia Artificial se refiere a sistemas diseñados por humanos utilizado para alcanzar ciertos objetivos complejos. Actuando en el mundo físico y digital, el sistema observa el entorno e interpreta los datos de forma estructurada, para así decidir cuál es la mejor acción a tomar para lograr el objetivo. Estos sistemas también se pueden

diseñar para poder aprender la adaptación del comportamiento analizando cómo el entorno se ha visto afectado en acciones anteriores (European Commission, 2018).

Para que los sistemas sean capaces de aprender a adaptarse a los entornos deben estar compuestos por un sistema de *Machine Learning* o *aprendizaje automático*, el cual representa un cambio dentro de la tecnología informática. Machine Learning es una rama de las ciencias de computación que busca permitir a las computadoras aprender sin ser programadas directamente, las computadoras aprenden tras mejorar su actuación por medio de la experiencia (Bi et al., 2019).

Tradicionalmente, un programador escribía un código para reflejar las reglas necesarias para procesar los datos de entradas, para así, obtener una respuesta de salida. Con el uso del aprendizaje automático, la computadora recibe los datos de entrada, al igual que antiguas respuestas de salida, para así crear reglas que pueden ser aplicadas a los datos nuevos, creando respuestas originales nuevas, siendo así un sistema basado en el entrenamiento, comparado a un sistema programado (European Commission. Joint Research Centre, 2018).

El uso del aprendizaje automático se ha convertido en un método ideal dentro de la Inteligencia Artificial para poder desarrollar softwares que permiten la práctica de reconocimiento de voz, procesamiento de lenguaje, control de robots, entre otros (Jordan & Mitchell, 2015). Este aprendizaje está asociado con la inteligencia humana, ya que tiene la capacidad de aprender y mejorar sus análisis por el uso de algoritmos computacionales, los cuales utilizan conjuntos de entrada y salida para reconocer los patrones y aprender de estos de manera efectiva (Helm et al., 2020). Al igual que la inteligencia humana, una vez se den repeticiones suficientes, la máquina será capaz de predecir la salida.

2.1.1.5. Cibercrimen

En la actualidad, el mundo digital está fuertemente conectado con las vidas de los seres humanos. Esto ha causado que los agentes criminales aprovechen esta conexión para atacar las debilidades de los sistemas, redes e infraestructuras digitales (Interpol, 2024). La globalización digital ha causado que los ciberdelitos traspasen fronteras, lo que dificulta la investigación y persecución de dichos delitos, ya que la víctima y el agresor se pueden encontrar en distintos lugares.

Los ciberdelitos, son todo tipo de delitos que ocurren por medio del Internet y las tecnologías de la información. En estos, dispositivos como las computadoras, tablets, dispositivos móviles, son utilizados para la comisión del delito (Brown et al., 2017). La Comisión Europea, define este tipo de delitos como aquellos actos criminales que se comenten en línea por medio de las redes de comunicación digital y los sistemas de información (Comisión Europea, 2023).

Al ser un fenómeno tan amplio, existen distintas clasificaciones. Por un lado, autores como Brown et al. (2017), los clasifican en dos categorías principales:

- En primer lugar, los delitos tradicionales que se cometen con la ayuda de una computadora. En estos, la tecnología es el principal instrumento utilizado para la comisión del delito. En estas categorías se encuentran delitos como el fraude, robo de identidad, distribución de pornografía de menores, actividades de organizaciones criminales, entre otras.
- En segundo lugar, los autores resaltan los delitos avanzados tecnológicamente, en los cuales se explotan las vulnerabilidades dentro del mundo digital. Estos delitos, utilizan la tecnología como objetivo al cual atacar. Son delitos que se realizan desde una computadora para atacar o vulnerar otra computadora o sistemas. Dentro de esta categoría se encuentran actividades como el hacking y el esparcimiento de virus informáticos (Brown et al., 2017). Es importante mencionar que el término *hacking* hace referencia al uso ilícito de técnicas para ganar acceso a sistemas o redes digitales (IBM Security, 2024b).

Sin embargo, la Comisión Europea (2023) clasifica estos delitos en tres categorías principales. En primer lugar, se encuentran los *delitos específicos del Internet*, siendo estos ataques contras los sistemas de información, como es el caso del phishing, por ejemplo, los agresores crean sitios bancarios falsos, en donde se le pide a las víctimas proporcionar sus datos bancarios, y así poder acceder a las cuentas bancarias de las víctimas.

Otra categoría proporcionada, es el *fraude y falsificación en línea*, los cuales se pueden realizar a mayor escala por la gran conexión que la tecnología otorga. Por último, se encuentra el *contenido ilegal en línea*, en el cual se incluye el material de abuso sexual infantil, actos terroristas, incitación al odio racial y glorificación de la violencia (Comisión Europea, 2023). A diferencia de

lo propuesto por los autores, la Comisión Europea no hace referencia a los delitos nativos tecnológicos como el *hacking*, sino, se centra mayormente en aquellos delitos tradicionales cometidos con la ayuda de la tecnología.

2.1.1.6. Big Data

Otro concepto importante de conocer es el de *Big Data*, Pese a que se considera un concepto abstracto, este hace referencia a las cantidades masivas de datos que se encuentran presentes en el ciberespacio. *Big Data* se entiende como el conjunto de datos que no pueden ser administrados y procesados por computadoras con alcance aceptable. El volumen de datos es uno de los factores principales de *Big Data*, ya que con el tiempo y los avances tecnológicos, el flujo de datos en el ciberespacio es mayor (Chen et al., 2014).

Sin embargo, el volumen no es el único criterio que conforma el concepto de *Big Data*. Por esta razón, se proporciona el *Modelo 3V*, el cual se caracteriza por tres componentes: volumen, velocidad y variedad.

- En primer lugar, el volumen hace referencia a la escala y el aumento de los datos que superan las medidas de almacenamiento tradicionales (Chen et al., 2014; Sagiroglu & Sinanc, 2013).

- En segundo lugar, la velocidad es necesaria para el flujo de datos y permitir que estos sean procesados; también, hace referencia al tiempo necesario para que se coleccionen los datos y se analicen (Chen et al., 2014; Sagiroglu & Sinanc, 2013).

- Por último, la variedad hace referencia a los distintos tipos de datos, que pueden clasificarse en: estructurados, semi estructurados y no estructurados. Los datos estructurados, son los que se clasifican y se etiquetan fácilmente; los semi estructurados, no se ajustan a clasificaciones fijas, pero utilizan etiquetas para poder separar los elementos. Los datos no estructurados, serán, por ende, aquellos que se clasifican de manera aleatoria y presentan dificultades a la hora de ser analizados (Chen et al., 2014; Sagiroglu & Sinanc, 2013).

El concepto de *Big Data* está altamente relacionado con el de Inteligencia Artificial, ya que ambos son considerados y entendidos como conceptos socio técnicos. Ambos utilizan procesos de estadística operacional para generar beneficios para aquellos que los utilicen (Elish & Boyd, 2018). El uso de datos es uno de los pilares fundamentales del funcionamiento de la Inteligencia Artificial. Por esta razón, el uso de Big Data resulta de gran importancia para poder así procesar grandes cantidades de datos. Big Data también permitirá realizar procedimientos de Machine Learning de manera automática (Elish & Boyd, 2018).

2.1.2. Inteligencia Artificial

Una vez ya entendido el concepto básico de la Inteligencia Artificial, resulta importante realizar una descripción más profunda sobre dicha herramienta. La Inteligencia Artificial se basa en el entrenamiento de grandes conjuntos de datos que permite realizar un juicio de valor proporcional a los datos sobre los cuales ha sido entrenado (Broadhurst et al., 2019).

Existen distintos tipos de Inteligencia Artificial dependiendo del enfoque que se le dé a la hora de su desarrollo. Sin embargo, existen dos enfoques principales que categorizan los distintos tipos.

- El primero hace referencia a los sistemas de conocimiento artesanal, siendo este el enfoque más antiguo, este sistema se basa en softwares desarrollados en base a la cooperación entre los programadores y sujetos expertos en aquella materia a cubrir (Allen, 2020).

- El segundo enfoque, por el contrario hace referencia al aprendizaje automático o *Machine Learning*, en este caso, como se ha mencionado en su definición, el conocimiento no es proporcionado por reglas programadas manualmente, sino que se generan reglas propias en base a los datos que se han evaluado. Este enfoque se basa en ejecutar algoritmos generados por humanos junto a los datos por los cuales la Inteligencia Artificial se entrena, generando así las reglas (Allen, 2020).

Los datos son la unidad básica de la Inteligencia Artificial, y estos afectan en la medida en que esta aprende. Por esto la calidad de los datos es de suma importancia, ya que así se evita la contaminación de la calidad de respuesta. Aplicando clasificadores, se podrá comprender las reglas

que forman las decisiones básicas de la programación, haciendo así que estos no se contaminen con tanta facilidad. (Broadhurst et al., 2019).

Los clasificadores de datos pueden ser asignados por individuos especialistas en la materia o por la misma Inteligencia Artificial, realizado por el aprendizaje automático. Estos clasificadores pueden ser realizados de manera aleatoria o por un análisis basado en la estadística de datos determinados para buscar el efecto de la causalidad. La calidad de los clasificadores dependerá de la calidad de los datos. (Broadhurst et al., 2019).

2.1.2.1. Tipos de Inteligencia Artificial

Al ser una herramienta tan compleja, existen distintos tipos de Inteligencia Artificial que se adaptan a las necesidades requeridas por el implementador. Cabe mencionar cuatro de estos tipos. En primer lugar se encuentra el aprendizaje supervisado, siendo este el tipo de aprendizaje automático en el cual los procesos y los algoritmos son supervisados por profesionales para poder etiquetar los datos entrados de manera correcta para que los datos de salida sean calificados adecuadamente en las categorías (Allen, 2020).

Los sistemas de aprendizaje supervisado pueden llegar a alcanzar un alto rendimiento, sin embargo, para esto, requieren conjuntos de datos etiquetados en gran cantidad para ello (Allen, 2020). Para poder alcanzar su rendimiento, utilizan funciones que siguen mapas de datos de entrada para así crear los datos de salida. De esta manera, el algoritmo aprende de los patrones ya creados y clasificados, siendo capaz de predecir las siguientes clasificaciones (Mahesh, 2019).

El segundo tipo a mencionar es el aprendizaje no supervisado. Estos son aquellos algoritmos que extraen las características de los datos sin necesidad de una supervisión profesional. Este tipo de Inteligencia Artificial se encarga de clasificar el conjunto de datos introducidos en sus categorías por la similitud de estos. Siendo útil cuando se busca explorar un conjunto específico de datos y poder desarrollar de manera automática las políticas operativas (Allen, 2020).

El aprendizaje no supervisado no posee respuesta correctas o incorrectas, los algoritmos son independientes en la búsqueda y presentación de datos estructurados, cuando se introduce información nueva, este utiliza las características aprendizajes para clasificarla de manera adecuada (Mahesh, 2019).

Esta tipología suele ser utilizada en casos de detección de fraude, ya que permite identificar aquellos patrones que no han sido clasificados, sin embargo, utilizado con el aprendizaje supervisado, permite identificar qué tipo de fraude específicamente es. En contraste con el grupo supervisado de aprendizaje, este se encargará de agrupar los datos en base a las similitudes, mientras el supervisado los clasificará (Allen, 2020).

En tercer lugar, el aprendizaje semi-supervisado, este como su nombre lo indica, utiliza técnicas de los dos tipos ya mencionados anteriormente, utilizando pequeñas cantidades de datos etiquetados como en el aprendizaje supervisado, para así, clasificar grandes cantidades de datas sin etiquetar (Allen, 2020). Este tipo de Inteligencia Artificial es útil, en aquellos casos en donde ya existen datos sin clasificar para poder etiquetarlos de manera más fácil. En estos casos se entrena la Inteligencia Artificial a etiquetar los datos en sus categorías (Mahesh, 2019).

Por último, se encuentra el aprendizaje en refuerzo, siendo este el más complejo de los mencionados, ya que en este, los datos que se utilizan para poder realizar el entrenamiento de la Inteligencia Artificial son recolectados de manera autónoma por la misma Inteligencia por el entendimiento del ambiente y las acciones que realiza dirigidas a las metas establecidas (Allen, 2020).

Existen cuatro aspectos claves del aprendizaje en refuerzo que hacen que este difiera del aprendizaje supervisado y no supervisado: (1) Los datos son generados y recopilados por el mismo agente de Inteligencia Artificial mientras interactúa con el entorno y recibe los cambios de este. (2) Las recompensas que requiere el aprendizaje en refuerzo serán los datos de entrada que recibe la Inteligencia Artificial cuando alcanza ciertos criterios. (3) Las recompensas solo tienen información parcial. Y, por último (4) el sistema aprende un sistema de acción que le permite tomar medidas que maximizan la recepción de recompensas (Allen, 2020).

Este tipo de Inteligencia Artificial ha demostrado un alto rendimiento en el desarrollo de sistemas en donde no existen etiquetas para los datos salientes (Allen, 2020). El aprendizaje en refuerzo es un área que permite tomar acciones en relación al ambiente para así maximizar las respuestas acumulativas (Mahesh, 2019).

2.1.2.2. Antecedentes

Aunque en la actualidad se considere que la Inteligencia Artificial es un fenómeno novedoso, la realidad es que esta herramienta ha estado en desarrollo desde la década de los 40. En esta década, se realizaron múltiples estudios y modelos que trataban la Inteligencia Artificial, principalmente el modelo realizado por Alan Turing el cual proporciona una visión abstracta descriptiva de las funciones cerebrales. Sin embargo, no fue hasta años más tarde que autores como John von Neumann y Norbert Wiener aplicaron su modelo, nombrando así a Turing como el padre de la Inteligencia Artificial (Toosi et al., 2021).

El modelo de Turing demostró que las computadoras podrían ser programadas para funcionar como una red simulando neuronas. Al igual, que demostró que su modelo sería capaz de resolver cualquier cálculo matemático, siempre y cuando este se presenta como un algoritmo. En 1956, en inicio de la Inteligencia Artificial comenzó a florecer, siendo acuñado y definido el término por primera vez (Toosi et al., 2021).

Durante esta temporada del nacimiento de la Inteligencia Artificial, se utilizó el aprendizaje en refuerzo, ya que este permite a la Inteligencia Artificial aprender de la interacción que posee con su entorno, para así, poder alcanzar las metas en base al refuerzo dado. Sin embargo, en 1957, ocurrió un cambio en la perspectiva de la Inteligencia Artificial, cuando el psicólogo Frank Rosenblatt creó un modelo análogo de red neuronal con la habilidad de aprender en base al error (Toosi et al., 2021).

Otro aspecto importante de esta temporada de la Inteligencia Artificial, fue la creación del primer robot en esta industria, *Unimate*, un brazo robótico utilizado en General Motors para la soldadura y otros aspectos mecánicos del proceso (Toosi et al., 2021).

Después de una larga época de éxito en este sector, la Inteligencia Artificial sufre una caída, por causa de las falsas predicciones que los expertos habían realizado. Durante el final de la década de los 60 hasta el final de los 80, esta herramienta sufrió un paro en investigaciones que no le permitió avanzar. Sin embargo, con los avances tecnológicos de la década de los 90, inicialmente, con la entrada del Big Data, esta herramienta se recuperó de su percance, ya que se requería de una visión automática para su procesamiento (Toosi et al., 2021).

En el 2001, IBM crea la Iniciativa de Computación Autonómica, siendo uno de los primeros diseños computacionales que requieren de poca interacción humana para poder conseguir los objetivos propuestos. La computación autonómica hace referencia al campo de investigación que estudia cómo los sistemas pueden crear comportamientos adecuados por sí mismos, es decir, sin ayuda humana. Pueden llegar a ser configurados y optimizados de manera autónoma, al igual que, pueden ser sistemas auto protectores y auto curadores. Permitiendo así que el propio sistema sea el que identifica un ataque y se defiende de este, aprendiendo de los errores cometidos previamente (Gill et al., 2022).

La llegada de la computación autónoma permitió, a su vez, la integración del *Machine Learning*, siendo este un proceso clave para la nueva ola tecnológica, integrando así grandes beneficios en esta. Los sistemas autónomos de computación que integren herramientas como la Inteligencia Artificial, permiten un ahorro en tiempo y costes, al igual que mayor estabilidad, ya que aquellas compañías que utilizan este sistema podrán tener mejor manejo de sus negocios implementando estrategias que permitan que la Inteligencia Artificial se adapte al entorno de la manera correcta para así, tener más beneficios (Gill et al., 2022).

Actualmente, se ha visto un gran avance en el ámbito de la Inteligencia Artificial, especialmente desde el 2020. Los programadores han sido capaces de crear algoritmos más completos, también, actualmente las computadoras son más rápidas permitiendo así procesar más información de la que antiguamente se podía procesar. Todos estos aspectos han hecho que la Inteligencia Artificial se vuelva aún más poderosa y tenga mayor capacidad de automatizar los procesos (Toosi et al., 2021).

A su vez, hoy en día la Inteligencia Artificial ha sido capaz de ser programada con capacidades que imiten la inteligencia humana, realizando tareas que requieren del razonamiento. Esta herramienta se encuentra cada vez más desarrollada hacia la capacidad de desarrollar de manera eficaz las tareas cognitivas. La Inteligencia Artificial, actualmente, se refleja como la representación digital o artificial del cerebro humano, llegando, así, a simular el proceso de aprendizaje para realizar tareas específicas (Shabbir & Anwer, 2018).

2.1.2.3. Visión al Futuro

Actualmente existe mucha especulación sobre cómo será el futuro de la Inteligencia Artificial, si será exitosa como lo que se ha visto en los últimos años, o si se tendrá una caída como ha ocurrido en el pasado. Múltiples autores han estudiado este fenómeno y sus posibles predicciones, siendo capaces de concluir que la Inteligencia Artificial se enfrentará a múltiples desafíos en los próximos años.

En primer lugar, se cree que los objetivos de la Inteligencia Artificial afectarán los derechos de la sociedad, al igual que su economía, en un futuro (Shabbir & Anwer, 2018). Uno de los principales retos que presenta la Inteligencia Artificial en un futuro, será la necesidad de regulación, a medida que su implementación se vuelve parte del día a día de la sociedad, será importante la regulación de esta herramienta, evaluando si será necesaria o no (Haenlein & Kaplan, 2019).

Sin embargo, se ha considerado ciertos puntos de micro regulación que se pueden llevar a cabo, como son plantear requisitos específicos en cuanto al entrenamiento y prueba de los algoritmos de la Inteligencia Artificial. Permitiendo así crear sistemas que permitan seguir unas garantías brindando así seguridad en los protocolos a seguir (Haenlein & Kaplan, 2019).

A su vez, se considera que la Inteligencia Artificial proporciona amenazas como la dependencia total de la vida humana en la tecnología, lo cual podrá a llegar a causar problemas sociales como el desempleo, discriminación social y desigualdad de poder en las sociedades (Shabbir & Anwer, 2018).

En segundo lugar, cabe mencionar, que el objetivo de la Inteligencia Artificial es facilitar el día a día de los seres humanos, pero, hay gran debate sobre las ventajas y desventajas que esto conlleva. Sin embargo, esta herramienta llegará a revolucionar la manera en que las compañías crecen y compiten entre ellas (Shabbir & Anwer, 2018).

Por último, múltiples compañías y gobiernos han invertido enormemente en este sector, como consecuencia, si la Inteligencia Artificial vuelve a tener una recaída, múltiples personas perderían sus trabajos como ha ocurrido en el pasado. La exageración y el miedo de la idea que la

Inteligencia Artificial llegará a alcanzar el nivel humano puede ser causa de una recaída del sistema (Toosi et al., 2021).

Por esta razón, se tiene que prestar importante atención a las limitaciones y obstáculos que se presentan en el ámbito. Entre las consideraciones a tomar para evitar la recaída, se encuentran aspectos como la aplicación de un método científico a la hora de investigar este ámbito, para así evitar confusiones de expectativas (Toosi et al., 2021).

2.2. Marco Jurídico

A medida que la tecnología avanza, el uso de la Inteligencia Artificial se vuelve cada vez más, parte del día a día de la sociedad. Sin embargo, la falta de regulación de esta herramienta, puede resultar en un mal uso causando daños a la sociedad.

El retraso en la regulación de la Inteligencia Artificial puede llevar a que los desarrolladores e inversores retiren sus recursos en los proyectos de esta herramienta, para evitar el potencial de riesgo que el desarrollo puede traer consigo (Broadhurst et al., 2019). Como se ha mencionado anteriormente, uno de los desafíos que tendrá la Inteligencia Artificial en un futuro será su regulación, aunque, actualmente varias organizaciones gubernamentales alrededor del mundo han empezado a crear un marco legislativo sobre la temática.

2.2.1. Regulación en otros países

Varios países a lo largo del mundo han creado iniciativas para una regulación en relación a la Inteligencia Artificial. Entre los países donde se ha visto una iniciativa de una regulación, cabe mencionar los siguientes: Estados Unidos de América, Reino Unido y Canadá

En primer lugar, Estados Unidos de América ha mostrado interés e iniciativa en la regulación de la Inteligencia Artificial, creando un anteproyecto para la carta de derechos de la Inteligencia Artificial. Este anteproyecto se basa en cinco principios para guiar el diseño y uso de los sistemas automatizados, al igual que, proteger los derechos de los usuarios de la Inteligencia Artificial (The White House, 2023). Entre los principios se encuentran (The White House, 2022):

- Sistemas seguros y eficaces, este hace referencia a la necesidad de sentirse protegido dentro de los sistemas electrónicos.

- Protecciones contra la discriminación algorítmica, este engloba la equidad necesaria en el uso de esta.
- Privacidad de datos, siendo este principio necesario para que los miembros de la sociedad se sienta protegido de prácticas abusivas de datos, al igual que deben tener autoridad sobre cómo se utilizan sus datos en el medio digital.
- Notificación y explicación, en el cual se explica cómo el usuario ha de saber que está utilizando un sistema automatizado.
- Alternativas humanas, consideración y el fallback, este hace referencia a poder tener acceso para estudiar y solucionar los problemas que se planteen.

Otro país que ha iniciado el desarrollo de su regulación es Reino Unido, quien establece cinco principios en su regulación (Department for Science, Innovation & Technology, 2024):

- El primero siendo la seguridad, protección y solidez, este explica cómo los sistemas de Inteligencia Artificial han de funcionar de manera segura y protegida durante todo su funcionamiento, al igual que, los riesgos que presenten, han de identificarse y evaluarse de manera continua.
- El segundo principio hace referencia a la transparencia y capacidad de explicación de la Inteligencia Artificial y sus funciones.
- El tercer principio hace referencia a la equidad, explicando cómo los sistemas de la Inteligencia Artificial no han de vulnerar los derechos de las personas y las organizaciones, discriminándolos injustamente, por esta razón, los desarrolladores de la herramienta han de considerar las descripciones de la equidad de la manera adecuada para su uso.
- En cuarto lugar, se encuentra el principio de rendición de cuentas y gobernanza, en este se comenta cómo se establecen medidas de gobernanza para garantizar el suministro y uso eficaz de la Inteligencia Artificial, estableciendo a la vez, líneas claras de responsabilidad a lo largo del uso de la herramienta.
- Por último, se encuentra el principio de reparación y contestabilidad, el cual explica que aquellos participantes en el desarrollo de la Inteligencia Artificial han de actuar cuando una decisión de esta herramienta sea perjudicial para la sociedad.

Al igual que estos países, Canadá ha propuesto una iniciativa para regular la cual se encuentra en el *Artificial Intelligence and Data Act.* En el cual se presenta una marco de regulaciones sobre el uso apropiado y no discriminatorio que la Inteligencia Artificial ha de presentar, al igual que se determina que las empresas han de responsabilizarse por su desarrollo y uso de esta herramienta. Esta regulación introduce requisitos nuevos para que las empresas garanticen la seguridad del desarrollo de la Inteligencia Artificial, siendo estos (Government of Canada, 2023):

- Diseño: las empresas han de identificar los riesgos que su herramienta de Inteligencia Artificial propone.
- Desarrollo: deberán evaluar el uso y limitaciones de la herramienta, asegurándose que los usuarios sean capaces de comprenderla.
- Implantación: se deberá poner en marcha estrategias adecuadas para mitigar los riesgos de la Inteligencia Artificial, implementando una supervisión continua de estas.

Estos países han sido los primeros en proponer un marco legislativo para la regulación de la Inteligencia Artificial, lo cual resalta la importancia de los avances tecnológicos y la necesidad de establecer normas que regulen su desarrollo y uso. Estas iniciativas demuestran la importancia y urgencia de abordar los riesgos que acompañan la implementación de esta herramienta.

2.2.2. Unión Europea

La Unión Europea ha sido la primera organización en regular la Inteligencia Artificial. Aprobando el pasado 13 de marzo de 2024 el *AI Act* (Ley de Inteligencia Artificia, en español) en base a las preocupaciones del rápido desarrollo que la tecnología presenta para la humanidad. Esta regulación tiene como objetivo proporcionar requisitos y obligaciones claras a los desarrolladores de la Inteligencia Artificial (European Commission, 2024).

La Ley de Inteligencia Artificia es parte de un amplio conjunto de políticas que buscan garantizar la seguridad y los derechos fundamentales de los particulares y empresas que utilizan la Inteligencia Artificial. Estas normas buscan garantizar que esta herramienta respete los derechos fundamentales, seguridad y principios éticos de la sociedad (European Commission, 2024).

Esta regulación asegura a los usuarios dentro de la Unión Europea que la herramienta de Inteligencia Artificial es segura de utilizar. Entre las reglas que esta regulación propone, se encuentra la obligación de determinar las aplicaciones consideradas de alto riesgo, prohibir aquellas prácticas que propongan un riesgo en su uso, abordar los riesgos creados por las aplicaciones de la Inteligencia Artificial y el requisito de una evaluación de la conformidad antes de que este sistema sea utilizado por el público (European Commission, 2024).

De la misma manera, la Ley de Inteligencia Artificia prohíbe los sistemas impulsados por esta herramienta que utilicen puntuación social y biométrica para la identificación de raza, orientación sexual o inclinación política. Al igual que prohíbe el uso de la Inteligencia Artificial para interpretar las emociones de los sujetos (Fung, 2024).

Esta regulación utiliza el riesgo como factor de acercamiento, postulando cuatro niveles principales del riesgo. En el eslabón más bajo se encuentra el riesgo mínimo, según la regulación, se permite el uso libre de la Inteligencia Artificial de bajo riesgo, como son los filtros de spam o aquellos videojuegos que utilizan la herramienta (European Commission, 2024).

El siguiente eslabón, es el riesgo limitado. Este hace referencia a la falta de transparencia que viene asociada con el uso de la Inteligencia Artificial. Esta categoría hace referencia a sistemas como los *chatbots* En estos casos, será necesario confirmar al usuario que se está utilizando un sistema de Inteligencia Artificial. De la misma manera, el desarrollador ha de garantizar que el contenido sea identificable (European Commission, 2024).

El tercer escalón, hace referencia al alto riesgo. Este incluye categorías donde la tecnología es utilizada como son la infraestructura crítica, la educación, servicios públicos y privados, control de fronteras, administración de justicia y en casos donde los derechos fundamentales de los ciudadanos se pueda ver afectado. Por último, se encuentra el riesgo inaceptable, este hace referencia a las actividades prohibidas como son los sistemas de puntuación social y manipulación (European Commission, 2024).

2.2.3. España

España ha sido otro país en tomar iniciativa en la creación de una regulación estable sobre la temática de la Inteligencia Artificial, estableciendo el *Real Decreto 817/2023, de 8 de noviembre,*

que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

En su primer artículo, se establece el objeto del Real Decreto, siendo este proporcionar un entorno controlado en el cual se pueda demostrar el cumplimiento de requisitos de la Inteligencia Artificial y que esta no presenta un riesgo para la seguridad y derechos fundamentales de los usuarios. El artículo dos explicará el ámbito de aplicación como toda aquella administración pública y entidad del sector público.

El Real Decreto 817/2023 establece también una serie de garantías y responsabilidades que los participantes han de tener, como es la protección de datos personales, lo cual se observa en el artículo 16; la responsabilidad de los participantes, explicado en el artículo 17, el cual hace referencia a cómo los usuarios y proveedores del sistema de Inteligencia Artificial, serán responsables de los daños causados a terceros por el uso de esta herramienta dentro del entorno de prueba. De la misma manera, el artículo 18 hace referencia a la confidencialidad aplicada a la información que los proveedores y participantes aporten.

Por otro lado, en el Código Penal Español (en adelante, CP), algunos ciberdelitos se encuentran tipificado en los artículos 186, 197, 197 bis, 197 ter, 197 quater, 197 quinquies, 249 y 264. En primer lugar, el artículo 186 se encuentra dentro del Capítulo IV: de los delitos de exhibicionismo y provocación sexual del Título VIII. Este artículo hace referencia a la venta, difusión o exhibición de material pornográfico de menores o personas con discapacidad, con una pena de prisión de seis mesas a un año o una multa de doce meses a veinticuatro meses.

El artículo 197 CP tipifica como delito la conducta llevada a cabo por aquellos que sin estar autorizados utilicen, apoderen o modifiquen datos que sean reservados en carácter personal o familiar de un tercero, y estén registrados en ficheros o soportes informáticos, y establece como castigado la pena de prisión de uno a cuatro años, al igual que una multa de doce a veinticuatro meses. Lo mismo se ve reflejado en el artículo 197 bis CP, e1cual establece que aquellos que no estén autorizados, vulneren las medidas de seguridad, accedan o faciliten el acceso por medio de sistemas informáticos, serán castigados con una pena de prisión de seis meses a dos años. Al igual que, menciona como aquellos que sin autorización debida intercepten transmisiones de datos

informáticos serán castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

De la misma manera, el artículo 197 ter CP, hace referencia a la adquisición de datos privados con el objetivo de facilitar la comisión de algún delito. El artículo 197 quater CP, por su parte, hace referencia a los delitos ya mencionados pero realizados por una organización o grupo criminal, en estos casos se aplicara la pena superior en grado. De igual forma, el artículo 197 quinquies CP, hace referencia a la responsabilidad penal que se aplica cuando el sujeto activo sea una persona jurídica.

Por otro lado, el artículo 249 CP hace referencia a las estafas informáticas, explicando que aquellos que con ánimo de lucro, interfieran, introduzcan, alteren, borren, transmitan o supriman de manera indebida los sistemas informática o datos informáticos para conseguir una transferencia no consentida de cualquier patrimonio perjudicando a otra persona, serán castigados con una pena de prisión de seis meses a tres años.

Por último, el artículo 264 CP explica cómo será castigado con una pena de prisión de seis meses a tres años, aquellos que por cualquier medio y sin autorización borre, dañe, deteriore, altere, suprima o haga inaccesible de manera grave los datos, programas o documentos informáticos ajenos. De la misma manera, en el artículo 264.2 CP se explica que se aplicará la pena de prisión será de dos a cinco años y una multa del tanto al décuplo del perjuicio ocasionado cuando ocurra una de las siguientes conductas:

a. Se cometa por una organización criminal;
b. Haya ocasionado daños especialmente graves o afecten a una gran cantidad de sistemas informáticos;
c. Haya perjudicado gravemente el funcionamiento de los servicios públicos esenciales;
d. Haya afectado el sistema informático de una infraestructura crítica o se haya creado una situación de peligro grave para la seguridad del Estado, Unión Europea o Estado Miembro de la Unión Europea.

2.2.4. Comparación de las regulaciones

Una vez analizados los distintos marcos jurídicos de diversos países alrededor del mundo, resulta esencial comparar estas regulaciones con aquella establecida en España. Como se ha estudiado en el apartado anterior, en España, el uso de la Inteligencia Artificial está regulado por el Real Decreto 817/2023, el cual resalta la necesidad de proporcionar un entorno controlado en donde se pueda supervisar la Inteligencia Artificial para probar que esta no presente un riesgo para la seguridad.

De la misma manera, las regulaciones en otros países también buscan proteger la seguridad de los ciudadanos, como ocurre en el caso de Estados Unidos de América, Reino Unido y Canadá. Estos países presentan normativas que se centran en garantizar que el desarrollo de la Inteligencia Artificial se lleve a cabo de manera ética y segura, donde exista una supervisión para poder prevenir los posibles riesgos que puedan afectar la seguridad y privacidad de los individuos. Estas similitudes muestran la importancia de unificar la regulación del uso de la Inteligencia Artificial.

España, Reino Unido, Canadá y Estados Unidos proporcionan una visión más humanista en sus marcos jurídicos, colocando la protección de la sociedad como enfoque principal. Estas regulaciones hacen especial énfasis en la privacidad, seguridad y transparencia en el desarrollo y utilización de la Inteligencia Artificial, enfocándose en garantizar que esta herramienta respete los derechos individuales y no presenten un riesgo o amenaza a la seguridad pública.

2.3. Ciberdelitos e Inteligencia Artificial

El avance tecnológico ha traído consigo una gran cantidad de beneficios para la sociedad, pero este desarrollo ha causado también la llegada de una nueva oleada de delitos, conocidos como ciberdelitos o delitos cibernéticos. Esta rama de delitos es realmente compleja, ya que el autor del delito y las víctimas se pueden encontrar en distintos lugares del mundo, de la misma manera, los efectos de esta tipología de delitos pueden afectar a toda la sociedad (United Nations, 2020).

La Europol informa que los ciberdelitos son un problema que ha crecido en múltiples países de la Unión Europea, con la automatización y digitalización de los medios de pagos, los datos financieros han sido objetivo clave para los ciberdelincuentes, sin embargo, este no es el único tipo de objetivo que estos agentes tienen (Europol, 2022).

Estos avances tecnológicos han brindado una gran cantidad de oportunidades para la sociedad, oportunidades que los ciberdelincuentes han tratado de explotar para así beneficiarse de estas. La Europol clasifica como *delitos de alta tecnología* a todos aquellos delitos donde el malware se infiltra y obtiene el control del sistema informático para así robar y/o dañar datos (Europol, 2022). Es importante recalcar, que el término malware hace referencia a aquellos programas informáticos que atacan de manera dañina a otros programas (Kramer & Bradfield, 2010)

Entre las metodologías de ataque en los delitos de alta tecnología, la Europol menciona estrategias como el (1) *Ransomware*, siendo ésta similar a un secuestro, ya que el agresor impide al usuario tener acceso a sus dispositivos y exige un pago como rescate para acceder a estos nuevamente. El (2) *Spyware*, el cual consiste en un programa que se instala en el ordenador de la víctima sin el conocimiento de esta, una vez instalada, el agresor puede vigilar y transmitir la información a terceros (Europol, 2022).

Al igual que menciona el uso de (3) *puerta trasera o el troyano con acceso remoto*, una estrategia que permite acceder a un sistema de manera remota, este puede ser instalado por otro malware y otorga un acceso casi total al agresor para realizar múltiples acciones (Europol, 2022). Estas estrategias, permiten a los agresores cometer delitos como el ciberterrorismo, ciber espionaje, pornografía infantil, ciberacoso, *phishing* y ataques de denegación de servicio (*DoS*).

El ciberterrorismo hace referencia a todas aquellas acciones que implican daños a personas y propiedades, que, frecuentemente, tienen fines políticos o ideológicos. Esta tipología busca sembrar miedo, ansiedad y violencia entre los miembros de la sociedad, llegando a afectar la disponibilidad e integridad de la información. Por otro lado, se entiende por ciber espionaje al conjunto de acciones que se realizan para espiar y obtener información sensible e importante para el beneficio de otras empresas o instituciones gubernamentales (Al-Khater et al., 2020).

La pornografía infantil en el ámbito cibernético hace referencia a la difusión de videos, audios y fotografías de menores utilizando vestimenta inapropiada, o utilizando poca o ningún tipo de vestimenta, en posiciones con connotación sexual (Ibrahim et al., 2021). La distribución de la pornografía infantil suele presentar dos fines principales, estos siendo con o sin ánimo de lucro. La distribución con ánimo de lucro suele ser vendida en sitios webs, mientras la distribución sin fines lucrativos se comparte utilizando la P2P (Al-Khater et al., 2020).

Por otro lado, el ciberacoso implica el uso de amenazas, chantaje y burlas para así intimidar, acosar y dominar a las víctimas por medio de las redes sociales e informáticas (Ibrahim et al., 2021). Se considera ciberacoso a su vez, actividades delictivas como son el robo de identidad, robo de tarjetas de crédito, intimidación y abuso y manipulación psicológica (Al-Khater et al., 2020).

El phishing es una tipología de ataque cibernético que busca atacar las debilidades del sistema, para persuadir a la víctima a realizar acciones que beneficien al atacante. Este es el tipo más común de ciberdelitos, ya que permite una conexión directa entre agresor y víctima. Por último, los ataques de denegación de servicio (*DoS*) son aquellos ataques que colapsan los sistemas, ya que pretenden agotar los recursos de estas y dejarlos indisponibles para los usuarios. En las últimas décadas, estos ataques han sido la gran preocupación dentro del ámbito de la ciberseguridad (Al-Khater et al., 2020; Ibrahim et al., 2021).

Por último, la inyección SQL hace referencia a la herramienta SQL*, Structured Query Language* (en español, *lenguaje de consulta estructurada*), la cual se utiliza para organizar, recuperar y gestionar datos que se encuentran almacenados en las bases de datos de las computadoras (Groff & Weinberg, 1999). La inyección SQL compromete la protección de la infraestructura de las bases de datos y sistemas de la red. Esta inyección es capaz de causar propagaciones de virus, violaciones de privacidad, control remoto de servidores y parálisis de las redes (Kareem et al., 2021).

2.3.1. Estadística del cibercrimen

La tecnología permite que todos los miembros de la sociedad estén conectados entre sí en cualquier momento, sin embargo, esta conexión permite, a la vez, que los agresores puedan contactar a las víctimas de manera simultánea. En el Portal Estadístico de la Criminalidad, publicado por el Ministerio del Interior Español, se publicó que en el año 2022 existieron 374.737 hechos conocidos de infracciones penales relacionadas con la delincuencia cibernética, de los cuales 15.097 fueron detenidos (Figura 1). Comparando estos datos con el año anterior, se observa un incremento de 22.7%, sin embargo, comparado al año 2018 el incremento de ciberdelitos ha sido de 133%, demostrando cómo estos presentan una amenaza cada vez mayor para la sociedad (Tabla 1).

Figura 1.

Comparación de los hechos conocidos, esclarecidos y detenciones en el ámbito de ciberdelitos en el año 2022.

Fuente: Elaboración propia con datos proporcionados por el Portal Estadístico de la Criminalidad del Ministerio del Interior (2022).

Tabla 1.

Incremento de los hechos conocidos de ciberdelitos del 2019 a 2022.

Incremento en base al 2018	
2019	35.80%
2020	79.20%
2021	90%
2022	133%

Incremento en base al año anterior	
2019	35.80%
2020	31.90%
2021	6.10%
2022	22.70%

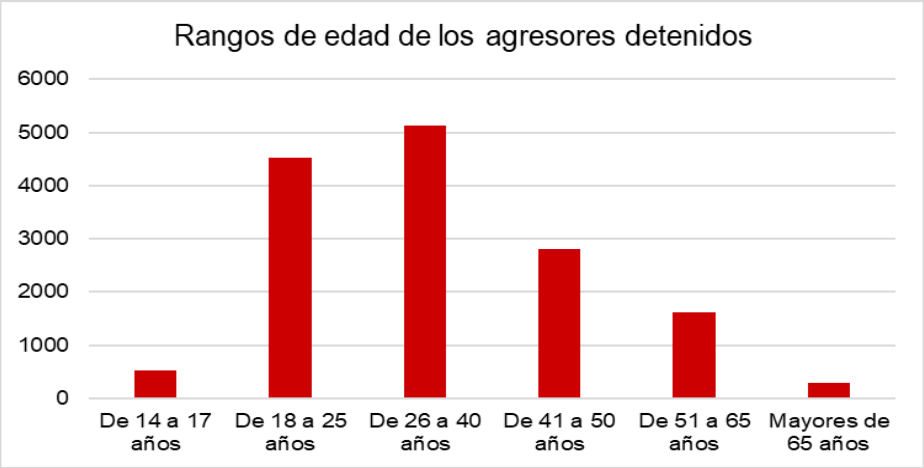
Fuente: Elaboración propia con datos proporcionados por el Portal Estadístico de la Criminalidad del Ministerio del Interior (2022).

En cuanto a la demografía de los agresores, el Portal Estadístico de la Criminalidad del Ministerio del Interior (2022) resalta que la mayoría de estos son hombres, ubicados en el rango de edad de 26 a 40 años, como bien se refleja en la Figura 2. De la misma manera, se demuestra que el fraude informático es el delito más recurrente, sin embargo, destaca una tendencia

interesante en las edades de 14 a 17 años, donde se observa que las agresoras femeninas tienden a involucrarse con mayor frecuencia en delitos de amenazas y coacciones.

Figura 2.

Rangos de edad de los agresores detenidos registrados por el Portal de Estadístico de la Criminalidad en el año 2022.



Fuente: Elaboración propia con datos proporcionados por el Portal Estadístico de la Criminalidad del Ministerio del Interior (2022).

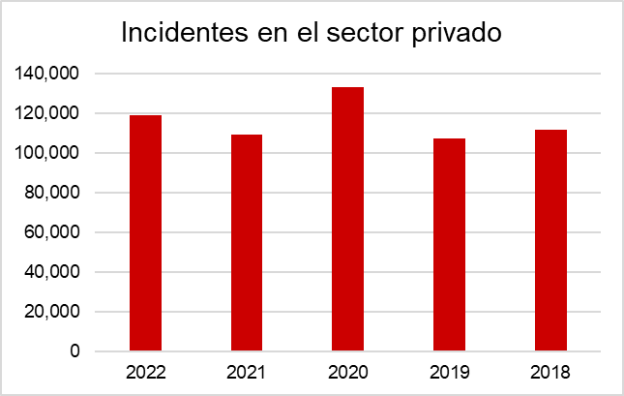
En otro reporte realizado por el Instituto Nacional de Ciberseguridad (INCIBE) (Instituto Nacional de Ciberseguridad, 2022) se concluyó que para el año 2022 se gestionaron un total de 118.820 incidentes de ciberseguridad en el sector privado, que, comparado al año anterior, ha incrementado un 8.8%, sin embargo, comparado al año 2020, ha disminuido 10% (Figura 3). En cuanto a la tipología más común en este sector, registrados por el INCIBE, resalta, como se observa en la Figura 4, como en el 2021 existió un pico en cuanto a los ataques de Malware comparado con los ataques ocurridos en el 2022, sin embargo, se registró que en el 2022, los ataques a los sistemas vulnerables tuvieron un aumento de 150% comparado al año anterior (Muniesa et al., 2022).

Estos datos estadísticos demuestran cómo los problemas informáticos han ido incrementando en los últimos años. Específicamente, cabe a mencionar que, dentro de los delitos contra el patrimonio, las estafas informáticas resaltan como la tercera tipología más común, con

un total de 335.995 casos conocidos (Figura 5). Este incremento en la incidencia de estafas informáticas resalta la necesidad de fortalecer las medidas de ciberseguridad, al igual que la necesidad de concienciar a los individuos y organizaciones sobre las amenazas digitales.

Figura 3.

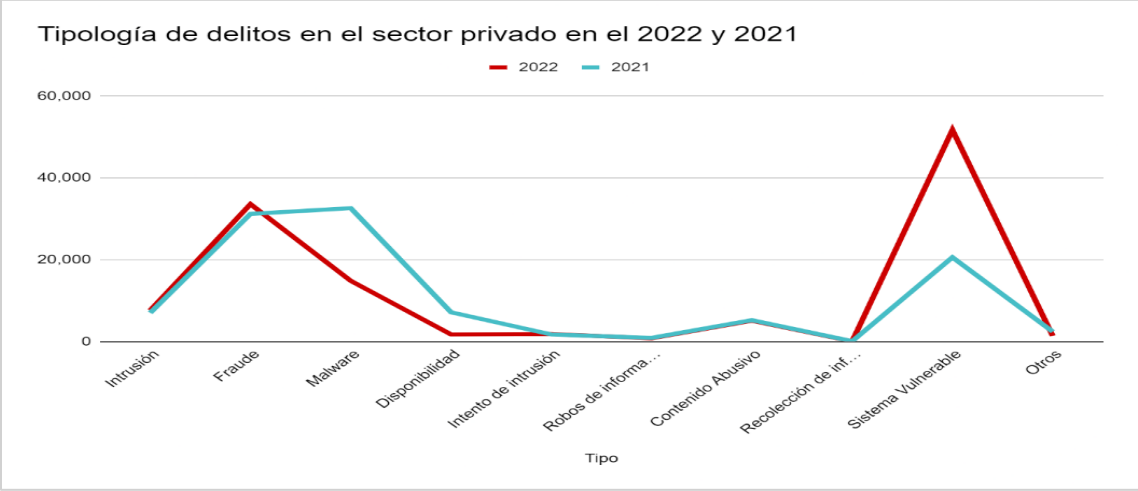
Incidentes ocurridos en el sector privado en el año 2022.



Fuente: Elaboración propia con datos proporcionados por el Instituto Nacional de Ciberseguridad (2022).

Figura 4.

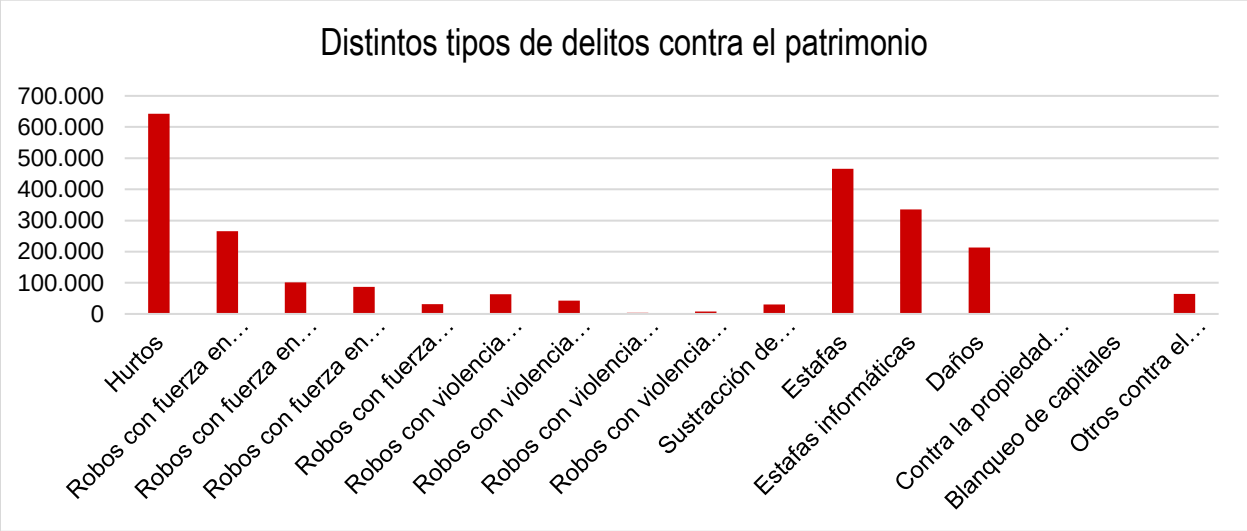
Comparación de la tipología de delitos en el sector privado durante los años 2021 y 2022.



Fuente: Elaboración propia con datos proporcionados por el Instituto Nacional de Ciberseguridad (2022).

Figura 5.

Cantidad de los distintos tipos de delitos contra el patrimonio durante el año 2022.



Fuente: Elaboración propia con datos proporcionados por el Portal Estadístico de la Criminalidad del Ministerio del Interior (2022).

2.3.2. Detección y lucha actual contra los ciberdelitos

Como se ha observado, los ciberdelitos son una amenaza a la seguridad, aumentando cada vez más a lo largo de los años. Esta tipología de delitos es uno de los mayores riesgos económicos a nivel internacional. Por esta razón, existe una necesidad de reforzar los sistemas de seguridad digital. Boes y Leukfeldt (2017) proponen una estrategia integrada de los sistemas de seguridad utilizados en el ámbito privado y en el ámbito público.

En primer lugar, se propone que los usuarios utilicen técnicas para proteger sus dispositivos informáticos, por ejemplo con el uso de un antivirus, al igual que se propone la concienciación de la actividad en línea, específicamente sobre la información personal que se comparte. De esta manera, los usuarios podrán disminuir la probabilidad de ser víctimas de ataques cibernéticos. Después, se encuentran los miembros de empresas de seguridad privadas y agentes de las Fuerzas y Cuerpos de Seguridad, quienes investigarán aquellos delitos que ocurran en los distintos ámbitos de la delincuencia cibernética (Boes & Leukfeldt, 2017).

Sin embargo, se ha demostrado que uno de los problemas principales que presenta esta tipología criminal, es su rápido crecimiento e innovación, el cuál crece a medida que se desarrollan nuevas tecnologías y herramientas. Otros de los problemas que se presentan son el anonimato digital y la falta de control dentro del espacio cibernético (Boes & Leukfeldt, 2017).

Por otro lado, la Comisión Europea ha propuesto diversas estrategias para luchar contra estos delitos, en primer lugar se encuentra la Estrategia de ciberseguridad de la Unión Europea para la Década Digital, publicada en el 2020, la cual tiene como objetivo apoyar a los Estados miembros en la defensa de sus ciudadanos y seguridad nacional por medio de instrumentos normativos, movilización y cooperación (European Commission, 2020b; Murphy, 2024).

Dentro de esta, se encuentra la idea de una *Ciber Unidad Conjunta*, la cual podría proporcionar una plataforma física y virtual de cooperación en materia de ciberseguridad dentro de la Unión Europea, buscando centrarse en la coordinación operativa y técnicas contra los incidentes y amenazas cibernéticos. Esta unidad podrá alcanzar tres objetivos principales, en primer lugar, podría garantizar la preparación de todas la comunidades de ciberseguridad, en segundo lugar, podría brindar apoyo y conocimiento continuo por el intercambio de información y en último lugar, permitirá una coordinación de respuesta en todos los países miembros (European Commission, 2020).

Otra de las estrategias mencionadas por la Comisión Europea, es la *Estrategia 2020-2025 de la Seguridad de la Unión*, esta tiene cuatro objetivos principales. El primero será velar por una política de seguridad que refleje el panorama cambiante de las amenazas; en segundo lugar, se busca crear una resistencia sostenible a largo plazo. El tercer objetivo será implicar a todos los sectores afectados en un planteamiento que englobe a toda la sociedad; y, el cuarto objetivo será reunir todas las áreas de la política que tienen un impacto en la seguridad (European Commission, 2020a).

De la misma manera, esta estrategia se basa en cuatro pilares fundamentales. El primer pilar, hace referencia a la lucha contra el terrorismo y el crimen organizado; el segundo pilar, hace referencia al futuro del entorno de la seguridad, dentro de este pilar encontraremos pasos para la protección de la infraestructura critica, espacios públicos y ciberseguridad. El tercer pilar, se refiere a crear un ecosistema de seguridad rígido y fuerte. Por último, el cuarto pilar hace referencia

a hacer frente a la evolución de las amenazas, específicamente aquellas que ocurren en el ámbito cibernético (European Commission, 2020a).

Al igual que la Comisión Europea, la Europol ha creado un Centro Europeo de la Ciberdelincuencia (EC3). Este proporciona evaluaciones especializadas en las nuevas tendencias y métodos que los delincuentes emplean. El EC3, se enfoca principalmente en tres tipos de ciberdelitos, el fraude en pagos, explotación sexual infantil y ciberdelincuencia. Este centro proporciona estrategias, análisis, apoyo forense y operacional (Europol, 2023a).

El Centro Europeo de la Ciberdelincuencia ha realizado contribuciones importantes a la lucha contra la ciberdelincuencia. Todos los años, este centro realiza un informe estratégico sobre las principales conclusiones, amenazas y novedades principales en esta materia, conocido como IOCTA. Este informe proporciona recomendaciones claves para el reforzamiento del orden y respuesta a la ciberdelincuencia de manera eficaz (Europol, 2023b; Murphy, 2024).

Otro factor importante en la prevención y lucha contra los ciberdelitos es la encriptación de datos. La encriptación es un método utilizado para asegurar los datos que se comparten en una red o sitio de almacenamiento inseguro (Boneh et al., 2010). Este proceso convierte el texto sin formato, siendo este el mensaje original que se desea enviar, en texto cifrado, este será el mensaje que no puede ser descifrado. Para poder desencriptar el mensaje, se requiere una llave que permita realizar este proceso (Thambiraja et al., 2012).

2.3.3. Inteligencia Artificial y ciberseguridad

El uso de la Inteligencia Artificial en el ámbito de la ciberseguridad es cada vez más relevante, ya que permite ser utilizada para mejorar la seguridad en el ámbito cibernético (Alhayani et al., 2021). Como se ha mencionado anteriormente, la Inteligencia Artificial ayuda al análisis de grandes cantidades de datos, sin embargo, esta herramienta puede y en ocasiones es utilizada para la detección de patrones.

Gran parte de los ciberdelitos siguen una estrategia ordenada a la hora de realizar sus ataques, en la cual los agresores buscan huecos y vulnerabilidades en el sistema, para así utilizar códigos malignos para acceder y transferir el malware, llegando así al último paso, la explotación, en donde se instala el código maligno y compromete al sistema, para así obtener la información buscada. En

estos casos, se podría aplicar la herramienta de la Inteligencia Artificial para generar avisos tempranos del ataque, permitiendo a los expertos en ciberseguridad tiempo previo para actuar y evitar que este suceda (Wirkuttis & Hadas, 2017).

La aplicación de técnicas de la Inteligencia Artificial también podrán ser utilizadas en el ámbito de la predicción de tendencias criminales, empleando una combinación de métodos analíticos para así poder estimar la probabilidad de manera estadística la probabilidad de que un crimen ocurra. De la misma manera, el uso de la Inteligencia Artificial muestra su relevancia en las técnicas defensivas de la ciberseguridad, ya que, en esta técnica, se hace referencia a los modelos de antivirus generados por la Inteligencia Artificial, al igual que a la categorización de amenazas (Broadhurst et al., 2019).

Dentro de las técnicas defensivas, la Inteligencia Artificial puede ser utilizada en métodos como la detección de malware, para detectar de manera rápida los ataques, ya que en base al aprendizaje de experiencias previas, esta herramienta podrá ser capaz de adaptarse y, así, ejecutar respuestas efectivas a los ataques. Al utilizar la Inteligencia Artificial para poder llevar a cabo este proceso, la respuesta será más rápida y precisa, ya que esta herramienta tiene la capacidad de analizar grandes cantidades de datos, aprendiendo así sobre las distintas variaciones de la detección de malware (Broadhurst et al., 2019).

La Inteligencia Artificial también se podrá utilizar para la detección tanto de vulnerabilidades en el sistema y como de amenazas. En ambos casos, esta herramienta es de gran utilización, ya que permite la automatización de estas tareas, ya que se puede entrenar a la Inteligencia Artificial a entender los distintos tipos de vulnerabilidades y amenazas que se han encontrado previamente, para así generar respuestas adecuadas a la agresión sufrida. También, esta herramienta tiene dos funciones importantes, analizar grandes cantidades de datos y ejecutar respuestas de manera más veloz que un humano (Broadhurst et al., 2019).

La ciberseguridad presenta grandes retos, como es la cantidad de datos a analizar, ya que con el crecimiento exponencial de los dispositivos electrónicos, cada vez más se transmiten datos, por lo que se ha de optimizar el proceso de su análisis. También, la heterogeneidad de los datos y sus fuentes hace más complicada la identificación y clasificación de los datos, al igual que ocurre con la velocidad en que los datos son producidos y procesados. Para tratar con estos retos, la

Inteligencia Artificial puede ser programada para evaluar y analizar la información de manera más rápida y eficiente para así poder responder a tiempo a un ataque (Wirkuttis & Hadas, 2017).

La automatización del proceso por medio de la Inteligencia Artificial causará que los agresores no puedan utilizar el mismo modus operandi ya que el sistema lo detectará con mayor facilidad. Al igual que minimiza el rango de error que se presenta a la hora de resolver los ciberataques (Ansari et al., 2022). Es importante mencionar que la Inteligencia Artificial permite crear sistemas que agilicen el proceso, sin embargo estos sistemas han de contar con aspectos como la privacidad, equidad, fiabilidad, causalidad y trazabilidad, para permitir que su análisis sea el adecuado (Rubio, 2021).

2.4. Rol de la criminología en el ámbito de la ciberseguridad

El papel del criminólogo es de relevante importancia en el mundo de la ciberseguridad, ya que estos profesionales poseen herramientas para entender y analizar las motivaciones, comportamientos y tendencias de los ciber agresores. De la misma manera, la ciberseguridad es un ámbito interdisciplinar, lo cual es esencial para poder entender todo lo que el espacio cibernético comprende, como es el aspecto fundamental de las investigaciones y los reportes realizados en el ámbito de la ciberseguridad, los cuales son realizados por profesionales en la criminología (Maalem Lahcen et al., 2020).

Sin embargo, el número de estudios criminológicos sobre la ciberdelincuencia son escasos por la falta de profesionales de la criminología especializados en esta temática, lo cual puede ser consecuencia de la dificultad a la hora de clasificar la ciberdelincuencia dentro del umbral de delitos tradicionales (Dupont & Whelan, 2021; Maalem Lahcen et al., 2020). Sin embargo, para afrontar este problema, algunos criminólogos han creado estrategias que consisten en el desarrollo de tipologías inclusivas dentro de la ciberdelincuencia para poder diferenciar entre los delitos que aprovechan la tecnología para aplicar formas ya existentes de delincuencia como es el caso del fraude o distribución de pornografía infantil; y los delitos que no existieran si no fuera por el ámbito digital, como son los delitos de hacking o malware (Dupont & Whelan, 2021).

Uno de los mayores impactos que la criminología ha tenido en el ámbito de la ciberseguridad es el desarrollo y aplicación de teorías que explican los factores de comportamiento humano del

desarrollo de ciberdelitos, como son el aprendizaje social, las técnicas de neutralización, y la teoría de las actividades rutinarias. Esta última es de gran relevancia para la criminología y la ciberseguridad (Dupont & Whelan, 2021; Maalem Lahcen et al., 2020).

Desarrollada por Cohen y Felson en 1979, la teoría de actividades rutinarias, explica que las estructuras de las actividades influyen en la oportunidad delictiva, afectando así, a lo que los autores denominan *violaciones predatorias por contacto directo*, siendo esto los actos ilegales que alguien efectúa de manera definitiva e intencionada hacia la persona o propiedad de otro (Cohen & Felson, 1979).

Los cambios estructurales que la teoría de las actividades rutinarias pueden influenciar el índice de delincuencia afectando el tiempo y el espacio en tres elementos principales: (1) delincuentes motivados, (2) objetivos adecuados y (3) ausencia de guardianes capaces. La ausencia de uno de los elementos es suficiente para impedir el éxito en la ejecución del delito. En el caso de la ciberdelincuencia, el delincuente motivado será el agresor, los objetivos adecuados, harán referencia a aquello que motiva al agresor, como puede ser la información bancaria, y la ausencia de guardianes, será la ausencia de antivirus o de una encriptación de la información (Cohen & Felson, 1979; Kigerl, 2012).

Por otro lado, como se ha mencionado previamente, otra de las teorías relevantes en la criminología que han tenido implicación en el ámbito de la ciberseguridad son las técnicas de neutralización propuestas por Sykes y Matza en 1957. Esta teoría explica cómo los agresores suelen desarrollar creencias que apoyan los valores de las leyes penales, por lo cual han de utilizar técnicas para neutralizar la culpa antes de cometer el delito. Los autores proponen cinco técnicas (Stalans & Donner, 2018; Sykes & Matza, 1957):

(1) Negación de la responsabilidad, que consiste en la falta de responsabilidad que el agresor se otorga por sus acciones, causando así un desplazamiento de la culpa.

(2) Negación del daño, en el que el agresor minimiza los daños causados a la víctima

(3) Negación de la víctima, en donde el agresor transforma a la víctima en culpable o que esta merece el daño causado.

(4) Condenar a los condensadores, técnica consistente en que el agresor no declara su comportamiento como erróneo o incorrecto.

(5) Apelación a lealtades superiores, donde el agresor argumenta cómo sus acciones son motivadas por valores más importantes o porque han de cumplir con las demandas de una sociedad mayor.

Utilizando como base esta teoría, se han realizado estudios que demuestran cómo el uso de dichas técnicas de neutralización están relacionadas con el aumento de prácticas como el hacking (Stalans & Donner, 2018; Sykes & Matza, 1957).

La criminología y el desarrollo de teorías criminológicas son de relevante importancia en el ámbito de la ciberseguridad, ya que esta visión permitirá el buen entendimiento de las amenazas que se presentan en el mundo digital. La visión multidisciplinar busca integrar explicaciones del comportamiento criminal cibernético en base al criminal tradicional, sin embargo, se vuelve una tarea compleja, ya que encontramos múltiples facetas que no pueden ser explicadas desde un solo punto de vista (Stalans & Donner, 2018).

La colaboración entre ambos campos podría ser altamente beneficiosa, sobre todo, a medida que los aspectos conductuales de la ciberseguridad toman cada vez más relevancia. La perspectiva criminológica permitirá entender las técnicas utilizadas en el ámbito de la ciberdelincuencia, al igual que permitirán que los profesionales tengan una visión interdisciplinaria, para así tomar en cuenta las distintas tácticas utilizadas por los agresores y poder combatirlas (Maalem Lahcen et al., 2020).

2.5. Objetivos de Desarrollo Sostenible

El 25 de septiembre de 2015, los Estados Miembros de las Naciones Unidas aprueban la conocida Agenda 2030, la cual busca “poner fin a la pobreza, proteger el planeta y mejorar las vidas y perspectivas de las personas en todo el mundo” (Naciones Unidas, s. f.-a). La Agenda 2030 se compone de 17 Objetivos de Desarrollo Sostenible (O.D.S.) a alcanzar para el año 2030.

En relación al presente trabajo, cabe destacar dos de estos objetivos, el O.D.S número 9 y el O.D.S número 16. En primer lugar, el O.D.S número 9, *Construir infraestructuras resilientes*,

promover la industrialización sostenible y fomentar la innovación, busca promover las infraestructuras resilientes, por medio de la industrialización sostenible, fomentando la innovación. Una de las metas de dicho objetivo hace referencia a modernizar la infraestructura promoviendo la adaptación a la tecnología, al igual que, menciona cómo se ha de apoyar el desarrollo tecnológico (Naciones Unidas, s. f.-b). En este O.D.S resalta la importancia de la ciberseguridad para permitir una infraestructura tecnológica segura en donde la protección de datos e integridad de las redes sea la prioridad, al igual que es un ámbito que permite que la adaptación tecnológica sea más segura para las empresas y miembros de la sociedad.

Por otro lado, el O.D.S número 16, *Promover sociedades justas, pacíficas e inclusivas*, busca promover sociedades pacíficas y responsables, en donde las personas puedan vivir en un ambiente sin miedo a ser víctima de cualquier tipo de violencia. En cuanto a las metas específicas de este O.D.S se encuentra la reducción de todas las formas de violencia; el fin de la explotación infantil; fortalecer la lucha contra el crimen organizado; entre otras (Naciones Unidas, s. f.-c). Este O.D.S propone aspectos fundamentales para poder promover las sociedades pacíficas y minimizar el miedo en la sociedad, con el desarrollo de las nuevas tecnologías, los ciberdelitos tienen mayor impacto en la vida de los miembros de esta. Cumpliendo este O.D.S se podrá reducir la violencia y delincuencia incluyendo la cibernética.

2.6. Formulación de Hipótesis: resultados esperados

En cuanto a las hipótesis planteadas en el siguiente trabajo de investigación, se encuentran:

H1: La Inteligencia Artificial se utiliza para el análisis eficaz y eficiente de la información digital, por medio de la automatización de procesos.

H2: La Inteligencia Artificial, junto el rol del criminólogo permite entender los patrones de delincuencia en su profundidad y desarrollar sistemas de Inteligencia Artificial eficientes en el ámbito de la ciberseguridad.

3 METODOLOGÍA DE INVESTIGACIÓN

3.1. Metodología

Para la realización del presente trabajo de investigación, se ha optado por una metodología cualitativa para así poder responder la pregunta de investigación y comprobar las hipótesis de formuladas. La metodología cualitativa utiliza herramientas como los textos y discursos para entender y poder profundizar en los distintos fenómenos, teniendo en cuenta las perspectivas de los participantes. Este tipo de investigación, utiliza técnicas como la observación, entrevista, cuestionario, entre otras (Guerrero, 2016).

Esta investigación se dividió en dos partes. La primera parte, se constituyó en una búsqueda exhaustiva de datos e información fiable sobre la temática. Para esto, se realizó una búsqueda de datos de organizaciones nacionales e internacionales como la Interpol, Europol, Portal Estadístico de la Criminalidad del Ministerio del Interior, Instituto Nacional de Ciberseguridad, entre otros. También, que se realizó una búsqueda de artículos científicos, como fuentes secundarias, en distintas bases de datos, para realizar un análisis de contenido con la finalidad de obtener un entendimiento profundo sobre la temática y regulaciones en distintos países del mundo, incluyendo España.

Posteriormente, se utilizó la técnica cualitativa de la entrevista, específicamente un formato de entrevista estructurada, esta tipología de entrevista se basa en seguir un guion de preguntas y realizarle las mismas preguntas a todos los entrevistados, siguiendo el mismo orden y formulación (Universidad de Castilla-La Mancha, 2021). Se utiliza esta técnica ya que, previamente, se ha realizado una revisión de literatura que ha permitido obtener conocimientos adecuados, por esto, se realiza la entrevista con el propósito de obtener información de primera mano de profesionales en el ámbito para poder analizar la perspectiva de estos, con su experiencia, conocimiento y opinión, permitiendo que se pueda responder la pregunta de investigación planteada.

Para realizar esta fase de la investigación se siguió un guion compuesto por 12 ítems (Anexo 1) que abordan distintos puntos como son los desafíos del uso de la Inteligencia Artificial en la ciberseguridad, el futuro del uso de la herramienta en este ámbito, el rol del criminólogo en relación

con el ámbito de seguridad cibernética, entre otros. Se contactó con 7 participantes los cuales trabajan en distintos países, todos con experiencia en el ámbito de la ciberseguridad (Tabla 2).

Esta muestra se consiguió por medio de un muestreo no probabilístico por conveniencia, ya que se conocía a los profesionales y se consideró el más adecuado a realizar. Se decidió realizar entrevistas a expertos en la materia ya que, por sus años de experiencia, pueden ser capaces de proporcionar una visión completa hacia la temática del presente trabajo de investigación.

De la misma manera, resulta importante mencionar el puesto profesional de cada entrevistado para analizar sus respuestas teniendo en cuenta su experiencia y trayectoria profesional. Entre los entrevistados se encuentran individuos que trabajan en sector público como es el Mayor General de la República Bolivariana de Venezuela y un profesor universitario en materia de ciberseguridad, estos proporcionan una visión integral sobre la materia. También, se encuentran individuos que trabajan en empresas privadas, quienes proporcionan una perspectiva actualizada sobre la defensa contra las amenazas cibernéticas.

Las entrevistas se realizaron durante los meses de febrero a mayo, por medio de videoconferencias en distintas plataformas (Zoom, Teams y Discord), debido a que los participantes se encontraban fuera del país o resultaba complicado ejecutar la entrevista de manera presencial. Dichas entrevistas se han grabado con el objetivo de realizar transcripciones posteriores.

Tabla 2.

Datos de la muestra investigada.

Muestra	**Género**	**Puesto Profesional**	**Transcripción correspondiente**
E1	Masculino	Oficial con el Grado de Mayor General de la República Bolivariana de Venezuela.	Anexo 2
E2	Femenino	Gerente en el departamento de ciberseguridad.	Anexo 3
E3	Masculino	Presidente de la empresa de Ingeniería de Ciberseguridad E4P Inc.	Anexo 4

E4	Masculino	Analista senior para una empresa de consultoría.	Anexo 5
E5	Masculino	Docente universitario con línea de investigación en la ciberespacio.	Anexo 6
E6	Masculino	Líder técnico del área de nuevas tecnologías en la empresa ETRA.	Anexo 7
E7	Femenino	Senior Compliance officer	Anexo 8

Fuente: Elaboración propia.

3.2. Consideraciones Éticas

Todos los participantes de esta investigación fueron informados del proceso y recibieron un consentimiento informado en el cual se plantea el propósito de la investigación, procedimiento a seguir y el derecho a retirarse en cualquier momento de la investigación sin ninguna consecuencia (Anexo 9). Dicho consentimiento ha sido firmado por todos los participantes.

3.3. Limitaciones del estudio

Es importante resaltar que la muestra de este estudio no es representativa, ya que solamente 7 individuos fueron entrevistados. Sin embargo, cabe destacar que los sujetos entrevistados tienen experiencia amplia y significativa sobre esta temática abordada, lo cual proporciona una visión profunda y detallada que puede aportar información valiosa a la investigación.

4 ANÁLISIS DE RESULTADOS

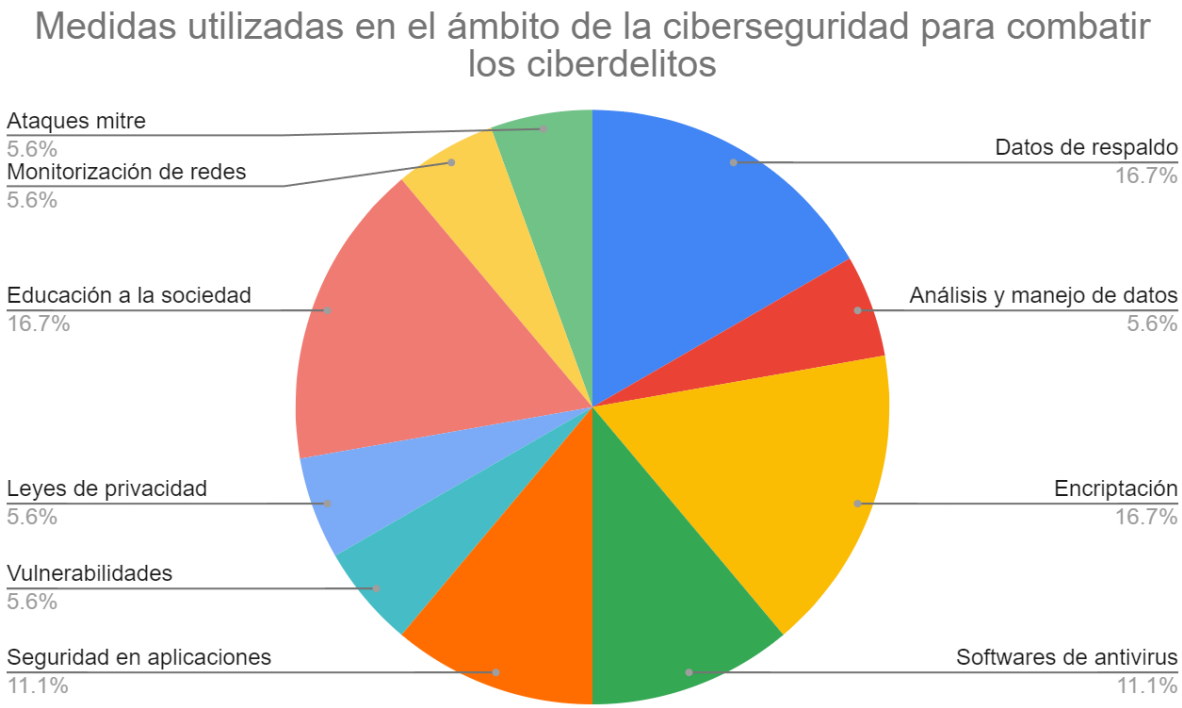
Una vez recogidas las muestras de las entrevistas y estudiado el fundamento jurídico y teórico, se procede a realizar el análisis de resultados de dichas entrevistas. Para ello, se clasificaron los resultados en cuatro categorías: (1) medidas utilizadas en la ciberseguridad para combatir los ciberdelitos; (2) uso de la Inteligencia Artificial en el ámbito de ciberseguridad; (3) aspectos éticos de la Inteligencia Artificial como herramienta de prevención y lucha contra los ciberdelitos, y (4) rol del criminólogo en el ámbito de ciberseguridad.

4.1. Medidas utilizadas en el ámbito de ciberseguridad para combatir los ciberdelitos.

Para poder analizar la temática de este trabajo de investigación, es necesario resaltar las medidas utilizadas por los profesionales para poder así tener una visión de las técnicas presentes en el ámbito de la ciberseguridad. Por esta razón, se consideró adecuado empezar la investigación con esta categoría, ya que permite así una contextualización actual de la temática. Se le preguntó a los profesionales entrevistados si podrían proporcionar una descripción general de las medidas de ciberseguridad utilizadas para combatir los ciberdelitos. A lo cual, los entrevistados dieron una visión completa sobre estas (Figura 6).

Figura 6.

Medidas utilizadas en el ámbito de ciberseguridad para combatir los ciberdelitos.



Fuente: Elaboración propia, con base en las respuestas de los entrevistados.

Se mencionó el análisis y manejo de datos con las protecciones adecuadas, para lo cual se utiliza mayormente la encriptación, que, como bien se ha estudiado en el marco teórico, permite proteger los datos y evitar que estos sean atacados y accedidos por agentes malignos. Dos de los

entrevistados mencionaron la encriptación como la medida mayormente utilizada, ya que permite la protección de estos datos. Uno de los entrevistados, explica el proceso de encriptación como:

> Poner datos conocidos allí [en el sistema] antes de que se encripten, y una vez que se encripta, recuperas esos datos conocidos, y puedes aplicar ingeniería inversa a esos datos para obtener la clave. Una vez que tienes la clave, entonces puedes obtener el resto de [los datos] también (E3, comunicación personal, 2024).

Como se ha estudiado anteriormente, los datos y el flujo de estos es de relevante importancia para la temática de la ciberseguridad, por esto, se mencionan los datos de respaldo como otra medida de relevante importancia a la hora de combatir los ciberdelitos. Los datos de respaldo, o *backup data*, permiten un nivel adicional de protección frente a delitos como el ransomware, al igual que, permite que estos sean restaurados en caso de pérdidas, robos o daños (Min et al., 2022; Ramesh et al., 2023).

"El Internet nunca fue un lugar seguro" (E3, comunicación personal, 2024), comenta uno de los entrevistados, haciendo hincapié en cómo el espacio cibernético ha sufrido de ataques a su seguridad desde que ha sido creado, ya que facilita el acceso a todo tipo de agentes. Para evitar poder crear medidas de prevención en este espacio, se utilizan los sistemas de antivirus. Esta medida es una de las más comunes utilizada por los usuarios habituales, para proteger sus dispositivos de ataques de malware (Pérez-Sánchez & Palacios, 2022).

Los sistemas de antivirus están dirigidos a crear mayor protección de la que ofrecen los sistemas operativos, siendo estos una medida preventiva, sin embargo, en ocasiones pueden ser utilizadas como medidas de ataques en donde se encargan de eliminar la infección del sistema para que este vuelva a su funcionamiento habitual (Koret & Bachaalany, 2013).

Otra medida importante en el ámbito de la ciberseguridad, la cual dos de los entrevistados mencionaron, es la seguridad en aplicaciones. El espacio cibernético ha permitido que muchos actores creen sus propias aplicaciones y que estas sean disponibles para todos los usuarios, siendo una parte vital de la vida de muchos individuos. La seguridad y la privacidad son dos de las principales preocupaciones que los individuos presentan a la hora de desarrollar y utilizar estas

aplicaciones. Sin embargo, la seguridad de estas es un proceso complejo que, en ocasiones, va más allá de los métodos tradicionales de seguridad de red (Mutchler et al., 2015).

La búsqueda o evaluación de vulnerabilidades también es otro factor de relevante importancia a la hora de combatir actuaciones de los ciber agresores. La evaluación de vulnerabilidad se realiza utilizando conocimientos adquiridos a base de las respuestas a accidentes previos. Esta evaluación posee la tendencia a ser un proceso subjetivo el cual requiere una estrategia analítica y una metodología de sistemas potente (Upadhyay & Sampalli, 2020). Uno de los entrevistados (E5) menciona la importancia de la monitorización constante de las redes para así identificar vulnerabilidades y posibles ataques que se realicen al sistema.

Uno de los entrevistados comenta cómo "una de las mayores vulnerabilidades es el hecho de que la gente, como los malos actores, en este momento están entrando mediante el uso de esquemas de correo electrónico y mediante el uso de clic en enlaces" (E3, comunicación personal, 2024). Explicando cómo uno de los mayores desafíos a los que se enfrentan los profesionales de la ciberseguridad es la vulnerabilidad humana y cómo estos suelen demostrar comportamientos de riesgo sin tomarlo en consideración, por esta razón, la exploración y evaluación de vulnerabilidades es de real importancia.

Al igual que se mencionan dos aspectos con una connotación menos técnica sobre la temática, estos siendo las leyes de privacidad y la educación a la sociedad y a los empleados. En cuanto a las leyes de privacidad, como se ha estudiado previamente, son de relevante importancia y están en constante actualización para adaptarse a los cambios que esta creciente tecnología trae. Por otro lado, la educación a la sociedad sobre esta temática es un aspecto fundamental, ya que permite informar a los miembros de la sociedad sobre los peligros a los cuales se pueden enfrentar en el espacio cibernético.

Por último, otro entrevistado (E6) hace referencia al uso de *Ataques Mitre*, los cuales "identifican las mecánicas o técnicas que utiliza el que ataca… para llevar a cabo su propósito" (E6, comunicación personal, 2024). Esta técnica permite simular ataques para así probar los mecanismos de defensas del sistema, al igual que permite identificar cuales técnicas de seguridad se adaptan de mejor manera a la prevención y detección de ciber amenazas (IBM Security, 2023b).

4.2. Uso de la Inteligencia Artificial en el ámbito de la ciberseguridad

Los ciberdelitos han crecido de manera exponencial, llegando a causar grandes problemas a nivel social y en los profesionales de la ciberseguridad. Por esta razón, se deben tomar medidas efectivas que permitan proteger la integridad de los sujetos y la información (Sarker, 2021). La tecnología ha sido una herramienta que ha ayudado positivamente a estos profesionales, pero, de la misma manera ha creado nuevas oportunidades para los ciberdelincuentes.

Una de las herramientas tecnológicas que ha sido utilizada en el ámbito de la ciberseguridad es la Inteligencia Artificial, mayormente en la automatización de funciones que permitan defender los sistemas. Anteriormente, se explicó cómo se utiliza esta herramienta en distintas técnicas como el análisis de datos y detección de patrones.

Para obtener una visión más completa, se le preguntó a los entrevistados que técnicas de la Inteligencia Artificial son utilizadas en el ámbito de la ciberseguridad en temática de prevención y detección de amenazas cibernéticas. A lo cual los profesionales proporcionaron una visión más específica, explicando cómo esta se puede utilizar para la criptografía, es importante resaltar que la criptografía implica la encriptación y desencriptación de la información, como ya se ha explicado anteriormente.

El uso de la Inteligencia Artificial en relación a la criptografía, ya que esta se basa en la conversión de texto normal en uno cifrado, el texto cifrado es una representación aleatoria y compleja del texto normal, aquí, la Inteligencia Artificial es de gran relevancia ya que permite automatizar este proceso generando cifrados que permitan la protección de la información. Permite reconocer patrones complejos de cifrado (Blackledge & Mosola, 2020).

Tres de los entrevistados (E1, E2 y E6), comentaron que, en cuanto al uso de la Inteligencia Artificial en la prevención de ciberdelitos destaca la importancia del monitoreo proactivo y la detección eficiente de amenazas que se experimentan. Este enfoque preventivo se alinea con las necesidades actuales que el mundo cibernético experimenta en relación a la seguridad, donde la capacidad de anticiparse a los ataques y responder de manera eficaz es fundamental para poder crear una protección sobre los datos y la privacidad de los usuarios.

La Inteligencia Artificial es una herramienta poderosa para el monitoreo preventivo de estas amenazas, ya que permite automatizar los procesos a base de aprendizaje continuo. Esto se ha estudiado anteriormente, cuando se menciona el aprendizaje automático, ya que esto permite identificar patrones en base a ataques previos. Al igual que, la Inteligencia Artificial es capaz de analizar grandes volúmenes de información, permitiendo identificar patrones sospechosos o anormales detectando así amenazas. La detección temprana de amenazas permitirá a los profesionales tomar medidas adecuadas para minimizar los riesgos y evitar posibles ataques antes de que estos causen un daño significativo.

De la misma manera el entrevistado E1 comenta sobre la importancia de esta herramienta en cuanto a la protección de la nube, haciendo énfasis en cómo aquí se concentra toda la información y es donde mayor riesgo se puede detectar. La tecnología de la nube o *cloud technology* hace referencia a un modelo que permite el acceso a los usuarios de manera cómoda y remota, al igual que se forma de un conjunto de recursos informáticos configurables de acceso rápido (Birje et al., 2015).

Esta tecnología posee múltiples beneficios por su fácil acceso y libertad proporcionada a los usuarios, sin embargo, tiene a su vez, múltiples debilidades como la pérdida de datos, poco control sobre el proceso, ataques al sistema, entre otros (Birje et al., 2015). Aquí resalta la necesidad de crear técnicas eficaces que permitan la prevención de ataques a la nube

Por otro lado, otro entrevistado (E4) comentó que se utiliza la Inteligencia Artificial en un sistema llamado *Attack IQ*, este sistema emula un ataque con el objetivo de poner a prueba la seguridad del sistema, generando así datos que permitan mejorar su seguridad. Para esto, se utilizan datos que vienen de emulaciones automatizadas de adversarios para así ayudar a mejorar las capacidades de defensas de las empresas (AttackIQ, 2024).

Otro de los entrevistados (E5) hace referencia a la uso de Machine Learning para “identificar patrones y anomalías indicativas de actividad maliciosa en tiempo real” (E5, comunicación personal, 2024). Este entrevistado comenta la importancia de combinar el conocimiento humano con las técnicas que la Inteligencia Artificial posee para así poder detectar y responder de manera más eficaz a las amenazas presentadas en el mundo digital.

La Inteligencia Artificial permite la detección de anomalías, prevención del fraude y análisis de riesgo. A medida que la tecnología avanza, las técnicas de seguridad han de fortalecer y adaptarse a estos cambios (Reddy, 2023).

De igual forma, se le preguntó a los profesionales de qué maneras se utiliza la Inteligencia Artificial para reducir el impacto de los ciberataques, sus respuestas se relacionan con las anteriores comentando que se utiliza para "automatizar los procesos y técnicas ya utilizadas" (E3, comunicación personal, 2024). Es decir, se utiliza la Inteligencia Artificial para mejorar estas técnicas, ayudando así a los profesionales a mejorar la seguridad de los sistemas y los usuarios.

Otro de los entrevistados (E1) mencionó cómo esta herramienta permite identificar los ataques cibernéticos, dando lugar a que se desarrollen técnicas específicas para combatir estos delitos. La identificación se realiza en base a patrones y datos previos obtenidos, el uso de la Inteligencia Artificial puede reducir el esfuerzo de los profesionales permitiendo así que se analicen grandes cantidades de datos para extraer así los patrones de la criminalidad, la identificación de estos, y permitiendo que los profesionales estén preparados a los ataques (Dakalbab et al., 2022).

De igual manera, uno de los entrevistados (E3) menciona cómo el uso de la Inteligencia Artificial, permite incorporar el desarrollo tecnológico en las técnicas ya utilizadas, como se ha mencionado anteriormente, la tecnología se encuentra en constante crecimiento, por lo cual es necesario crear medidas que se adapten adecuadamente a estos cambios.

Muchos de los profesionales comentaron que la Inteligencia Artificial se utiliza mayormente para "mejorar las técnicas que se están utilizando ahora" (E3, comunicación personal, 2024), permitiendo que estos procesos se mejoren y se adapten a las necesidades de la sociedad. Igualmente, se puede enfocar esta herramienta para el desarrollo de habilidades que vayan al mismo tiempo que el desarrollo de la Inteligencia Artificial, ya que, como menciona uno de los entrevistados "existe una desconexión debido al avance muy rápido de la Inteligencia Artificial" (E2, comunicación personal, 2024).

Como se ha estudiado anteriormente, el desarrollo de la Inteligencia Artificial ha aumentado exponencialmente en las últimas décadas, con un crecimiento relevante en los últimos años. Resulta necesaria la adaptación a este desarrollo, ya que, como bien ha mencionado uno de los

entrevistados, los agentes malignos tienen el mismo acceso a estas herramientas por lo cual se convierte en un arma de doble filo. Por esta razón, resulta fundamental que los profesionales mantengan técnicas actualizadas que se adapten a las necesidad de seguridad que los usuarios experimentan.

Uno de los entrevistados comenta que la Inteligencia Artificial ha de tener un canal que "permita el ingreso de toda la información posible en el ciberespacio" (E1, comunicación personal, 2024), sin embargo, este canal ha de contar con un sistema que permita la veracidad y confiabilidad de la información. El entrevistado comenta que se ha de crear un "corpus confiable en el algoritmo" (E1, comunicación personal, 2024), el *corpus* hace referencia al conjunto de datos científicos o literarios que se encuentran de manera ordenada y pueden servir como base a una investigación (RAE, 2024). En este contexto, se menciona el uso de información válida en el algoritmo de la Inteligencia Artificial para crear recursos viables que los profesionales puedan utilizar.

Este entrevistado también comenta cómo se han de "incorporar todas las técnicas y procedimientos para evitar amenazas al sistema" (E1, comunicación personal, 2024). Lo cual, como han mencionado anteriormente los otros entrevistados, hace referencia a la mejora de las técnicas ya utilizadas, dando así paso a crear procedimientos eficaces que permitan prevenir las amenazas cibernéticas a los usuarios.

La Inteligencia Artificial es una herramienta que permite potenciar las técnicas ya utilizadas en la ciberseguridad, haciendo así que se tomen respuestas ágiles a los incidentes que ocurren. Esta herramienta permite "optimizar la identificación de riesgos … [y] fortalecer la capacidad de respuesta ante amenazas" (E5, comunicación personal, 2024).

De la misma manera, resalta el uso de la Inteligencia Artificial en la identificación de patrones, ya que es una herramienta que permite identificar aquello que "los ojos humanos no pueden ver" (E4, comunicación personal, 2024). Permitiendo, de este mismo modo, un seguimiento más fácil sobre lo que ocurre en el mundo digital, ya que en ocasiones el rápido desarrollo de este ámbito complica el seguimiento por parte de los profesionales de la ciberseguridad. La Inteligencia Artificial presenta un papel fundamental en la vigilancia y alerta de posibles amenazas, permitiendo así que los profesionales ahorren tiempo valioso en relación a los ataques (E7).

Al ser una herramienta tan compleja, se le preguntó a los entrevistados a que desafíos consideran que los profesionales de la ciberseguridad se enfrentarán con el uso de la Inteligencia Artificial. A lo cual se comentó que uno de los mayores desafíos será la falta de entrenamiento (E2 y E5) y de actualidad (E4), ya que al estar creciendo a diario, nueva información se adhiere y causa que los profesionales deban estar constantemente actualizados sobre las posibles amenazas. Otro entrevistado (E1), comenta qué detectar amenazas sin afectar la velocidad y universalidad del sistema será un gran desafío que los profesionales experimentarán.

Sin embargo, dos de los entrevistados (E5 y E6) mencionan qué el mayor desafío será la necesidad de datos de calidad de ataques previos, para poder entrenar los modelos de Inteligencia Artificial, al igual que será un desafío la interpretación, ética de su uso y la necesidad de estar constantemente actualizando los datos. A su vez, se menciona como será un desafío (E7) encontrar un equilibrio entre la precisión y los falsos positivos.

La Inteligencia Artificial, al ser una herramienta que ha cobrado mayor poder y relevancia en los últimos años en la temática de la seguridad, exige un entrenamiento importante a los profesionales que han de usarla. Por esta razón, se le preguntó a los entrevistados qué habilidades consideran que los profesionales han de tener para poder aprovechar el uso de herramientas como la Inteligencia Artificial. Sus respuestas se pueden clasificar en las siguientes categorías: (1) Habilidades técnicas, (2) Habilidades académicas, (3) Habilidades comunicativas y (4) Habilidades sociales (Tabla 3).

Las habilidades técnicas hacen referencia a aquellas específicas del contexto de ciberseguridad. En este caso los profesionales hacen referencia a que los individuos tengan la información adecuada, entendiendo la tecnología en todos sus aspectos, incluyendo la tecnología de la nube, que, se ha vuelto una temática popular en el ámbito de la ciberseguridad. Al igual, que se incluye técnicas como el control el acceso a los datos sensibles y los individuos que han de tener ese acceso; el entendimiento de la seguridad móvil, la cual hace referencia a la ausencia de peligro o riesgos mediante el uso de ordenadores móviles y dispositivos de comunicación (IBM Security, 2024c).

Tabla 3

Habilidades que los profesionales han de tener para aprovechar el uso de la Inteligencia Artificial.

Habilidades Técnicas	Habilidades Académicas	Habilidades Comunicativas	Habilidades Sociales
Seguridad móvil. Computación en la nube. Información adecuada. Entender la tecnología. Identificar y gestionar el acceso a datos sensibles. Educación, entrenamiento e investigación. Entender sobre el Machine Learning. Revisar los foros de hackers. Programación.	Teoría de Sistemas. Psicología del comportamiento. Razonamiento matemático, lógico y complejo. Conocimientos de seguridad y defensa. Lógica predictiva. Conocimiento de ingeniería electrónica, telecomunicación y computación. Comprender los fundamentos de la Inteligencia Artificial. Resolución de problemas.	Etiqueta adecuada de comunicación. Escritura de negocios. Buenos dotes de comunicación.	Establecer relaciones. Resolución de conflictos. Buen servicio al cliente. Amabilidad. Diplomacia. Trabajo y gestión de equipos. Entendimiento del comportamiento social.

Fuente: Elaboración propia, con base en las respuestas de los entrevistados.

Dentro de estas habilidades, también, resalta el entrenamiento, educación e investigación constante por parte de los profesionales en materia de la Inteligencia Artificial, para así estar al día de todos los cambios que esta herramienta posee. El entrenamiento constante permite a los profesionales estar al tanto del crecimiento de la Inteligencia Artificial, para así tomar medidas adecuadas sobre la prevención y actuación de estos ciberdelitos. También se menciona el entendimiento de los foros de hackers, ya que en estos se mencionan estrategias que utilizan los hackers para poder desarrollar formas de ataque nuevas, al igual que resalta la necesidad de conocer los lenguajes de programación como Python y Java.

Por otro lado, las habilidades académicas hacen referencia a los conocimientos que permitirán a los profesionales aprovechar el uso de la Inteligencia Artificial de la mejor manera posible. Aquí los entrevistados hicieron referencia a habilidades como el razonamiento matemático, lógico y complejo. Este tipo de razonamiento permite a los profesionales analizar, comprender y resolver problemáticas complejas de manera adecuada, promoviendo una visión amplia y adecuada a estos. De la misma manera, los entrevistados comentaron que los profesionales han de tener conocimientos generales de seguridad y defensa, ya que, estos han de entender cómo se desarrolla la criminalidad y qué medidas existen para combatirla. Al igual que han de conocer sobre la psicología del comportamiento, lógica predictiva o lógica de primer orden y teoría de sistemas, para así poder tener los recursos necesarios a la hora de enfrentar los ciberdelitos.

Por otra parte, los profesionales han de tener habilidades comunicativas, como buenos dotes de comunicación, escritura de negocios, y seguir la etiqueta adecuada de comunicación, lo cual hace énfasis a la escucha activa, el respeto entre comunicadores, claridad en la habla, y empatía. De la misma manera, han de tener habilidades sociales como la amabilidad, diplomacia, buen servicio al cliente, resolución de conflictos, trabajo y gestión de equipos, y establecer relaciones.

La capacidad de desarrollar y perfeccionar estas habilidades ya mencionadas permite a los expertos tener una visión integral y sólida en su desarrollo profesional. Estas no solamente facilitan la interacción y colaboración entre compañeros de trabajo, sino que también promueven una comprensión más profunda del contexto de los ciberdelitos, resaltando la necesidad y perspectiva de los usuarios víctimas o potenciales víctimas. En el contexto de la Inteligencia Artificial, donde la tecnología se encuentra en constante crecimiento y causando posibles problemáticas éticas y

sociales, estas habilidades resultan necesarias ya que, como los entrevistados han mencionado, la ciberseguridad es un mundo donde los profesionales han de estar en constante comunicación con su equipo, poseer buenas habilidades comunicativas les permitirá a los profesionales ser capaces de explicar las amenazas que el sistema posee para así combatirlas de la manera más eficiente posible.

La Inteligencia Artificial, al ser una herramienta con un gran potencial, puede suponer tanto beneficios como problemas en este ámbito. Se le preguntó a los entrevistados cuál creían que sería el papel de esta herramienta en el futuro en cuanto a la lucha contra los ciberdelitos. Uno de los entrevistados reiteró que "será un arma de doble filo" (E4, comunicación personal, 2024), ya que podrá ser una herramienta de gran beneficio para los profesionales, pero, a su vez podrá ser utilizada por los agentes malignos. La Inteligencia Artificial permite que los profesionales de la ciberseguridad sean capaces de mejorar las técnicas que ya poseen (E3), mejorar la prevención y detección de amenazas (E1 y E5). Sin embargo, sigue siendo una herramienta que se encuentra en desarrollo por lo cual es importante tener cuidado en su uso y el posible uso que los agentes malignos le den.

4.3. Aspectos éticos que rodean la Inteligencia Artificial como herramienta de prevención y lucha contra los ciberdelitos

La Inteligencia Artificial ha sido una herramienta que ha proporcionado grandes beneficios y oportunidades para ámbitos como el financiero, de salud y sobre todo en el ámbito tecnológico, siendo de suma importancia para este. Sin embargo, esta es una herramienta que puede causar daños potenciales si no es utilizada con cuidado (Faiza et al., 2022). Uno de los entrevistados califica esta herramienta como "un arma de doble filo" (E3, comunicación personal, 2024), ya que puede ser de gran utilidad, pero, esta también está disponible para agentes malignos que buscan utilizarla para facilitar el proceso de ataque a los sistemas.

Se le pregunta a los entrevistados si consideran que el uso de la Inteligencia Artificial en su ámbito traerá consecuencias éticas, específicamente en términos de privacidad y protección de datos, a la cual, todos mencionaron creer que sí. Se explicó cómo se considera que la llegada de la Inteligencia Artificial en la ciberseguridad traerá consigo muchos problemas éticos, uno de los

entrevistados comenta como esto es una consecuencia de la falta de barreras que los usuarios y desarrolladores de la Inteligencia Artificial ponen.

Otro entrevistado hace referencia a las leyes de privacidad, mencionando que estas "quedarán en un marco obsoleto con respecto a la Inteligencia Artificial" (E2, comunicación personal, 2024). Lo cual resalta que será necesario actualizar las regulaciones actuales para poder abordar los desafíos que esta herramienta presenta. De la misma manera, otro de los entrevistados comenta cómo estas medidas y uso de esta herramienta "deben regularse de manera estricta" (E1, comunicación personal, 2024). Sin embargo, como se ha estudiado previamente, distintas instituciones han tomado medidas para regular esta herramienta de la manera adecuada, aunque, por su constante evolución, estas medidas han de ajustarse a estos cambios, ya que se presentarán grandes problemáticas.

De la misma manera, este entrevistado comenta cómo no únicamente se verá afectada éticamente la transferencia de datos, sino que "es algo más complejo, [como] es el uso de robots para producir información" (E2, comunicación personal, 2024). Los robots de Inteligencia Artificial son máquinas con sistemas semiautónomos que tienen la capacidad de realizar acciones y tomar decisiones con la colaboración humana. Aunque los robots con programas de Inteligencia Artificial han sido de gran ayuda para la sociedad, estos también han causado problemáticas sociales y éticas, como bien menciona el entrevistado (Tóth et al., 2022).

El entrevistado E5 menciona como será necesario revisar las políticas de privacidad para garantizar la transparencia en la toma de decisiones de la Inteligencia Artificial. De la misma manera, el entrevistado E6 hace referencia a los posibles sesgos que esta herramienta tome en cuanto al análisis de datos.

4.4. Rol del criminólogo en el ámbito de ciberseguridad

En el mundo digital, los ciberdelitos se han convertido en una de las mayores amenazas para los usuarios, en este caso, el rol del criminólogo se ha convertido en uno fundamental dentro de la ciberseguridad, ya que le permite entender y prevenir estos delitos. Recordemos que la criminología se define como una ciencia que "se ocupa del delito, delincuente, la víctima y el

control social del comportamiento delictivo" (García-Pablos de Molina, 1989), siendo esta vital para el desarrollo de estrategias eficaces de prevención de los delitos.

La ciberseguridad ha sido un problema social cada vez mayor, en donde la criminología tiene gran presencia, específicamente en la investigación de delitos en el ámbito cibernético, al igual que, en la creación de políticas de respuesta efectivas. De la misma manera, la criminología permite entender de mejor manera los factores de comportamiento de los ciber agresores Esta ciencia, al combinarse con la ciberseguridad, se posiciona como prioridad de la prevención de delitos digitales, especialmente con el uso de la Inteligencia Artificial (Dupont & Whelan, 2021).

A lo cual uno de los entrevistados comenta que este rol será esencial "siempre y cuando las universidades comiencen a preparar a los profesionales en esta dirección" (E2, comunicación personal, 2024). Esta observación destaca un punto crítico, que el entrevistado también menciona, siendo este la necesidad de una evolución educativa que permita a los criminólogos enfrentar y anticipar las nuevas modalidades criminales que emergen con el avance tecnológico.

En el contexto actual digital, la desinformación y propagación de noticias falsas puede afectar la seguridad social en gran manera, aquí, se podría considerar cómo el papel del criminólogo se vuelve más importante en el ámbito de la ciberseguridad. Uno de los entrevistados resaltó la importancia de estos profesionales en la lucha contra el mal uso de las tecnologías. Este entrevistado, resalta la importancia del criminólogo para identificar los efectos de este mal uso y difusión de *Fake News.* Los profesionales criminólogos están capacitados para comprender los procesos sociales que rodean la propagación de la desinformación, al igual que poseen todas las habilidades necesarias para crear planes preventivos.

Lo mismo ocurre con los *Deepfakes,* los cuales son imágenes manipuladas por medio de la Inteligencia Artificial de personas, en las cuales se pueden realizar declaraciones que nunca se han dicho originalmente, haciendo creer que sí, culpabilizando así a la persona (Instituto Nacional de Ciberseguridad, s. f.). Uno de los entrevistados (E4, comunicación personal, 2024) comenta como los profesionales de la criminología podrán ser capaces de aportar una perspectiva que permita identificar cuándo se trata de un *Deepfakes* y cuándo es realmente la persona.

Por otro lado, dos de los entrevistados (E1 y E5) resaltaron la importancia de la criminología en la creación de planes de prevención de ciberdelitos. Los criminólogos poseen una visión única que les permite comprender los patrones y factores delictivos, lo cual se podrá aplicar al ámbito digital. Al realizar planes preventivos de ciberdelitos, los criminólogos serán capaces de identificar áreas de vulnerabilidad, factores de riesgos y de protección, contribuyendo así a poder sensibilizar y proteger a la población. Estos planes podrán ser automatizados por medio de la Inteligencia Artificial, en cuanto al análisis de datos, predicciones de riesgo y desarrollo de estrategias.

5 CASOS PRÁCTICOS

Los ciberdelitos presentan cada vez una amenaza mayor para la sociedad, causando miedo y problemáticas sociales, por esta razón se considera apropiado mencionar casos recientes en el ámbito de la ciberseguridad y las acciones tomadas por los expertos en estas áreas para así tener una visión global y actual de la temática estudiada. En primer lugar, se menciona el caso de hackeo de *MGM Resorts*, los cuales se llevaron a cabo en septiembre de 2023 por un grupo de hackers de edades comprendidas entre los 19 y los 22 años, llamado *Scatter Spider* (Sanuy, 2023).

Este grupo paralizó los sistemas informáticos de la cadena hotelera *MGM Resorts* y casinos en la ciudad de Las Vegas (EEUU), causando que se cerraran los casinos y que los clientes de los hoteles no pudieran utilizar las tarjetas para tener acceso a sus habitaciones. De la misma manera, este grupo de cibercriminales impidió el acceso a los empleados a sus correos electrónicos (Collier, 2023).

Este ciberataque causó que la empresa hotelera sufriera una pérdida de 100 millones de dólares. Estos ataques tuvieron como consecuencia un robo de los datos privados de los clientes, incluyendo: nombres, número de pasaporte, número de carné de conducir, número de seguridad social, teléfonos móvil, fechas de nacimientos y direcciones postales (MGM Resorts, 2023). Este mismo grupo de cibercriminales realizó el mismo ataque en la cadena de casinos *Caesars Entertainment.* En ambos casos, se determina el ataque como un *Ransomware*, que consiste en que, como se ha estudiado previamente, el agresor impide al usuario el acceso a su dispositivo, y, estos exigen un pago para que se pueda acceder a los datos nuevamente.

Para estos casos se tomaron medidas de actuación distintas. Por un lado *Caesars Entertainment* decidió pagar 15 millones de dólares para poder recuperar los datos (Schappert, 2023b). Mientras que la empresa hotelera *MGM Resorts* decidió tomar una respuesta distinta, cerrando los sistemas e iniciando una investigación (MGM Resorts, 2023). Sin embargo, no se han aportado nuevas actualizaciones sobre dicha investigación.

Se ha mencionado que este ataque ocurrió cuando el grupo *Scatter Spider* llamó al servicio de asistencia informática de *MGM Resorts* utilizando el nombre de uno de los empleados que encontraron en la plataforma *LinkedIn*. Los miembros fueron capaces de convencer a los operadores de informáticos para cambiar la contraseña del sistema, dándoles así el acceso a este (Schappert, 2023a).

Lo ocurrido en este caso es lo que los profesionales denominan un *ataque de ingeniería social*, el cual hace referencia a la manipulación o engaño por parte del agresor hacia la víctima, para que ésta revele información crítica (Syafitri et al., 2022). La ingeniería social, busca obtener información sensible con el propósito de ser vendida o utilizada con un fin específico, como ocurre en el caso de Las Vegas, siendo este uno de los mayores riesgos que se presentan en el ámbito ya que el factor humano es difícil de controlar (Salahdine & Kaabouch, 2019).

En este caso, el robo de los datos se causa por fallos de los profesionales, por lo cual, basado en la información recolectada por los expertos, esto demuestra que se ha de entrenar a los profesionales para evitar su susceptibilidad. Se podría utilizar la Inteligencia Artificial para minimizar estos fallos, aplicando medidas preventivas que protejan la seguridad de la empresa. En este caso, se podrá crear un sistema que permita la recuperación de contraseñas por medio de una doble autenticación, lo que permite verificar que el solicitante es realmente quien dice ser. La Inteligencia Artificial podrá realizar este proceso, proporcionando los datos de la doble autenticación, creando patrones alfanuméricos aleatorios que el sujeto ha de proporcionar en el sistema para así poder recuperar sus datos. Esto permitirá tener un proceso más seguro para evitar que los agentes malignos exploten las vulnerabilidades del sistema para realizar sus ataques.

Otro caso relevante a mencionar es el reciente hackeo a Microsoft Azure, una plataforma de tecnología en la nube, que permite a los usuarios administrar o crear aplicaciones (Microsoft Azure, 2024). Sin embargo, en materia de ciberseguridad esta aplicación ha causado grandes

problemáticas, revelando una *vulnerabilidad de día cero*, el cual hace referencia a los ataques que se realizan aprovechando fallos desconocidos en el sistema, ya bien sea de software, hardware o firmware. Su nombre *día cero*, hace referencia a que los profesionales tienen cero días para poder solucionar el fallo (IBM Security, 2024a; Mudaliar, 2024).

Esta vulnerabilidad causó que cientos de cuentas ejecutivas fueran comprometidas a una pérdida de datos por medio del phishing y hacking de las cuentas. Este ciberataque incluía la suplantación de identidad de los usuarios, extracción de datos privados y el fraude financiero. Estas brechas de seguridad suelen ser cada vez más comunes en empresas tecnológicas, por lo cual han de crearse medidas eficaces que protejan a los usuarios de daños como estos (Mudaliar, 2024).

El ataque de Microsoft Azure ocurre por un error de validación en el código principal que causó que los tokens de Azure pudieran ser falsificados por actores malignos. Este ataque afectó a 25 organizaciones, incluyendo entidades gubernamentales. Se obtuvo acceso no autorizado a los correos electrónicos y datos de los usuarios, filtrándose datos privados de estos (The Hacker News, 2023).

Como se ha estudiado anteriormente, los expertos comentaron la importancia de explorar las vulnerabilidades que el sistema puede tener, para así crear soluciones rápidas y eficaces. Cuando se mencionan este tipo de vulnerabilidades de día cero, presentan una gran consecuencia en la seguridad de los usuarios. Este tipo de errores se pueden minimizar con el uso de herramientas de Inteligencia Artificial, ya que éstas podrán realizar controles de vulnerabilidades preventivos de manera automática, identificando los posibles puntos de acceso de los agresores sobre el sistema para así poder solventarlos antes de que el programa sea público.

6 CONCLUSIONES

La tecnología es un área que se encuentra en constante crecimiento, que permite a sus usuarios realizar procedimientos de manera más eficaz. Sin embargo, de la misma manera, ha permitido a los agentes malignos ser capaces de utilizarla para cometer delitos. Por esta razón, el campo de la ciberseguridad ha de estar en constante evolución y actualización, ya que se enfrenta a delitos cada vez más diversos y sofisticados.

A lo largo del presente trabajo se ha estudiado e investigado el relevante papel de la Inteligencia Artificial en relación a la prevención y lucha contra los ciberdelitos. El foco principal del estudio ha sido investigar y analizar las distintas funciones que la Inteligencia Artificial podrá tener en la prevención de los ciberdelitos, al igual que su uso a la hora de luchar contra ellos. Durante el estudio de la temática se observó cómo la Inteligencia Artificial es una herramienta basada en el entrenamiento de datos que permiten analizar y crear respuestas adecuadas a la situación presentada. Sin embargo existen varias problemáticas sobre el uso de la Inteligencia Artificial y la privacidad de datos. Para tratar de dar solución a estos problemas varios países alrededor del mundo han creado un marco jurídico para así proteger a los ciudadanos de posibles ataques causados por esta.

Aunque ningún país ha formalizado una regulación sobre esta temática, la Unión Europea ha sido la primera organización internacional en aprobar su regulación *AI Act*, la cual proporciona los requisitos y obligaciones que han de seguirse a la hora de desarrollar herramientas de Inteligencia Artificial, para así, a su vez, respetar los derechos fundamentales y seguridad de la sociedad. Los ciudadanos han de sentir que la Inteligencia Artificial no presenta una amenaza a su bienestar digital y que estos están protegidos por una regulación fiable. Sin embargo, algunos países alrededor del mundo han mostrado interés en regular el uso y desarrollo de la Inteligencia Artificial, ya que de la misma manera que aporta un gran beneficio para la sociedad, su mal uso también puede causar serias consecuencias en cuanto a la seguridad de los individuos.

En línea con la temática del presente trabajo, la tecnología ha traído consigo la capacidad de cometer múltiples delitos por el medio digital, de ahí la importancia de regular y crear medidas preventivas que eviten la propagación de estos. Para evitarlo, los profesionales utilizan herramientas como el uso de sistemas de antivirus para poder crear mayor protección en los usuarios, datos de respaldo, seguridad de aplicaciones y búsqueda y evaluación de vulnerabilidades. Estas medidas ayudan a los usuarios a tener sistemas seguros en donde no se vean vulnerados sus derechos, ni su privacidad.

De la misma manera, la Inteligencia Artificial ha sido una herramienta de gran relevancia y éxito en el mundo de la ciberseguridad, ya que le permite a los profesionales reforzar y mejorar

las técnicas ya utilizadas, automatizando estos procesos y permitiendo la detección temprana de amenazas para así poder actuar de manera adecuada y minimizar los posibles daños. La Inteligencia Artificial es una herramienta capaz de realizar tareas complejas, permitiendo así poder automatizar las funciones defensivas de los sistemas, como es el caso de la criptografía, mecanizando este proceso para crear claves de protección de información.

También es una herramienta capaz de realizar monitoreos y detección de amenazas que los sistemas experimentan, dando un enfoque preventivo que permite que las necesidades de los miembros de la sociedad en materia de seguridad se vean satisfechas. Al igual que permite analizar grandes volúmenes de información, lo cual permite poder identificar patrones delictivos para así tomar medidas que permitan evitar el ataque antes de que este se cause.

En relación a la primera hipótesis de esta investigación, *la Inteligencia Artificial se utiliza para el análisis eficaz y eficiente de la información digital, por medio de la automatización de procesos,* se considera que el uso de la Inteligencia Artificial ha demostrado su eficacia dentro del ámbito de la ciberseguridad, permitiendo su uso en la mejora y automatización de técnicas ya utilizadas por los profesionales en este ámbito. La hipótesis ha sido confirmada, ya que, tras la revisión bibliográfica y las entrevistas realizadas a los profesionales, se ha podido observar cómo la Inteligencia Artificial es una herramienta utilizada por los profesionales en el ámbito de la ciberseguridad para prevenir y detener los ciberdelitos.

De la misma manera en cuanto a la segunda hipótesis, *lH2a Inteligencia Artificial, junto el rol del criminólogo permite entender los patrones de delincuencia en su profundidad y desarrollar sistemas de Inteligencia Artificial eficientes en el ámbito de la ciberseguridad*, también se ha podido confirmar. Tras el estudio y análisis de los datos y publicaciones previas, se determina esta como válida, ya que el ámbito criminológico ha sido capaz de proporcionar teorías útiles en el ámbito de la ciberseguridad, además de una visión completa basada en su fundamentación interdisciplinar. Sin embargo, los profesionales hacen énfasis en la necesidad de preparar a los estudiantes universitarios a enfrentar esta tipología criminal. Los profesionales criminólogos poseen el conocimiento y herramientas necesarios para poder entender los patrones criminales y así poder crear medidas preventivas que disminuyan la propagación de los delitos cibernéticos. Sin

embargo, resultará necesario formar a estos profesionales en materia de ciberseguridad para que estos conozcan todas las dimensiones que la ciberdelincuencia presenta.

El uso de la Inteligencia Artificial ha demostrado ser altamente viable en el mundo de la ciberseguridad, mostrando su utilización en distintos ámbitos, permitiendo a los profesionales automatizar los procesos, siendo más eficaces por medio de la detección temprana y actuando de manera apropiada a la situación. Sin embargo el mundo de la tecnología está en constante evolución, por lo cual los profesionales de la ciberseguridad han de estar en un continuo aprendizaje. La Inteligencia Artificial es una herramienta que beneficia a estos profesionales, permitiendo el análisis de patrones previos para así prevenir futuras líneas de criminalidad.

6.1. La amplitud y limitaciones de la investigación

En relación a la amplitud, cabe destacar que se ha realizado un análisis de la bibliografía más reciente sobre el tema y entrevistado a 7 profesionales expertos en la materia, lo cual también, es una de las limitaciones del presente estudio, ya que con mayores medios se podría conseguir la opinión de profesionales con mayor experiencia en este ámbito. Sin embargo, los individuos entrevistados son profesionales con larga trayectoria en el mundo de la ciberseguridad, por lo tanto se considera su visión como una fundamental y enriquecedora para la investigación de este trabajo.

6.2. Futuras líneas de investigación

El papel de la Inteligencia Artificial está cobrando una importancia creciente en el ámbito de la ciberseguridad, un campo que se enfrenta a constantes desafíos que se encuentran en constante evolución por el desarrollo continuo que presenta el mundo cibernético y, en consecuencia, los ciberdelitos también. En este contexto es crucial que las investigaciones futuras se enfoquen en el desarrollo y la implementación de nuevas medidas de seguridad, y que estas traten cuestiones de protección digital y cómo fomentarlas, como podría ser el estudio de aplicaciones concretas de Inteligencia Artificial en el ámbito de la ciberseguridad.

El mundo digital está en constante evolución, con nuevas tecnologías y aplicaciones emergiendo diariamente. Esta rápida expansión resalta la importancia de promover la investigación en este sector para mantenerse al día con estos avances. Sin embargo, además de fomentar la investigación, es esencial asegurarse que los profesionales, especialmente aquellos en

el campo de la criminología, estén adecuadamente capacitados en la temática de ciberseguridad. La delincuencia digital se ha convertido en una amenaza cada vez más significativa para la seguridad de los miembros de la sociedad, por lo que resulta vital que estos profesionales no sólo entiendan los desafíos asociados al ámbito, sino que también cuenten con las herramientas claves para desarrollar estrategias preventivas en este. Estas estrategias han de ser diseñadas para anticiparse a los riesgos que la ciberdelincuencia puede presentar.

7 REFERENCIAS BIBLIOGRÁFICAS

Aiyanyo, I., Samuel, H., & Lim, H. (2020). A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. *Applied Sciences*, *10*(17). https://doi.org/10.3390/app10175811

Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*, *531*, 1-6. https://doi.org/10.1016/j.matpr.2021.02.531

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, *8*, 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Allen, G. (2020). Understanding AI Technology. *Joint Artificial Intelligence Center (JAIC) Department of Defense*, *2*(1). https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*, *11*(9), 81-90. https://doi.org/10.17148/IJARCCE.2022.11912

AttackIQ. (2024). *Security Optimization Platform* [AttackIQ]. https://www.attackiq.com/platform/

Bi, Q., Goodman, K. E., Kaminsky, J., & Lessler, J. (2019). What is Machine Learning? A Primer for the Epidemiologist. *American Journal of Epidemiology*, kwz189. https://doi.org/10.1093/aje/kwz189

Birje, M., Challagidad, P., Tapale, M., & Goudar, R. H. (2015). *Security Issues and Countermeasures in Cloud Computing*.

Blackledge, J., & Mosola, N. (2020). Applications of Artificial Intelligence to Cryptography. *Transactions on Machine Learning and Artificial Intelligence*, *8*(3), 21-60. https://doi.org/10.14738/tmlai.83.8219

Boes, S., & Leukfeldt, E. R. (2017). Fighting Cybercrime: A Joint Effort. En R. M. Clark & S. Hakim (Eds.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*. Springer International Publishing. https://doi.org/10.1007/978-3-319-32824-9

Boneh, D., Sahai, A., & Waters, B. (2010). Functional Encryption: Definitions and Challenges. *Functional Encryption: Definitions and Challenges*, 253-273. Cryptology print Archive.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499. https://doi.org/10.1080/0735648X.2019.1692426

Broadhurst, R., Ball, M., Maxim, D., Brown, P., & Niven, A. (2019). *Artificial Intelligence and Crime: A Report for the Korean Institute of Criminology*.

Brooks, D. (2009). What is security: Definition through knowledge categorization. *Security Journal*, *23*(3), 225-239. https://doi.org/10.1057/sj.2008.18

Brown, G., Hoffman, R., & Siegel, L. (2017). Global Criminology. En *CRIM: Introduction to Criminology* (3.ª ed., pp. 320-332). Nelson.

Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. *Mobile Networks and Applications*, *19*(2), 171-209. https://doi.org/10.1007/s11036-013-0489-0

Clark, D. (2010). Characterizing Cyberspace: Past, Present and Future. *Massachusetts Institute of Technology*. https://dspace.mit.edu/bitstream/handle/1721.1/141692/Clark%20%282010%29%20Characterizing%20cyberspace.pdf?sequence=1&isAllowed=y

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589

Collier, K. (2023). *Who are the hackers that breached MGM's Las Vegas operations?* NBC NEWS. https://www.nbcnews.com/tech/security/mgm-las-vegas-hackers-scattered-spider-rcna105238

Dakalbab, F., Abu Talib, M., Abu Waraga, O., Bou Nassif, A., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. *Social Sciences & Humanities Open*, *6*(1), 100342. https://doi.org/10.1016/j.ssaho.2022.100342

Department for Science, Innovation & Technology. (2024). *Implementing the UK's AI Regulatory Principles*.

Dewett, T., & Jones, G. R. (2001). The role of information technology in the organization: A review, model, and assessment. *Journal of Management*, *27*(3), 313-346. https://doi.org/10.1177/014920630102700306

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 76-92. https://doi.org/10.1177/00048658211003925

Elish, M. C., & Boyd, D. (2018). Situating methods in the magic of Big Data and AI. *Communication Monographs*, *85*(1), 57-80. https://doi.org/10.1080/03637751.2017.1375130

European Commission. (2018). *A definition of AI: Main capabilities and scientific disciplines*. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

European Commission. (2020a). *European Security Union*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

European Commission. (2020b). *The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2023). *Cybercrime—European Commission*. European Commission: Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

European Commission. Joint Research Centre. (2018). *Artificial intelligence: A European perspective.*

European Commission. Joint Research Centre. (2020). *AI watch: Defining Artificial Intelligence: Towards an operational definition and taxonomy of artificial intelligence.* doi.org/10.2760/382730

Europol. (2022). *Cybercrime*. Europol. https://www.europol.europa.eu/crime-areas/cybercrime

Europol. (2023a). *European Cybercrime Centre—EC3*. Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol. (2023b). *IOCTA, internet organized crime threat assessment 2023.* Publications Office. https://data.europa.eu/doi/10.2813/587536

Faiza, S. F., Rizwan, M., & Kulsoom, U. E. (2022). Artificial Intelligence Incidents & Ethics A Narrative Review. *International Journal of Innovation and Technology Management, 2*(2), 52-64. https://doi.org/10.54489/ijtim.v2i2.80

Folsom, T. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *Tulane Journal of Technology & Intellectual Property*, *9*, 75-121. https://ssrn.com/abstract=1350999

Fung, B. (2024). EU approves landmark AI law, leapfrogging US to regulate worrying new technology | CNN Business. *CNN*. https://www.cnn.com/2024/03/13/tech/ai-european-union/index.html

García-Pablos de Molina, A. (1989). La aportación de la criminología. *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, *3*, 79-95.

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K.,

Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., … Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514. https://doi.org/10.1016/j.iot.2022.100514

Government of Canada. (2023). *Artificial Intelligence and Data Act*. Government of Canada; Innovation, Science and Economic Development Canada. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act

Groff, J. R., & Weinberg, P. N. (1999). *The Complete Reference: SQL*. Osborne/McGraw-Hill.

Guerrero, M. A. (2016). La investigación cualitativa. *INNOVA Research Journal*, *1*(2). https://doi.org/10.33890/innova.v1.n2.2016.7

Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, *61*(4), 5-14. https://doi.org/10.1177/0008125619864925

Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I., & Ramkumar, P. N. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine*, *13*(1), 69-76. https://doi.org/10.1007/s12178-020-09600-8

IBM Security. (2023a). *Cost of a Data Breach Report*. IBM. https://www.ibm.com/downloads/cas/E3G5JMBP

IBM Security. (2023 b). *¿Qué es MITRE ATTA&CK)*. IBM. https://www.ibm.com/es-es/topics/mitre-attack

IBM Security. (2024a). *What is a Zero-Day Exploit?*. IBM. https://www.ibm.com/topics/zero-day

IBM Security. (2024b). *What Is Hacking?*. IBM. https://www.ibm.com/topics/cyber-hacking

IBM Security. (2024c). *What is Mobile Security?*. IBM. https://www.ibm.com/topics/mobile-security

IBM Security. (2024d). *What is Offensive Security?*. IBM. https://www.ibm.com/topics/offensive-security

Ibrahim, S., Nnamani, D., & Okosun, O. (2021). Types of Cybercrime and Approaches to Detection. *IOSR Journal of Computer Engineering*, *23*, 24-26. https://doi.org/10.9790/0661-2305022426

Instituto Nacional de Ciberseguridad. (2022). *Balance de Seguridad*. INCIBE. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

Instituto Nacional de Ciberseguridad. (s. f.). *Deepfakes*. INCIBE. https://www.incibe.es/aprendeciberseguridad/deepfakes

Interpol. (2024). *Cybercrime*. Interpol. https://www.interpol.int/en/Crimes/Cybercrime

ISO/IEC 27002. (2005). *ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management*. https://www.iso.org/standard/50297.html

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255-260. https://doi.org/10.1126/science.aaa8415

Kareem, F., Ameen, S., Ahmed, A., Salih, A., Ahmed, D., Kak, S., Najat, Z., Yasin, H., Mahmood, I., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. *Asian Journal of Research in Computer Science*, *10*(3), 13-32. https://doi.org/10.9734/AJRCOS/2021/v10i330242

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, *30*(4), 470-486.

Koret, J., & Bachaalany, E. (2013). *The Antivirus Hacker's Handbook*. Wiley.

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in Computer Virology*, *6*(2), 105-114. https://doi.org/10.1007/s11416-009-0137-1

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado, 281*, del 24 de noviembre de 1995

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(10), 1-18. https://doi.org/10.1186/s42400-020-00050-w

Mahesh, B. (2019). Machine Learning Algorithms -A Review. *International Journal of Science and Research (IJSR)*, *9*(1), 381-386. https://doi.org/10.21275/ART20203995

Marinescu, D. C. (2017). Chapter 1—Complex Systems. En D. C. Marinescu (Ed.), *Complex Systems and Clouds* (pp. 1-32). Elsevier. https://doi.org/10.1016/B978-0-12-804041-6.00001-3

MGM Resorts. (2023). *Notice of Data Breach*. MGM Rewards. https://www.mgmresorts.com/en/notice-of-data-breach.html

Microsoft Azure. (2024). *Qué es Azure: Servicios en la nube de Microsoft | Microsoft Azure*. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure

Min, D., Ko, Y., Walker, R., Lee, J., & Kim, Y. (2022). A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *41*(7), 2038-2051. https://doi.org/10.1109/TCAD.2021.3099084

Ministerio del Interior. Portal Estadístico de la Criminalidad. *Gobierno de España*. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23*(18), 1-9. https://doi.org/10.1007/s11920-021-01228-w

Mudaliar, A. (2024). Azure Data Breach Compromises Microsoft. *Spiceworks Inc*. https://www.spiceworks.com/it-security/vulnerability-management/news/azure-microsoft-exchange-servers-active-exploitation-hackers/

Muniesa, P., Herrera, D., Guerrero, J., Martínez, F., Rubio, M. R., Gil, V., Santiago, A. M., & Gómez, M. (2022). *Informe sobre la cibercriminalidad en España 2022*.

Murphy, C. (2024). Understanding cybercrime. *European Commission*.

Mutchler, P., Doupe, A., Mitchell, J., Kruegel, C., & Vigna, G. (2015). *A Large-Scale Study of Mobile Web App Security*. *50*.

Naciones Unidas. (s. f.-a). La Agenda para el Desarrollo Sostenible. *Desarrollo Sostenible*. Recuperado 14 de abril de 2024, de https://www.un.org/sustainabledevelopment/es/development-agenda/

Naciones Unidas. (s. f.-b). Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación. *Desarrollo Sostenible*. Recuperado 14 de abril de 2024, de https://www.un.org/sustainabledevelopment/es/infrastructure/

Naciones Unidas. (s. f.-c). Objetivo 16: Promover sociedades justas, pacíficas e inclusivas. *Desarrollo Sostenible*. Recuperado 14 de abril de 2024, de https://www.un.org/sustainabledevelopment/es/peace-justice/

National Institute of Standar and Technology. (2024). Cyberspace. En *NIST*. https://csrc.nist.gov/glossary/term/cyberspace

Onn, C. W., & Sorooshian, S. (2013). *Mini Literature Analysis on Information Technology Definition*.

Oxford Dictionary. (2022). Security. En *Oxford Dictionary*. https://www.oed.com/search/dictionary/?scope=Entries&q=security

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences, 12*, 1-18. https://doi.org/10.3390/app12031076

RAE. (2020). Tecnología. En *Diccionario esencial de la lengua española*. https://www.rae.es/desen/tecnología

RAE. (2024). Corpus. En *«Diccionario de la lengua española»—Edición del Tricentenario*. https://dle.rae.es/corpus

Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2023). A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing. *BOHR International Journal of Computer Science*, *2*, 1-7. https://doi.org/10.54646/bijcs.019

Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial. *Boletín Oficial del Estado*, *268*, de 9 de noviembre de 2023.

Reddy, A. (2023). *Artificial intelligence advantages in cloud fintech application security*. *4*(8), 48-53.

Rubio, G. (2021). El uso de la AI para ciberseguridad. *Revista da UI_IPSantarém*, *9*(4), 91-97.

Sagiroglu, S., & Sinanc, D. (2013). Big data: A review. *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 42-47. https://doi.org/10.1109/CTS.2013.6567202

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

Sanuy, A. (2023). *Caos en Las Vegas por una oleada de ciberataques del grupo de jóvenes hackers «la Araña Desordenada»*. La Vanguardia. https://www.lavanguardia.com/tecnologia/20230918/9234028/mgm-resorts-apaga-sistemas-informaticos-casinos-ataque-cibernetico-pmv.html

Sarker, I. (2021). *AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions*. https://doi.org/10.20944/preprints202101.0457.v1

Schappert, S. (2023a). *Caesars SEC breach report: $15m ransom paid*. Cyber news. https://cybernews.com/news/caesars-15m-ransom-sec-breach-report-6t-stolen-data/

Schappert, S. (2023b). *MGM says it recovered from cyberattack, employees tell different story*. Cyber news. https://cybernews.com/news/mgm-touts-cyber-attack-recovery-on-track-employees-tell-different-story/

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Shabbir, J., & Anwer, T. (2018). Artificial Intelligence and its Role in the Near Future. *Cyber, Intelligence and Security*, *1*(1), 103-119. https://doi.org/10.48550/arXiv.1804.01396

Stalans, L., & Donner, C. (2018). Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. *Cyber Criminology. Advanced Sciences and Technologies for Security Applications.*, *24*, 25-45. https://doi.org/10.1007/978-3-319-97181-0_2

Syafitri, W., Shukur, Z., Mokhtar, U., Sulaiman, R., & Azwan, M. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325-39343. https://doi.org/10.1109/ACCESS.2022.3162594

Sykes, G., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664-670. https://doi.org/10.2307/2089195

Thambiraja, E., Ramesh, G., & Umarani, R. (2012). A Survey on Various Most Common Encryption Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(7).

The Hacker News. (2023). *Microsoft Bug Allowed Hackers to Breach Over Two Dozen Organizations via Forged Azure AD Tokens*. The Hacker News. https://thehackernews.com/2023/07/microsoft-bug-allowed-hackers-to-breach.html

The White House. (2022). *Blueprint for an AI Bill of Rights*. The White House.

The White House. (2023). *Applying the Blueprint for an AI Bill of Rights | OSTP*. The White House. https://www.whitehouse.gov/ostp/ai-bill-of-rights/applying-the-blueprint-for-an-ai-bill-of-rights/

Toosi, A., Bottino, A. G., Saboury, B., Siegel, E., & Rahmim, A. (2021). A Brief History of AI: How to Prevent Another Winter (A Critical Review). *PET Clinics*, *16*(4), 449-469. https://doi.org/10.1016/j.cpet.2021.07.001

Tóth, Z., Caruana, R., Gruber, T., & Loebbecke, C. (2022). The Dawn of the AI Robots: Towards a New Framework of AI Robot Accountability. *Journal of Business Ethics*, *178*(4), 895-916. https://doi.org/10.1007/s10551-022-05050-z

United Nations. (2020). *Cybercrime*. United Nations: UNODC ROMENA. https://www.unodc.org/romena/en/cybercrime.html

Universidad de Castilla-La Mancha. (2021). *Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario* (J. M. Tejero González, Ed.). Ediciones de la Universidad de Castilla-La Mancha. https://doi.org/10.18239/estudios_2021.171.00

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 101666.

Velasco, C. (2022). *Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments*. *23*(1), 109-126. https://doi.org/10.1007/s12027-022-00702-z

Volti, R. (2017). *Society and Technological Change* (Eight Edition). Worth Publisher.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wirkuttis, N., & Hadas, K. (2017). Artificial Intelligence in Cybersecurity. *Cyber, Intelligence, and Security, 1*(1), 103-119.

World Economic Forum. (2023). *The Global Risk Report 2023 18th Edition* (18). https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

8 ANEXOS

8.1. Anexo 1. Guion de las entrevistas realizadas.

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?
2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?
3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?
4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?
5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?
6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?
7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?
8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?
9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?
10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?
11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?
12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

8.2. Anexo 2. Transcripción de la entrevista 1 (E1)

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

Mi Nombre es Pascualino Angiolillo Fernández, soy Oficial con el Grado de Mayor General de la República Bolivariana de Venezuela. Ex Rector de la Universidad Nacional Experimental Politécnica de la Fuerza Armada Bolivariana. Actualmente estoy a orden del Ministerio de la Defensa.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

La Ciberseguridad es un asunto de interés de Estado y en la Fuerza Armada Nacional, siempre procuramos cumplir con todas las medidas que garanticen un entorno altamente confiable, reduciendo al mínimo los riesgos y amenazas que atenten contra la Seguridad de nuestra nación en todos los ámbitos.

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Los Organismos de Seguridad y Defensa de nuestro país, cuentan con Departamentos especializados en prevenir y erradicar los ciber delitos. Inicialmente hacemos énfasis en los temas de prevención y concientización, para educar a toda la población, en esta materia. Con esta estrategia, entonces se crean las condiciones para activar la inteligencia social, es decir, todos los habitantes del país, se convierten en fuentes de información que coadyuva con la inteligencia (análisis de información) y seguridad integral del país.

Para alcanzar este fin, el País se organiza por niveles en lo que se conoce como: El Sistema Defensivo Territorial, que reúne a todos los ámbitos y organiza los niveles de gobierno y la población en estructuras jerarquizadas conocidas como Órganos de Dirección de Defensa Integral (ODDI) desde el nivel nacional, pasando por los niveles Estatales, Municipales, Parroquiales y Comunales.

En cada ODDI se establece un Puesto de Dirección, en donde todos los actores se reúnen y aportan la información necesaria para garantizar el Proceso de Planificación bajo un entorno de seguridad integral. Dichos Órganos de Dirección de Defensa Integral tiene como Marco legal, la Constitución Nacional de la República Bolivariana de Venezuela en un título Referido a la

Seguridad de la Nación, desde donde se desprende el Principio de Corresponsabilidad en materia de Seguridad Nacional, es decir, todos los habitantes del país, incluso los extranjeros que habiten en él y todo los entes del gobierno, son Responsables en materia de seguridad y defensa en cada uno de los ámbitos (Político, Social, Cultural, Geográfico, Ambiental, Económico y Militar). El ámbito tecnológico es considerado transversal a todos los anteriores citados.

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?

En mi opinión, la Inteligencia Artificial es un Algoritmo de Razonamiento Lógico basado en una postura onto-epistémica propia de la naturaleza humana. En algunas ocasiones puede tener un enfoque lógico ambivalente, por lo que cuáles patrón divergente a ese esquema, pudiera considerarse como un elemento de alerta y atención

Hablando desde el punto de vista de la Teoría de los Sistemas, cualquier variable desencadenante que altere el equilibrio del sistema, puede considerarse como un elemento perturbador que debe ser atendido de inmediato para evitar el caos.

De Allí, yo considero que los enfoques y técnicas desde el Punto de Vista de la Inteligencia Artificial que deben utilizarse para la detección y prevención de amenazas cibernéticas, tienen que ver con modelos matemáticos basados en la Teoría de la Complejidad, la Teoría de los Sistemas y técnicas de razonamiento lógico, que representen la postura onto epistemológica del ser humano, plasmada en los algoritmos de Inteligencia Artificial que son elaborados en la nube (Donde se concentra toda la información) y donde existe el mayor riesgo.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

Considero que la Inteligencia Artificial debe tener un canal que permita el ingreso de toda la información posible en el Ciber Espacio, esto con el fin de expandir el razonamiento lógico del sistema, sin embargo, el ingreso de dicha información, debe contar con un sistema tecnológico, deductivo e inductivo que permita la confiabilidad y veracidad de las fuentes. La creación de un corpus confiable en el algoritmo, es fundamental para garantizar la, Ciberseguridad.

Hablando en términos médicos científicos: Debemos controlar la Sinapsis que recibe la información y también las redes neuronales que las tramiten, antes de que sean procesadas en el sistema, Cerebro.

Lo mismo debemos hacer en el proceso de razonamiento lógico de respuesta ante los estímulos, que en la Inteligencia Artificial es un Algoritmo que en mi opinión, se compara con el Cerebro y los Sentidos. Aquí también debemos incorporar todos las técnicas y procedimientos para evitar amenazas al sistema.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?

El mayor desafío es el de detectar amenazas, sin afectar la Universidad y velocidad del sistema.

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?

Las experiencias de Irán, Rusia y China quienes gracias a sus protocolos han evitado daños a su seguridad por parte de ciber piratas.

8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?

Razonamiento Matemático, Lógico y Complejo, Conocimientos Generales de Seguridad y Defensa, Psicología del Comportamiento, Lógica Predictiva, Teoría de Sistemas y otros conocimientos de Ingeniería Electrónica, Telecomunicaciones y Computación.

9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

Tomando en consideración la Prevención (Educación-Concientización). Incorporando el Desarrollo Tecnológico y profundizando en las experiencias de otros actores.

10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

Debe regularse de manera estricta

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?

Por Supuesto que sí. En Venezuela, el CICPC practica ese rol y los criminólogos han desarrollado un extraordinario plan preventivo.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

Considero que la Inteligencia Artificial será un mecanismo tecnológico al servicio del bien para la prevención de estas omisiones.

8.3. Anexo 3. Transcripción de la entrevista 2 (E2)

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

   Mi nombre es Teresa Lamus y soy Gerente y Abogado Comercial.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

   Llevo 14 años trabajando en esta área.

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Manejo de Datos con sus respectivas medidas de protección, leyes en cuanto a privacidad y Transferencia y manejo de datos (encrypted).

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así ¿Cuáles?

Si, se utiliza para el monitoreo preventivo, entrenamiento y desarrollo de tecnología que permitan la detección temprana de ataques cibernéticos.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

En el desarrollo de herramientas nuevas que vayan al ritmo del Inteligencia Artificial, en este momento existe una desconexión debido al avance muy rápido del Inteligencia Artificial.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?

Desafíos son muchos el primero es la falta de entrenamiento que existe, se hable mucho de Inteligencia Artificial pero no hay una coherencia entre lo que está pasando en el mercado y los conocimientos que se manejan.

La Inteligencia Artificial no es algo simple de explicar existen muchas complejidades y la sociedad va a un paso más lento, vamos a comenzar a ver muchos delitos productos del Inteligencia Artificial que no existen aún en el marco legal, ya van a ir más allá de transacciones fraudulentas.

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?

Ahora la mayoría de las instituciones financieras tienen herramientas como reconocimiento de voz, autenticación para ingresar a los portales del banco y esto ayuda mucho.

8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?

Entrenamiento, mucha investigación y ver el Inteligencia Artificial como una herramienta de beneficio pero también de mucho cuidado y análisis.

9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

Identificación de ataques cibernéticos.

10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

Absolutamente, las leyes de privacidad se quedaran en un marco obsoleto con respecto al Inteligencia Artificial, ya no es transferencia de datos únicamente, es algo más complejo, es el uso de robots para producir información.

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?

Siempre y cuando las universidades comiencen a preparar a los profesionales en esta dirección si, debe existir una relación entre el aula y la sociedad, la educación debe evolucionar y crear nuevos marcos de aprendizaje.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

Aún hay mucho camino por recorrer, por ahora es una herramienta que está evolucionando pero es un arma que se debe manejar con cautela.

8.4. Anexo 4. Transcripción de la entrevista 3 (E3).

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

Me llamo Tony Orlando. Soy ciudadano canadiense. Por cierto, nací en Italia. Vine cuando tenía siete años, y la mayor parte de mi educación ha sido en Canadá. Actualmente soy presidente de la empresa de ingeniería de ciberseguridad aquí llamada E4P Inc., que es Ingenieros para la Profesión. Y lo que estamos haciendo es tratar de crear una disciplina de ciberseguridad, como un ingeniero.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

Mucho antes de que tú nacieras, yo trabajaba en lo que se llaman líneas dedicadas, y las infraestructuras críticas se ponían en líneas dedicadas. Las líneas dedicadas eran muy caras. Así que pasar a Internet fue una transición fácil. El único problema es que Internet en sí no es una red segura. No se puede hacer segura porque tú y yo no podríamos comunicarnos si lo fuera. Ahora sería mucho más complicado. Así que aquí tenemos una espada de dos filos.

Bueno, tenemos esta red que esencialmente es insegura, y estamos tratando de poner datos seguros allí, y ahí es donde están los problemas. Bien, estamos trabajando con eso, y nos estamos asegurando de que los ingenieros están en la parte superior de la lista de asumir la responsabilidad de asegurarse de que el equipo está al día y que el personal que está trabajando en las redes están al día también. Llevo mucho tiempo en esto. Me has preguntado un poco sobre mis antecedentes.

Pero sí, he estado alrededor desde 1972. Trabajé para una empresa como ingeniero de campo, y luego trabajé como ingeniero de diseño, y esto es en la tecnología informática, dentro de la tecnología de chip de diseño. Y a partir de ahí, me propague a más software, e hice un montón de lo que se llamaba microcódigo en el momento, que es lo mismo que el firmware. Bueno, y el firmware es lo que controla el hardware para hacer ciertas cosas, y aquí es donde básicamente me metí en la seguridad.

Yo sabía que el problema de seguridad era un gran problema allí. La seguridad del hardware es difícil porque tienes que estar al lado de la computadora para ser capaz de robar algo de la computadora. Cuando se trata de ingeniería de microcódigo, es un poco diferente. Es como si esto

se pudiera hacer de forma remota, y aquí es donde está el problema hoy en día. Muchas de las cosas se pueden hacer a distancia.

También tengo mi propio departamento de TI y mi propia empresa, e instalé redes en aquellos días

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Internet nunca fue realmente seguro. Era segura cuando lo dirigían los militares, pero sólo porque funcionaba con líneas dedicadas y líneas que no eran accesibles para gente como tú o yo o lo que fuera. Y además, no teníamos el conocimiento. No teníamos el poder informático para entrar en esas redes.

No importa lo que hagas con la seguridad, la seguridad, incluso la encriptación, hay maneras alrededor de la encriptación. Hay una manera de evitarla encriptación, no necesitas preocuparte por el esquema de encriptación de lujo, muy complicado, porque todo lo que necesitas hacer es poner datos conocidos allí antes de que se encripten. Y una vez que se encripta, recuperas esos datos conocidos, y puedes aplicar ingeniería inversa a esos datos para obtener la clave. Y una vez que tienes la clave, entonces puedes obtener el resto de las cosas también.

Entonces, ¿qué es lo básico? Bueno, datos de respaldo, definitivamente, sabes, necesitas datos de respaldo. Encriptación, sí, necesitas la encriptación, aunque, tiene sus propios defectos, necesitas la encriptación.

El software antivirus, por ejemplo, alguien inyecta un virus en tu ordenador, necesitas saber si ese software antivirus está ahí.

La seguridad de las aplicaciones es que la gente escribe sus propias aplicaciones, y no siempre son necesariamente seguras, porque no siguen las reglas del software que les permite construir esa seguridad. Así que la seguridad se convierte ahora en una cosa individual, algo que el individuo tiene que inyectar en sus programas con el fin de hacerlos seguros.

Hay vulnerabilidades en eso también. Las vulnerabilidades, por supuesto, una de las mayores vulnerabilidades es el hecho de que la gente como los malos actores en este momento están entrando mediante el uso de esquemas de correo electrónico.

Y una vez que haga clic en este enlace, pueden descargar, como, por ejemplo, como un registrador de teclado, y ese registrador de teclado realiza un seguimiento de todo lo que la persona entra.

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?

Si, sobre todo la criptografía, esto es un arte que, creo que va a ser mejorado que más adelante, hablaremos de ello mejorado enormemente con la Inteligencia Artificial.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

Principalmente para mejorar las técnicas que se están utilizando ahora, como la encriptación.

Lo que se puede hacer es tal vez el uso de la Inteligencia Artificial para la biometría. Bueno, eso podría ser una manera de evitarlo. Pero recuerda lo que dije, que muchos de estos malos actores ya están, ya saben cuándo algo sale, y ya saben cómo usarlo. Pasan mucho tiempo usándolo. No estamos hablando de dos o tres hackers, estamos hablando de miles de ellos. Seguro que has oído hablar de los hackers Black Cat de Rusia. Estas son organizaciones que se componen de miles de personas y miles de personas inteligentes para el caso.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?

La Inteligencia Artificial se puede utilizar para la ciberseguridad, así como también puede ser utilizada por los malos actores también. Se tiene un cuchillo de doble filo aquí, dónde, puede ser bueno y malo la gestión de Firewalls, protección de contraseña, la detección de sí una contraseña es una contraseña débil o es una contraseña que es bastante común. Somos la naturaleza humana y la naturaleza humana, no nos gusta memorizar cosas como contraseñas muy complicadas. Y mucha gente, se encuentran una contraseña y utilizan la misma contraseña una y otra y otra vez, en cada sitio que van.

Bueno, la Inteligencia Artificial podría, evitar que eso suceda, cuando tienes esta incorporada en un navegador. Y por cierto, la próxima revisión de Google tendrá un módulo de Inteligencia Artificial para detectar cosas como la reutilización de contraseñas, contraseñas débiles y cosas así.

No sé lo bueno que es, pero estará disponible allí. Pero, cuando ves algo así, está disponible para todo el mundo, incluidos los malos actores.

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?

Porque no estoy realmente involucrado en ningún sitio en particular, los estoy monitoreando y me entero de casos como el MGM, por ejemplo, y tuvimos uno con el gasoducto, donde Universidades fueron golpeadas en Canadá y todos ellos se derivan en este momento de la ingeniería social.

La mayoría de los agentes malignos estaban allí porque rompieron el sistema de protección debido a las debilidades de los empleados que estaban dispuestos a dar información. ¿Y cómo se controla eso? Una universidad como la Universidad de Winnipeg fue golpeada aquí. Tienes 20-30.000 estudiantes y tienes, no sé cuánto personal tienen allí. Todos tienen diferentes niveles o deberían tener diferentes niveles de seguridad.

Así que eso podría ser un área donde la Inteligencia Artificial podría ser capaz de ayudar y estoy seguro de que será capaz de distinguir entre la seguridad de las personas individuales a ciertas áreas de la red.

8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?

En primer lugar, hay que tener buenas dotes de comunicación. Hay habilidades técnicas, por supuesto, pero debes tener buenas habilidades de comunicación. Tienes que ser capaz de comunicarlas cosas, como, por ejemplo, habilidades de comunicación en networking, escritura de negocios, amabilidad, ser diplomático, tener un buen servicio al cliente, seguir la etiqueta adecuada de comunicación, ser capaz de realizar resoluciones de conflictos, habilidades de negociación y amabilidad, básicamente, son las realmente grandes, grandes aquí.

Y luego, por supuesto, el trabajo en equipo. Tienes que, y por cierto, ahora, todo esto es, estoy asumiendo que el individuo ya sabe acerca de la parte técnica de la misma. Estos son los rasgos humanos. Y tienes la gestión de conflictos, sacas una resolución y tu jefe va a decir, eso es

demasiado caro de implementar. Así que tienes que ser capaz de sortear esto a través de la gestión de conflictos.

Tienes que ser capaz de comunicarte para que se entienda lo que quieres decir. Tienes que ser capaz de negociar. Establecer relaciones es muy importante. Cuanta más gente conozcas en distintos ámbitos, mejor te irá. Formar equipos, ser capaz de crear tu propio equipo, gestionar equipos, resolver conflictos, todo eso son cosas bastante sencillas que son importantes.

Asegúrate de tener la información adecuada. Asegúrate de que entiendes la tecnología, como la computación en nube. Controlar el acceso a los datos sensibles y quién debe tener ese acceso de control. Identificar y gestionar el acceso. Tratar de pensar, la seguridad móvil, entender la seguridad móvil. Educar a los empleados sobre la seguridad cibernética de forma continua, no sólo una vez.

9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

Se utiliza para automatizar los procesos y técnicas ya utilizadas.

10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

Creo que esa es otra pregunta difícil. Pero sí, habrá muchos problemas éticos. No cabe duda. Ya hay gente que no quiere poner barreras a ciertos procesos de Inteligencia Artificial, porque dicen que es una violación de los derechos humanos, una violación de la libertad de expresión, etcétera.

De nuevo, es algo que nos hacemos a nosotros mismos. Tenemos que, llegar a un cierto momento y decir, estas son las cosas que puedes decir, y estas son las cosas que no puedes decir.

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?

La Inteligencia Artificial está corriendo fuera de control en estos momentos. Bueno, algunas personas están hablando de la Inteligencia Artificial destruir la humanidad. Ahora, si eso es cierto o no, no lo sé. Pero déjame darte un escenario. Ahora somos prisioneros de nuestras propias

delicias. Lo robé de Hotel California. Usted está familiarizado con ella. Así que somos prisioneros de nuestros propios placeres.

Has preguntado sobre criminología. Bueno, todo depende de cómo se use este dispositivo. Hay mucha desinformación en internet que debería ser información criminal. Hay un montón de mentiras, un montón de cosas que simplemente no son ciertas. Se utilizan para incriminar a la gente. No tienen límites. Y, como pones algo en línea, si lo haces con algún sitio de medios sociales, como Facebook, por ejemplo, es como si yo te contara un secreto. Vale, y entonces sales y le cuentas a otro un secreto, pero ahora le das tu propio toque. ¿Dónde está la parte criminal?

Si se lo dices a la gente con tus propias palabras, y tus propias ideas, has cambiado mi mensaje original, cosa de la que te hablé. Y entonces esa persona le dice a alguien más y se propaga, va una y otra y otra vez hacia el resultado final. En el momento en que llega al resultado final, es absolutamente diferente de lo que era la idea original.

Así que la pregunta ahora es, ¿a qué nivel se va a asociar la criminología con eso? Es bastante difícil de visualizar. Sí, podemos establecer reglas básicas. Podemos establecer barandillas. La gente no sigue las reglas, les gusta romper las reglas. No siguen las barandillas porque si hay una barandilla, intentarán romperla. Sí. Es sólo un hecho de la naturaleza humana. Y sé lo que estás tratando de conseguir es que es, sólo puedo decir que va a ser muy difícil. Muy difícil de manejar.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

Es difícil de determinar, porque, como he dicho, es un arma de doble filo, pero creo que nos ayudará a mejorar las técnicas que tenemos.

8.5. Anexo 5. Transcripción de la entrevista 4 (E4).

1) ¿Podría decirnos cuál es su nombre, nacionalidad y cargo actual?

Analista senior para una empresa de consultoría, principalmente hago pruebas de penetración.

2) ¿Qué experiencia has tenido en el mundo de la ciberseguridad?

Para esta empresa 1 año pero en general 3 años.

3) ¿Podría ofrecernos una visión general de las medidas de ciberseguridad que se utilizan actualmente para luchar contra la ciberdelincuencia?

Utilizamos diferentes medidas como ver las foros de hackers y sobre todo la seguridad de las aplicaciones web.

4) ¿Conoce las técnicas de Inteligencia Artificial que se están utilizando para la detección y prevención de ciber amenazas? En caso afirmativo, ¿cuáles?

Sí, utilizamos Attack IQ que es una herramienta que simula ataques para identificar las amenazas a prevenir.

5) ¿Cómo cree que puede utilizarse la Inteligencia Artificial para mejorar los enfoques tradicionales de la ciberseguridad?

Hace que sea más fácil saber lo que está pasando y atacar las amenazas a las que nos enfrentamos.

6) ¿Podría decirnos cuáles son los principales retos a los que se enfrentarán los profesionales a la hora de implementar la Inteligencia Artificial en la ciberseguridad?

Va a ser difícil mantenerse al día con la nueva información que se está añadiendo, la Inteligencia Artificial es un arma de doble filo que puede ayudar pero también crear más problemas.

7) ¿Tienes algún ejemplo de escenarios reales en los que una solución de ciberseguridad en la que se haya utilizado Inteligencia Artificial haya tenido éxito?

Sí, Microsoft ha implementado un uso de Inteligencia Artificial en sus operaciones que puede ayudar a combatir estas amenazas.

8) ¿Qué habilidades cree que son necesarias que tengan los profesionales para sacar el máximo partido de la Inteligencia Artificial en su trabajo?

Deberían aprender y entender Machine Learning, así como cómo funcionan los chatbots y los foros de hackers, porque aquí se desarrollan virus y es importante estar al tanto.

9) ¿En qué formas actuales se está utilizando la Inteligencia Artificial para reducir el impacto de los ciberataques en su entorno de trabajo?

Se está utilizando de manera que ayuda a ver lo que los ojos humanos no pueden ver, porque a veces es difícil hacer un seguimiento de todo lo que está sucediendo y a veces las cosas están sucediendo tan rápido que no se puede identificar.

10) ¿Considera que el uso de la Inteligencia Artificial en el campo de la ciberseguridad podría traer problemas éticos, especialmente en términos de privacidad y protección de datos?

Sí, será un problema.

11) ¿Considera que el papel de un criminólogo es fundamental para poder crear estrategias preventivas de la ciberdelincuencia con el uso de la Inteligencia Artificial?

Sí, especialmente con las *Deepfakes* será difícil identificar cuando alguien es real o no, y el criminólogo puede aportar una perspectiva para identificar cuando la gente realmente dijo algo o no.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en la lucha contra la ciberdelincuencia?

Sí, será un arma de doble filo, así que debemos tener cuidado con ella porque puede ayudarnos pero también puede ayudar a los actores malignos.

8.6. Anexo 6. Transcripción de la entrevista 5 (E5)

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

Mi nombre es Oscar Ramírez, soy venezolano egresado de pregrado y postgrado de la universidad de Georgia Institute of Technology. Actualmente soy Profesor de la Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA) en calidad de asesor, con línea de investigación en ciberespacio.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

Ingrese en IBM como programador en 1970 y egresé como Director de Línea de Telecomunicaciones y Estándares en 1990, y a partir de este año me dedique desarrollar proyectos privados sin fines de lucro, teniendo como telón de fondo la industria del conocimiento de siglo XXI en la era del ciberespacio, único espacio dual, físico y virtual, desarrollado completamente por el ser humano.

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Teniendo en cuenta que la ciberseguridad es la práctica, capacidad, o procesos, para defender el espacio cibernético, en la actualidad, dichas medidas de ciberseguridad pueden abarcar, desde firewalls y antivirus hasta sistemas de detección de intrusiones, hasta sistemas de autenticación multifactorial. Además, para prevenir ciberdelitos también se emplean técnicas como el cifrado de datos, la monitorización de redes y la educación continua de los usuarios.

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?

Por supuesto. Existen varias técnicas avanzadas de Inteligencia Artificial se utilizan para la detección y prevención de amenazas cibernéticas. Los algoritmos de Machine Learning aprenden de datos históricos para identificar patrones y anomalías indicativas de actividad maliciosa en tiempo real. Las Redes Neuronales Artificiales, inspiradas en el cerebro humano, procesan grandes volúmenes de datos para reconocer patrones complejos asociados con ataques, detectando amenazas avanzadas y adaptándose a nuevas técnicas. El Aprendizaje por Refuerzo permite a los sistemas ajustar sus estrategias al interactuar con el entorno, haciéndolos más resilientes en

entornos cibernéticos dinámicos. El Procesamiento de Lenguaje Natural analiza grandes volúmenes de texto para detectar indicios de ingeniería social y phishing. Combinadas con el conocimiento experto humano, estas técnicas de Inteligencia Artificial permiten a las organizaciones anticipar, detectar y responder rápidamente a una amplia gama de amenazas cibernéticas, mejorando significativamente su postura de seguridad.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

La Inteligencia Artificial puede potenciar la ciberseguridad al acelerar la detección de amenazas, permitir respuestas ágiles a incidentes y ajustarse automáticamente a patrones de ataque cambiantes. Esta capacidad de adaptación y automatización complementa los enfoques tradicionales al agregar una capa adicional de inteligencia y eficiencia a las estrategias de seguridad. La Inteligencia Artificial no solo optimiza la identificación de riesgos, sino que también fortalece la capacidad de respuesta ante amenazas en evolución, mejorando significativamente la postura de seguridad de las organizaciones.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?

Los desafíos clave que los profesionales enfrentarán en la implementación de la inteligencia artificial en ciberseguridad incluyen la necesidad de datos de calidad para entrenar modelos de Inteligencia Artificial, la interpretación de decisiones algorítmicas, la garantía de la transparencia y ética en el uso de la Inteligencia Artificial, y la capacitación del personal para comprender y trabajar con estas tecnologías emergentes. Estos desafíos resaltan la importancia de contar con datos precisos, la capacidad de interpretar las decisiones de los algoritmos, la necesidad de mantener altos estándares éticos y transparentes en el uso de la Inteligencia Artificial, y la importancia de capacitar al personal para aprovechar al máximo el potencial de estas tecnologías en el ámbito de la ciberseguridad.

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?

En el caso del phishing, por ejemplo, el uso de sistemas de Inteligencia Artificial para detectar y prevenir ataques de phishing en tiempo real es un ejemplo efectivo de cómo la Inteligencia

Artificial puede reducir el impacto de los ciberdelitos. Estos sistemas analizan patrones de lenguaje, detectan esquemas maliciosos, se adaptan continuamente, y automatizan respuestas para mitigar amenazas. Su implementación ha demostrado reducir la tasa de éxito de los ataques de phishing en entornos corporativos, aunque se debe tener en cuenta el potencial de la Inteligencia Artificial para ser utilizada por ciberdelincuentes, requiriendo vigilancia constante y medidas de seguridad adicionales.

8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?

Para aprovechar eficazmente las tecnologías emergentes y disruptivas de la Inteligencia Artificial en el trabajo, se requiere una combinación equilibrada de habilidades duras y suaves. En cuanto a las habilidades duras, es fundamental comprender los fundamentos de la Inteligencia Artificial, dominar el aprendizaje automático para desarrollar modelos predictivos, tener habilidades de programación en lenguajes como Python o Java, ser capaz de analizar datos para extraer información relevante y comprender el Procesamiento del Lenguaje Natural. En cuanto a las habilidades suaves, se destacan la capacidad de pensamiento crítico y resolución de problemas, la disposición al aprendizaje continuo, la comunicación efectiva para transmitir ideas de manera clara, la colaboración en equipo para lograr objetivos comunes y la adaptabilidad a entornos cambiantes. Estas habilidades combinadas permiten a los profesionales no solo aprovechar al máximo las tecnologías emergentes de la Inteligencia Artificial, sino también adaptarse y liderar en un entorno laboral impulsado por la innovación y la transformación digital.

9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

La Inteligencia Artificial desempeña un papel crucial en la reducción del impacto de los ciberataques en el ámbito laboral. Mediante el análisis en tiempo real de diversos tipos de datos, la Inteligencia Artificial puede detectar tempranamente amenazas y anomalías, permitiendo una respuesta rápida y eficiente. Además, la automatización de tareas repetitivas libera a los expertos para concentrarse en actividades estratégicas, mientras que el aprendizaje continuo mejora constantemente las capacidades de detección y respuesta. El análisis predictivo y preventivo permite anticipar posibles ataques y tomar medidas proactivas para fortalecer las defensas. Finalmente, la optimización de recursos gracias a la Inteligencia Artificial es especialmente valiosa

en un contexto de escasez de talento en ciberseguridad. En resumen, la Inteligencia Artificial se ha convertido en una herramienta indispensable para la ciberseguridad moderna, permitiendo a las organizaciones hacer frente a amenazas cada vez más sofisticadas de manera más efectiva y eficiente.

10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

El uso de la Inteligencia Artificial en ciberseguridad plantea desafíos éticos significativos, especialmente en relación con la privacidad y protección de datos personales. Se destaca la necesidad de revisar las políticas de privacidad, implementar técnicas de anonimización y cifrado, y garantizar la transparencia en las decisiones de la Inteligencia Artificial. Además, se debe abordar el riesgo de sesgos y discriminación en los datos de entrenamiento, así como el potencial de uso indebido por parte de ciberdelincuentes. Para mitigar estos riesgos, es esencial establecer políticas claras, promover la transparencia y educar a los profesionales sobre las implicaciones éticas, colaborando con expertos en ética para desarrollar directrices y mejores prácticas que permitan aprovechar de manera segura y confiable el potencial de la Inteligencia Artificial en ciberseguridad.

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?

La participación de un criminólogo resulta fundamental en la creación de estrategias preventivas eficaces de ciberdelitos mediante el uso de la Inteligencia Artificial. Los criminólogos, con su conocimiento del comportamiento delictivo y los factores que impactan en el crimen, ofrecen una perspectiva esencial para analizar y contrarrestar las amenazas digitales. La combinación de la experiencia de los criminólogos con las capacidades de la inteligencia artificial en ciberseguridad permite desarrollar estrategias más robustas y adaptables para prevenir y combatir de manera efectiva los ciberdelitos en un entorno digital en constante cambio.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

El papel de la Inteligencia Artificial en el futuro en la lucha contra los ciberdelitos será fundamental y cada vez más relevante. Con el avance de la tecnología, se espera que la Inteligencia

Artificial desempeñe un papel crucial en la detección temprana de amenazas, la identificación de patrones de comportamiento malicioso, la respuesta automatizada a incidentes de seguridad, y la adaptación continua a las nuevas tácticas de los ciberdelincuentes. Además, se espera que la Inteligencia Artificial contribuya significativamente a la prevención de ataques cibernéticos mediante el análisis predictivo de vulnerabilidades, la optimización de la respuesta a incidentes y la mejora de la eficiencia en la detección proactiva de amenazas en tiempo real. En resumen, se espera que la Inteligencia Artificial sea una herramienta clave en la lucha contra los ciberdelitos, proporcionando capacidades avanzadas para proteger la seguridad digital de individuos y organizaciones en un entorno cada vez más complejo y sofisticado

8.7. Anexo 7. Transcripción de la entrevista 6 (E6)

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

Muy bien, pues mira, actualmente trabajo en una empresa llamada ETRA, en el área nuestra es de nuevas tecnologías, es en la práctica de innovación y desarrollo. Y yo estoy en un departamento de seguridad, tanto seguridad física como seguridad ciber como híbrida, porque al final el mundo es muy pequeño y ambas se solapan muchas veces. En esta parte de proyectos europeos, estoy ahora mismo como líder técnico.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

Alrededor de cinco años.

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Entonces, como líder técnico tenía que organizar y gestionar toda esta parte también, en la parte de ciber normalmente se sigue una llamada, los ataques mitre, que eso identifican un poco las mecánicas o las técnicas que utiliza el que ataca, el ciber atacante, para llevar a cabo su propósito. En este caso el propósito puede ser, pues eso, atacar una máquina o producir ataques o conquistarla o crear un ransomware o un malware o introducir. Bueno, hay un montón de propósitos, estos malévolos.

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?

Si, en teoría, en proyectos de innovación no solo trabajamos sobre esa tabla, sino que vamos un pasito más allá y utilizamos módulos o algoritmos de inteligencia artificial que lo que permiten es predecir hacia dónde quiere ir el atacante, entonces, eso es un poquito la mecánica.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

A través de redes neuronales, pues eso, entrenar algoritmos, entrenar la IA para que pueda predecirte ataques futuros. O sea, normalmente los atacantes siguen unos patrones de ataque, entonces, pues eso, la inserción de un USB, el poder copiar un fichero adentro de la máquina, ciertos pasos ya son indicativos de que algo se puede dar en un futuro. Incluso a lo largo del tiempo,

porque normalmente los ataques, los más elaborados suelen ser en el tiempo. O sea, no es un día realizar todo el ataque, sino que va paulatinamente dejando pequeñas piezas, y entonces, utilizando esas piezas, paulatinamente al final, pues logra un objetivo, que es entrar en la máquina, o conquistarla, o introducir un troyano, malware, y demás.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la Inteligencia Artificial en materia de ciberseguridad?

Hombre, las claves sobre todo es la posesión de los datos, tener históricos de datos de ataques pasados para luego predecir ataques futuros, es la clave. Y sobre todo incorporar a esa nueva inteligencia, o a esa nueva conocimiento, pues todo el bagaje anterior que tiene. Entonces, claro, hay que estar constantemente refrescando todos esos datos

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?
8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la Inteligencia Artificial en su trabajo?

A ver, en teoría debe tener conocimientos informáticos, también conocimientos de las personas, también es un poco de hacer psicología también a veces. Además, no solamente en la parte ciber, a lo mejor todo se puede producir por una parte física, o sea, el que haya alguien entrado en una instalación, el haya insertado un USB, eso es una parte física. Entonces, también hay un debate enorme sobre qué corresponde a lo físico y qué corresponde a lo ciber. Entonces, puede haber ataques que empiecen por lo físico y acaban en un ataque ciber. Y en cuanto a conocimiento, pues eso tiene que saber muy bien cómo están todos los mecanismos de seguridad que existen actualmente. En temas de inteligencia artificial, pues deberías saber cómo están desarrolladas esas inteligencias, aunque parece que todo evoluciona, que poco a poco no necesita un bagaje tan técnico la persona de ciber, porque muchas veces al final ya todo puede ser implementado por otra inteligencia artificial a su vez que te va facilitando esa labor.

9) ¿De qué maneras actuales se utiliza la Inteligencia Artificial para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

Pues mira, justamente relacionado con proyectos europeos. A nivel organizativo, aquí se sigue una ISO, creo que es la 27001, que hay unas pautas muy claras de qué conocimiento debe tener

todo trabajador para que no haya este tipo de ataques. Y entonces mi organización actualmente respeta todas esas a rajatabla. Y bueno, pues existe una multitud de, bueno también hay muchas campañas de concienciación, de cómo el atacante quiere enviar correos fraudulentos o scamming. Hay muchísimas técnicas que a través de concienciación y de educación dentro de nuestra organización, pues los diferentes trabajadores toman conciencia y saben qué tienen que hacer o qué no tienen que hacer. Luego a nivel de, como te he comentado, a nivel de proyectos europeos, el tema de predecir también tenemos mecanismos que son automáticos que ya dentro de la propia organización prevén movimientos anómalos dentro de nuestra propia red.

10) ¿Considera que el uso de la Inteligencia Artificial en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

Bueno, es muy buena pregunta. Actualmente efectivamente hay muchos problemas éticos, legales. Bueno, ahora ha salido la nueva ley europea de inteligencia artificial y bueno, los organismos tienen que estar preparados para poder adecuarse a esas normas y a esas leyes. Y efectivamente, como el concepto dice, la inteligencia artificial intenta simular comportamientos humanos. Entonces, dentro de los comportamientos humanos, dentro de toda esa información, existen sesgos. Y efectivamente esos sesgos hay que intentar neutralizarlos. V.A.C., cuando recibes todos los datos de una gran cantidad de datos o un data set enorme o de Big data, tienes que intentar quitar todos esos sesgos. Como sesgos te puedo poner ejemplos. Había la inteligencia artificial relacionada con entrevistas de trabajo de Amazon, pues eso, sesgaba a la población por edad, la sesgaba por género y por raza. Entonces, claro, eso hay que tener mucho cuidado. Entonces, efectivamente, los datos y porque la población misma tiene esos sesgos, entonces hay que intentar tratarlos y corregirlos

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la Inteligencia Artificial?

Muy bien, pues efectivamente va a ser una herramienta del día a día y seguro que se va a utilizar para multitud de casos o multitud de problemas o combinando información diversa dentro de una escena de un crimen, pues la IA puede a lo mejor ver cosas que el mismo criminólogo no puede ver. Incluso con eventos pasados dentro de la criminología puede haber escenas que tú has incorporado a esa IA, a esa base de datos, y entonces ves dentro de esas escenas a lo mejor hay patrones comunes que luego te permiten resolver de manera efectiva esos casos.

12) ¿Cuál cree que será el papel de la Inteligencia Artificial en el futuro en cuanto a la lucha contra los ciberdelitos?

Pues va a estar presente en todos los organismos, efectivamente. Creo que la propia IA podrá ser capaz de eso, de manera automatizada, prever, resolver problemas, automatizar procesos para corrección de errores o corrección de vulnerabilidades, tanto a nivel organizativo, a nivel de desarrollos de aplicaciones, creo que va a ser todo inteligente artificial.

8.8. Anexo 8. Transcripción de la entrevista 7 (E7)

1) ¿Podría decirme su nombre, nacionalidad y cuál es su posición actual?

Mi nombre es Dalila Mouchaouche, soy francesa y actualmente tengo la posición de Senior Compliance officer en un banco privado de Luxemburgo.

2) ¿Qué experiencia ha tenido en cuanto a la ciberseguridad?

He tenido una experiencia de hace dos años en un banco privado en la protección de oficial de datos.

3) ¿Podría proporcionar una descripción general de qué medidas de ciberseguridad se utilizan actualmente para combatir ciberdelitos?

Hay varias que se aplican actualmente en el entorno bancario y financiero como: Mantener actualizados los sistemas y softwares del banco, impartir formación continua sobre ciberseguridad a los empleados, encriptar los datos y crear copias de seguridad periódicamente, utilizar contraseñas seguras.

4) ¿Está usted al tanto de técnicas de la Inteligencia Artificial que se utilicen para la detección y prevención de amenazas cibernéticas? Si es así, ¿cuáles?

No.

5) ¿Cómo cree que la Inteligencia Artificial puede enfocarse para mejorar los enfoques tradicionales de la ciberseguridad?

Las soluciones de IA pueden identificar datos en la sombra, vigilar las anomalías en el acceso a los datos y alertar a los profesionales de la ciberseguridad sobre posibles amenazas por parte de cualquiera que acceda a los datos o a la información sensible, ahorrando un tiempo valioso en la detección y corrección de problemas en tiempo real.

6) ¿Podría comentarnos cuáles son los desafíos claves que los profesionales tendrán en cuanto a la implementación de la IA en materia de ciberseguridad?

Yo diría que es esencial encontrar el justo equilibrio entre precisión y falsos positivos. Ataques de adversarios: Los ciberdelincuentes pueden intentar manipular los sistemas de IA mediante ataques de adversarios. Es esencial implementar mecanismos de defensa sólidos contra este tipo de ataques.

7) ¿Tiene algún ejemplo de escenarios reales en donde una solución de ciberseguridad ha tenido éxito?

   No tengo ejemplos específicos

8) ¿Qué habilidades considera que son necesarias para que los profesionales aprovechen eficazmente las tecnologías de la IA en su trabajo?

Conocimientos técnicos: Ciencia de datos y análisis de datos, Python R y otros lenguajes de programación, matemáticas y estadística, ingeniería rápida, computación en la nube, seguridad y cumplimiento normativo

9) ¿De qué maneras actuales se utiliza la IA para obtener reducir el impacto de los ciberataques dentro de su ámbito laboral?

Las soluciones de IA pueden identificar datos en la sombra, vigilar las anomalías en el acceso a los datos y alertar a los profesionales de la ciberseguridad sobre posibles amenazas por parte de cualquiera que acceda a los datos o a la información sensible, ahorrando un tiempo valioso en la detección y corrección de problemas en tiempo real.

10) ¿Considera que el uso de la IA en el ámbito de la ciberseguridad podría traer problemas éticos, especialmente en cuanto a la privacidad y protección de datos?

    Sí, y no puede cumplir el GDPR.

11) ¿Considera que el rol de un criminólogo es esencial para poder crear estrategias preventivas de ciberdelitos con el uso de la IA?

    Si.

12) ¿Cuál cree que será el papel de la IA en el futuro en cuanto a la lucha contra los ciberdelitos?

Está revolucionando nuestra forma de concebir la ciberseguridad. La IA es más rápida que cualquier ser humano a la hora de analizar, detectar, supervisar y responder a las ciber amenazas.

Puede rastrear conjuntos de datos masivos para detectar patrones que indiquen una amenaza o un punto débil en las ciberdefensas en un tiempo récord.

8.9. Anexo 9. Consentimiento Informado.

HOJA DE INFORMACIÓN

Título del TFG: El Papel de la Inteligencia Artificial en la Prevención y Lucha contra Ciberdelitos

Promotor: Universidad Europea de Valencia

Investigador: Valery Masi

Centro: Universidad Europea de Valencia

Nos dirigimos a usted para informarle sobre un estudio de investigación que se va a realizar en la Universidad Europea de Valencia, en el cual se le invita a participar. Este documento tiene por objeto que usted reciba la información correcta y necesaria para evaluar si quiere o no participar en el estudio. A continuación, le explicaremos de forma detallada todos los objetivos, beneficios y posibles riesgos del estudio. Si usted tiene alguna duda tras leer las siguientes aclaraciones, nosotros estaremos a su disposición para aclararle las posibles dudas. Finalmente, usted puede consultar su participación con las personas que considere oportuno.

¿Cuál es el objetivo de este estudio? El objetivo principal del presente Trabajo de Fin de Grado será investigar y analizar las distintas funciones que la Inteligencia Artificial podrá tener en la prevención de los ciberdelitos, al igual que sus funciones con relación a la investigación de estos.

RESUMEN DEL ESTUDIO: A medida que el mundo digital va creciendo, los ciber delitos suponen amenazas cada vez más importantes en la sociedad, por lo cual, se deben tomar medidas para prevenir estos delitos.

La Inteligencia Artificial, es una herramienta tecnológica con gran potencial para reforzar la ciberseguridad, permitiendo ser utilizada para la detección de amenazas. Una investigación en este ámbito será de relevante interés, ya que permitirá demostrar la urgencia de nuevas soluciones innovadoras en la lucha del ciber delito, resaltando el importante papel de la Inteligencia Artificial en la prevención y resolución de estos.

PARTICIPACIÓN VOLUNTARIA Y RETIRADA DEL ESTUDIO: La participación en este estudio es voluntaria, por lo que puede decidir no participar. En caso de que decida participar, puede retirar su consentimiento en cualquier momento. En caso de que usted decidiera abandonar el estudio, puede hacerlo permitiendo el uso de los datos obtenidos hasta ese momento para la finalidad del estudio, o si fuera su voluntad, todos los registros y datos serán borrados de los ficheros informáticos.

¿Quién puede participar? El estudio se realizará en voluntarios adultos. El reclutamiento de los participantes será a través de solicitud de participación. Si acepta participar, usted va a formar parte de un estudio en el que se incluirán 4 profesionales en materia de ciberseguridad.

¿Cuáles son los posibles beneficios y riesgos derivados de mi participación? Es posible que usted no obtenga ningún beneficio directo por participar en el estudio. No obstante, se prevé que la información que se obtenga pueda beneficiar en un futuro de este ámbito y pueda contribuir a realizar un cambio de pensamiento en el profesional de la criminología. Al finalizar la investigación podrá ser informado, si lo desea, sobre los principales resultados y conclusiones generales del estudio.

¿Quién tiene acceso a mis datos personales y como se protegen? El tratamiento, la comunicación y la cesión de los datos de carácter personal de todos los sujetos participantes se ajustará a lo dispuesto en la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales.

¿Recibiré algún tipo de compensación económica? No se prevé ningún tipo de compensación económica durante el estudio. Si bien, su participación en el estudio no le supondrá ningún gasto.

¿Quién financia esta investigación? El promotor del estudio es el responsable de gestionar la financiación de este. Para la realización del estudio, el promotor de este ha firmado un contrato con el centro donde se va a realizar.

OTRA INFORMACIÓN RELEVANTE: Si usted decide retirar el consentimiento para participar en este estudio, ningún dato nuevo será añadido a la base de datos y puede exigir la destrucción de sus datos y/o de todos los registros identificables, previamente retenidos, para evitar la realización de otros análisis. También debe saber que puede ser excluido del estudio si los investigadores del

estudio lo consideran oportuno, ya sea por motivos de seguridad, por cualquier acontecimiento adverso que se produzca o porque consideren que no está cumpliendo con los procedimientos establecidos. En cualquiera de los casos, usted recibirá una explicación adecuada del motivo que ha ocasionado su retirada del estudio.

CALIDAD CIENTÍFICA Y REQUERIMIENTOS ÉTICOS DEL ESTUDIO: Este estudio ha sido sometido al registro de la Comisión de la Investigación de la Universidad Europea de Madrid, Valencia y Canarias, que vela por la calidad científica de los proyectos de investigación que se llevan a cabo en el centro.

PREGUNTAS: Llegando este momento le damos la oportunidad de que, si no lo ha hecho antes, haga las preguntas que considere oportunas. El equipo investigador le responderá lo mejor que sea posible.

INVESTIGADORES DEL ESTUDIO: Si tiene alguna duda sobre algún aspecto del estudio o le gustaría comentar algún aspecto de esta información, por favor no deje de preguntar a los miembros del equipo investigador: Valery Masi Legidos. En caso de que una vez leída esta información y aclaradas las dudas decida participar en el estudio, deberá firmar su consentimiento informado. Este estudio ha sido registrado por la Comisión de la Investigación de la Universidad Europea de Madrid, Valencia y Canarias.

CONSENTIMIENTO INFORMADO:

D./Dª. _____, de____ años, con DNI_____ y domicilio en _____. He recibido una explicación satisfactoria sobre el procedimiento del estudio, su finalidad, riesgos, beneficios y alternativas. He quedado satisfecho/a con la información recibida, la he comprendido, se me han respondido todas mis dudas y comprendo que mi participación es voluntaria. Presto mi consentimiento para el procedimiento propuesto y conozco mi derecho a retirarlo cuando lo desee, con la única obligación de informar sobre mi decisión al investigador/a responsable del estudio.

En Valencia, a día_____ de _____ de _____.

_____ _____

Firma del investigador/a Firma y Nº de DNI del participante