INCIDENCIA DE LA (IA) INTELIGENCIA ARTIFICIAL PARA LA PREVENCIÓN DE ATAQUES DE SEGURIDAD INFORMÁTICA USANDO LA TÉCNICA DE INGENIERÍA SOCIAL

LEONARDO ANDRES CIFUENTES ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2024

INCIDENCIA DE LA (IA) INTELIGENCIA ARTIFICIAL PARA LA PREVENCIÓN DE ATAQUES DE SEGURIDAD INFORMÁTICA USANDO LA TÉCNICA DE INGENIERÍA SOCIAL

LEONARDO ANDRES CIFUENTES ROJAS

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

Director
Ing. Joel Carroll Vargas P.hD(c)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2024

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Florencia Caquetá, 20 de Mayo de 2024

DEDICATORIA

Esta monografía se encuentra dedicada primeramente a Dios por permitirnos realizar nuestros sueños anhelados a lo largo de la vida buscando siempre la superación personal, aun cuando las circunstancias se encuentren en contra, lo que nos lleva atravesar caminos y momentos difíciles, pero que gracias a la constancia, disciplina y dedicación se derrumban grandes barreras, que permiten al ser humano sobreponerse y salir avante cumpliendo sus sueños y de poso aportar en algo en la trasformando la humanidad para que cada día sea más consiente; además quiero expresar un sentido de agradecimiento para mi familia que muchas veces sacrifican espacios de felicidad, solo para permitirme avanzar en las actividades académicas que los enorgullecen.

AGRADECIMIENTOS

Con el desarrollo de esta esta monografía quiero agradecer especialmente a todas las personas que apoyaron y participaron en el proceso investigativo, destacando primeramente a mi familia por la paciencia y a los directivos, docentes, estudiantes y comunidad académica de la Universidad Nacional Abierta y a Distancia UNAD, en especial al equipo que conforma la Escuela de Ciencias Básicas Tecnología e Ingeniería de la Especialización en Seguridad Informática y particularmente al director de la Monografía por el apoyo y las asesorías correctas en este camino al éxito.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

INTELIGENCIA ARTIFICIAL (IA): de acuerdo con Meseguer González, P. y López de Mántaras Badia, se considera La inteligencia artificial es la Ciencia e ingeniería que permite diseñar y programar ordenadores de forma que realicen tareas que requieren inteligencia.

EL APRENDIZAJE AUTOMÁTICO (ML): según Kaspersky 2022 describe como la utilización de comportamientos "existentes, lo que permite la toma de decisiones basadas en datos y conclusiones anteriores. La intervención humana sigue siendo necesaria para realizar algunos cambios. Es probable que el aprendizaje automático sea la disciplina de ciberseguridad de la IA más importante hasta la fecha"[1].

INGENIERÍA SOCIAL: según el instituto nacional de seguridad INCIBE[2] argumenta que la ingeniería social basa su comportamiento en una premisa básica: los humanos son más fáciles de controlar que las máquinas. Este tipo de ataque utiliza técnicas de manipulación psicológica para que los usuarios revelen información confidencial o realicen cualquier acción que pueda beneficiar al ciberdelincuente.

HUNTING: este se basa sobre el principio de infectar muchos usuarios a través de la sola comunicación, por lo cual se identifica principalmente en campañas de phishing, como los realizados contra entidades energéticas o bancarias, También son utilizados en ataques cuyo objetivo es realizar una campaña de infección por malware, como las que se llevaron a cabo para realizar ataques de ransonware.

CIBERSEGURIDAD: Los autores Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L[3], definen de manera precisa que la ciber• seguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de

[1] KASPERSKY, 2022. La IA y el aprendizaje automático en la ciberseguridad: cómo determinarán el futuro. latam.kaspersky.com [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity.

[2] Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. INCIBE [en línea], 2019. [Consulta: 19 marzo 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.

[3] Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad.. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/bibliotecaueb/titulos/172144

la información vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, em• presa u organización.

PHISHING: Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o “suplanta su identidad”) a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

PHARMING: El pharming, una combinación de los términos "phishing" y "farming", es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. El pharming aprovecha los principios con los que funciona la navegación por Internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de Internet, como www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión.

VISHING: El Vishing (abreviatura de phishing por voz) es un tipo de estafa que se realiza a través de llamadas telefónicas con el objetivo de obtener los datos personales o bancarios de una persona. Los ciberdelincuentes suplantan la identidad de un tercero (banco, empresa o persona) con la finalidad de conseguir que la víctima proporcione información privada o sensible, que pueda servirle de utilidad al defraudador para cometer ciberdelitos. Generalmente, el ciberdelincuente le informa a su víctima sobre “posibles” cargos que se están realizando a alguna de sus cuentas bancarias.

VECTOR DE ATAQUE: Los vectores de ataque en ciberseguridad son las formas o medios que permiten a ciberdelincuentes transmitir códigos maliciosos, con el propósito de obtener beneficios económicos.

ANÁLISIS DIGITAL FORENSE: El análisis forense digital es una rama de la policía científica centrada en la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos.

RESUMEN

A través de la presente monografía, se busca analizar la importancia de la inteligencia artificial para disminuir la cantidad de ocurrencia de ataques por ingeniería social, que suceden a menudo tanto para los usuarios corporativos como para la línea particular o individual, es por esta razón que mediante la consulta de diferentes fuentes bibliográficas, se identifica la importancia de aplicar inteligencia artificial como una de las herramientas modernas, para combatir la ocurrencia de ciberdelitos, los cuales según diversas fuentes, cada día se masifican colocando en riesgo a los usuarios tecnológicos, en el cual hoy en día existe todo un ecosistema digital de Big Data que es difícil controlar por las capacidades humanas, y por ende esta propuesta se basa en comprender la efectividad automatización de procesos a partir de la predicción y el aprendizaje artificial como medida de protección para la información y los datos.

En ese contexto, el documento se centra en identificar, los diferentes aportes de la inteligencia artificial para la prevención de ataques por ingeniería social, contribuyendo al cambio del paradigma de los antivirus reactivos, los cuales se activan una vez se materializa la amenaza, para dar paso a una nueva generación de antivirus proactivos con los cuales se anticipan a la ocurrencia alimentados por los algoritmos y la conectividad de la inteligencia artificial; por otra parte, una de las conclusiones y resultados más importantes a la que se llega con el abordaje metodológico del presente estudio, se evidencia en reconocer en que la inteligencia artificial es una tecnología emergente, de las cual hasta el momento existen pocos estudios avanzados en materia de cibercrimen, por lo tanto la presente pieza documental sirve como pilar o referente para abordar nuevos estudios desde la academia o a través de la investigación científica que adelante el estado y sus instituciones para proteger los intentares a una sociedad, mayormente usuarias de las tecnologías y dispositivos electrónicos.

Palabras Claves: Ingeniería social, inteligencia artificial, ciberseguridad, cibercrimen, ataques informáticos.

ABSTRACT

This text focuses on the significance of artificial intelligence in the fight against social engineering attacks, which are a type of cyberattack in which criminals deceive individuals to obtain confidential information. These attacks pose a threat to both corporate and individual users.

The monograph argues that artificial intelligence is a crucial tool in preventing these attacks as it can analyze suspicious patterns and behaviors in real-time, which is difficult to achieve with human capabilities alone. Furthermore, it highlights that artificial intelligence technology can predict and anticipate threats before they occur, as opposed to traditional antivirus programs that only react after a threat has materialized.

The text also emphasizes that while artificial intelligence is an emerging technology in the field of cybersecurity, its potential is significant. Although there are few advanced studies on the subject at present, it is expected to become an important research area. The monograph serves as a solid foundation for future studies in this field, both in the academic and research conducted by governmental and academic entities.

In summary, the text highlights the importance of artificial intelligence in preventing social engineering attacks and suggests that this technology will play a pivotal role in the future of cybersecurity.

Keywords: Social engineering, artificial intelligence, cybersecurity, cybercrime, computer attacks.

INTRODUCCIÓN

La ciberseguridad se ha convertido para la humanidad como una área indispensable, en razón al progreso vertiginoso en el cual nos enfrentamos día a día en el cual cada vez, los seres humanos son más dependientes de la tecnología, la cual gracias a sus avances en los últimos tiempos, permiten la ejecución de tareas rutinarias por el ser humano que con el simple hecho de ejecutar una acción en el dispositivo móvil desencadena toda una interconexión global con respuestas instantáneas, tareas que en la antigüedad tardan días y hasta años para lograse; pero esta dependencia aunque es una ventaja también pude ser una desventaja ya que para el momento existen millones de bases de datos en las cuales reposan nuestra información y datos personales, económicos, médicos entre otros que deben estar salvaguardados en razón a que hacen parte de la vida del ser humano y que al estar manos incorrectas podría generar dificultades no solo a nivel particulares si no a nivel corporativo o empresarial, es así que diferentes fuentes y agencias gubernamentales como INTERPOL, EUROPOL , NACIONES UNIDAS, FBI, OEA publican cifras sobre el crecimiento exponencial de ataques informáticos con el fin de lograr apoderase de todo tipo de información y datos para su comercialización o provecho propio.

En concordancia la presente monografía tiene como finalidad, identificar la incidencia de las inteligencia artificial como herramienta para controlar y disminuir los ataque ocasionados por ingeniería social, mediate una revisión de bibliografía sistemática en la cual se analicen las aplicaciones de esta herramienta, así como el impacto que se genera para tres grupos de la sociedad la ocurrencia de una ataque por ingeniería social, para logra generar recomendaciones sobre la validez y aplicabilidad de esta herramienta, en el entendido que gracias a sus características pude tener algunas implicaciones en su uso por el alcance de aprendizaje que llega alcanzar influyendo en el desarrollo de la humanidad.

De la misma manera se busca generar, conciencia en la sociedad sobre la responsabilidad y uso adecuado de la tecnología, en el cual el usuario es la primera barrera de protección siempre y cuando apliqué todas las recomendaciones suministradas por las entidades en el campo de la ciberseguridad, además de utilizar un aliado para su protección como lo puede ser la inteligencia artificial que en cierto momento pude llegar a comprender que se está siendo víctima de un ataque por esta modalidad.

1. DEFINICIÓN DEL PROBLEMA

1. ANTECEDENTES DEL PROBLEMA

Según lo afirma Naciones Unidas a través de la Agencia Digital para América Latina y el Caribe Elac 2022, en el cual mencionan que el consumo digital ha crecido de manera exponencial principalmente en la última década, hasta llegar el punto de volverse indispensable para la vida de cada persona, generando cada día mayor dependencia de los sistemas de información y de las bases de datos, gracias a su versatilidad que permite optimizar diferentes tareas que a diario realizan las personas ya sea para su uso personal o a nivel empresarial, que anteriormente demandaban de tiempo y gasto de recursos de todo tipo[4].

Este crecimiento trae consigo peligros para la información y los datos, que sin duda alguna a medida que el ecosistema digital se expande también surgen nuevas formas de afectar la seguridad de la información, por parte de los ciberdelincuentes que constantemente están innovando en sus estrategias para burlar las barreras y controles existentes, que de acuerdo con la cámara colombiana de informática el comportamiento del cibercrimen en Colombia, se ve reflejado en el número de denuncias instauradas ante el sistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN) a través del aplicativo a denunciar, identificando que al finalizar el mes de noviembre del 2021 se habían registrado 46.527 denuncias por distintos delitos lo que equivale a un incremento del 21% respecto al 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021[5], es decir sin contabilizar el año de pandemia, el incremento alcanzó un 107% acumulado entre el incremento suscitado durante el 2020 y el aumento continuo durante el 2021 , de las cuales la mayoría de actuaciones delictivas son cometidas a través de modalidades de engaño o lo que se conoce como ingeniería social, en donde luego de analizar diferentes comportamientos del ser humano como el respeto a la autoridad, voluntad de ayudar, temor a perder un servicio, respeto social entre otros que conllevan a buscar la forma de perpetrar el objetivo para apoderarse del control de la información y los datos obteniendo muchas veces un beneficio económico.

[4] Comisión Económica para América Latina y el Caribe (CEPAL), Tecnologías digitales para un nuevo futuro (LC/TS.2021/43), Santiago, 2021

[5] Bautista García, Fredy. Tendencias del cibercrimen 2021 -2022 Nuevas amenazas al comercio electrónico, Diciembre de 2021, vol 1, p 9-10. ISBN

El problema surge principalmente, en que debido a la robustes de información y grandes bases de datos de almacenamiento, se hace imposible realizar controles manuales y dedicados principalmente a los comportamientos de los usuarios finales, quienes terminan en gran medida facilitando la operación del ciber delincuente, el cual plantea diversas modalidades y modus operandi, para lograr llevar a cabo su vector de ataque, que en muchos de los casos termina por apodarse de aquella información valiosa para la persona o para le organización, hasta el punto de cobrar por el rescate de la misma o en el peor de los casos afectar la infraestructura critica de un estado dejándola fuera de servicio lo que afecta a millones de usuarios.

A nivel de Latinoamérica el panorama no es distinto en materia de ciberseguridad, dado que el estudio realizado por la Organización de Estados Americanos OEA, segura mediante el estudio realizado en el año 2019 enfocado a unos de los principales objetivos de ataque como es el sector bancario el estudio arrojo que con relación a la "gestión, respuesta y recuperación ante incidentes de seguridad digital, la mayor adopción de aplicaciones web y móviles en el sector bancario en la región de América latina y el caribe, ha hecho que la industria sea propensa a un incremento en los ataques cibernéticos avanzados. Es así que la materialización de incidentes digitales se presenta en más de un tercio de las entidades en la región. Por lo cual es imperativo que las entidades crediticias medianas y pequeñas actualicen sus estrategias de gestión, respuesta y recuperación ante incidentes y ejecuten periódicamente evaluaciones de madurez junto con las acciones correspondientes derivadas, debido a que Los eventos más comunes fueron el código malicioso o malware con una equivalencia del 80%, seguido de la violación de políticas de escritorio con un total de 63% y en tercer puesto el phishing dirigido para tener acceso a sistemas del banco (57% del total de bancos analizados; pero el estudio también revela que los eventos como el phishing, la ingeniería social, y el software espía (malware o troyanos) fueron los más frecuentes contra sus usuarios de servicios financieros"[6], de ahí la necesidad de fomentar la utilización de tecnologías emergentes para combatir estos comportamiento de la seguridad digital.

[6] *ORGANIZACIÓN DE ESTADOS AMERICANOS OEA. desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. Primera Edición. San José de Costa Rica. OEA ASOBANCARIA. 2019. 172 p.*

Por ultimo un aspecto determinante en el crecimiento exponencial de los delitos informáticos en especial por ingeniería social, lo constituyo la pandemia con un crecimiento acelerado del problema, debido a dependencia digital para realizar actividades laborales como el teletrabajo y la educación virtual entre otras actividades cotidianas, aspecto que lo ratificó la octava edición de la con la Conferencia de INTERPOL y Europol sobre Ciberdelincuencia realizada para el día 06 de octubre de 2020 de manera virtual en cual se menciona que son seis ciberamenazas mundiales, que van desde el phishing hasta el ransonware, de las cuales se propone la implementación de tecnologías emergentes así como el trabajo articulado por las organización de dedicadas en la lucha contra el cibercrimen.[7]

2. FORMULACIÓN DEL PROBLEMA

¿Cuáles son los mecanismos y estrategias específicas de la Inteligencia Artificial (IA) que permiten una contribución en la prevención y reducción de la incidencia de vectores de ataques de seguridad informática a través de la técnica de ingeniería social?

[7] *8a Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: «Media humanidad está en peligro». Interpol.int [en línea], 2022, Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/8a-Conferencia-de-INTERPOL-y-Europol-sobre-Ciberdelincuencia-Media-humanidad-esta-en-peligro.*

2 JUSTIFICACIÓN

De acuerdo con el informe presentado por SAFE - Tendencias del Cibercrimen 2021 – 2022 emitido por el equipo Tic Tac de la Cámara Colombia de Informática [8] explican que el comportamiento actual de los ciberdelitos obedece a la proliferación del uso de tecnologías para realizar actividades sencillas y complejas para todas personas, que gracias a factores como la pandemia agudizó el uso masivo de sistemas de información como por ejemplo el teletrabajo, operaciones bancarias, contenido streaming, capacitación, conferencias entre otros que han conllevado a que día a día se desarrollen nuevas y mejores formas de afrontar la realidad desde el ciberespacio; paralelamente este auge convierte a los usuarios en ciberdependientes, teniendo en cuenta que el avance ha llegado al punto de capturas datos biométricos para su funcionamiento y centralización de múltiples apps y sistemas de información que se encargan de la administración de los datos, pero que en el momento de presentar fallas el usuario queda totalmente imposibilitado de efectuar actividades en razón a la dependencias tecnológica.

Los mismos autores establecen que “el ciberdelito se ha convertido en la tipología criminal de mayor crecimiento en Colombia durante los últimos tres años; impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico cuyo crecimiento alcanzó el 59.4% en las transacciones durante el periodo de cuanterentena obligatoria y del 35% durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE”[9], es por ello que según los afirma Rincón Nuñez, P. M. (2023 p 15) “En Colombia, la situación en cuanto a los ataques de ingeniería social va en aumento, de acuerdo con el informe publicado por la Cámara Colombiana de Informática y Telecomunicaciones (2019), Tendencias cibercrimen Colombia 2019-2020, los incidentes que más se reportan en el país son: Phishing, 42%; suplantación de identidad, 28%; envío de malware, 14%; y los fraudes, 16%. Según este informe, la tendencia para el año 2020 en Colombia es que este tipo de ataques de ingeniería social aumenten, haciendo uso de BEC (Business Email Compromise) basado en Deepfake InterSedes, (técnica de inteligencia artificial que permite la edición de videos y audios falsos de personas que hacen pasar por reales), Botnets para difusión de correos extorsivos, uso de perfiles falsos para

[8] Informe SAFE - Tendencias del Cibercrimen 2021 - 2022. Cámara Colombiana de informática. Etipo Tic Tac. Bogotá. 2022. Pag 27

[9] Ibid

difundir malware y tráfico de datos robados en Darknet”[10]; por esta razón y de acuerdo a diferentes fuentes bibliográficas consultadas existe la imperiosa necesidad de adelantar investigaciones en materia de seguridad informática, para evitar ataques de seguridad informática que inician desde la ingeniería social, con el fin de obtener provecho mediante la información recolectada en el vector de engaño, que posteriormente les es útil para obtener el acceso el acceso total al objetivo planteado; es por lo cual se requiere conocer el alcance de múltiples herramientas que existen hoy en día para contrarrestar toda la todas aquellas tendencias del cibercrimen, entre ellas contamos con la (IA) o mejor conocida como la inteligencias artificial, la cual a partir de imitar la inteligencia humana pueden llegar evitar distintos ataques, por ende es necesario conocer desde diferentes autores cual es el estado del arte en esta temática moderna para generar un documento de lineamientos a futuras investigaciones en la materia.

Es nuestra responsabilidad como comunidad académica generar bibliografía responsable y crear profundizaciones en temáticas emergentes como lo es la inteligencia artificial que de acuerdo con (Kardoudi 2023) explica que “La IA avanzada podría representar un cambio profundo en la historia de la vida en la Tierra, y debería planificarse y gestionarse con el cuidado y los recursos correspondientes”[11] por lo que han sido poco exploradas, como lo es el caso de la utilización de la inteligencia artificial para contrarrestar los diferentes vectores de ataque por ingeniería social, logrando conocer su alcance a partir de análisis de masas bibliográficas y buenas prácticas del sector de la seguridad de la información.

Es gracias a la necesidad de proteger al activo más valioso, que hoy en día existe para los seres humanos, y es su información privada y sus datos personales, puesto que de ser accedidos de manera ilícita, generan la violación a la intimidad, un derecho fundamental que tienen todos los seres humanos del cual Colombia no es diferente, razón por la cual, se fundamenta la necesidad de elaborar estudios que permitan que permitan generar argumentos sólidos para la creación de estrategias de protección a los ciber usuarios.

[10] Rincón Nuñez, P. M. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. InterSedes, 24(49), 120-150.

[11] KARDOUDI, O., 2023. Expertos internacionales piden parar el desarrollo de la inteligencia artificial. elconfidencial.com [en línea]. [Consulta: 15 mayo 2023]. Disponible en: https://www.elconfidencial.com/tecnologia/novaceno/2023-03-29/inteligencia-artificial-chatgpt-regulacion-expertos_3601529/.

3 OBJETIVOS

3. OBJETIVOS GENERAL

Analizar la incidencia de la Inteligencia Artificial (AI), para la prevención de ataques de seguridad informática mediate la técnica de ingeniería social, por medio de una revisión sistemática de bibliografías y publicaciones, que permiten conocer una alternativa moderna, en materia de seguridad informática aplicable a entornos personales y corporativos.

4. OBJETIVOS ESPECÍFICOS

- Examinar las características de la inteligencia artificial, aplicada en procesos de prevención para ataques de seguridad informática realizados mediante la técnica de ingeniería social, que permitan la implementación como una herramienta moderna y alternativa en la seguridad informática

- Investigar por medio de una revisión sistemática de literatura y publicaciones las vulnerabilidades, riesgos, amenazas e impactos, de los ataques realizados por ingeniería social y sus diferentes consecuencias para la información y los datos de manera personal o corporativo.

- Describir el aporte que realiza la defensa proactiva basada en inteligencia artificial, como herramienta de anticipación, ante la ocurrencia de circuitos de ataque de seguridad informática, que incorporen la ingeniería social como método para afectar las dimensiones de la información y los datos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En esta sección de la monografía, se elaborará una revisión bibliográfica de las diferentes teorías, a partir de las cuales se sustenta el funcionamiento de la inteligencia artificial, así como la ingeniería social.

El proceso de aprendizaje de la inteligencia artificial: La inteligencia artificial hoy en día es una las herramientas mayormente utilizadas para el desarrollo tecnológico en especial para el área de la robótica basada en la teoría propuesta por Alan Turing y mencionada por Meseguer González, P. ; López De Mántaras Badia, R, en el cual describen que el prestigioso matemático afirmo que, en lugar de intentar emular mediante una maquina la mente de un adulto, quizá sería más factible intentar emular la mente de un niño y luego someter a la maquina a un proceso de aprendizaje que diera lugar a un desarrollo cognitivo de dicha mente hasta alcanzar el equivalente de una mente adulta[12], principio en el cual se basa la inteligencia artificial dado que se encarga de aprender mediante métodos probalísticos sobre diferentes comportamientos para lograr una predicción, como lo hace un ser vivo entre ellos el ser humano y así remplazar tareas cotidianas, pero que sin duda alguna estas actividades son orientadas a grandes cálculos matemáticos.

4.1.2 Paradigmas de la inteligencia artificial: Lledo Yague, F. (Dir.), Ortuzar, B. mencionan que el autor de los dos grandes paradigmas de la inteligencia artificial fue el señor Alan Turing, el cual nombro al primero como el paradigma simbólico, en donde básicamente considera los sistemas inteligentes como solucionadores de problemas que reciben datos y proporcionan una respuesta a partir de dichos datos. Es decir, para el paradigma simbólico lo relevante de un sistema inteligente es la capacidad de proporcionar una respuesta a un problema dado; por otro lado, implementa un segundo paradigma denominado conexionista, que considera que dado que solo conocemos un sistema inteligente natural, nuestro cerebro, cualquier sistema inteligente artificial debe imitarlo; al surgir estos dos grandes modelos se logra interpretar que existe la combinación entre la teoría y la aplicación que dio origen a la computacional o soft computing después de la mitad del siglo XX[13].

4.1.3 El arte de la manipulación humana: Es denominada a la ingeniería social como un arte dado que según el Dr. Robert Cialdini existen 6[14] principios

[12] MESEGUER GONZÁLEZ, P. ; LÓPEZ DE MÁNTARAS BADIA, R. **Inteligencia artificial**. ed. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2017. 159 p.

[13] LLEDO YAGUE, F. (Dir.), ORTUZAR, B. (Dir.) ; MONJE BALMASEDA, O. (Dir.). La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0: los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes. ed. Madrid: Dykinson, 2021. 673 p.

[14] ROBERT B. CIALDINI, Influence: The Psychology of Persuasion. Harper Collins Publ. Estados Unidos, 2021. 592p. ISBN 9780063136892

fundamentales para persuadir a una persona el primero de ellos se trata de la reciprocidad, en el cual el ser humano una vez le hagan un favor se siente con la obligación de devolver ese favor, el segundo consiste en la coherencia, compromiso y consistencia, lo que significa que toda persona basa en sus principios siempre va a respetar esos orígenes por lo que cuando se encuentran ante una situación evalúan esos principios y si los mismos son coherentes y consistentes actúan, seguidamente encontramos la aprobación social significa que lo que hacen otras personas lo puedo hacer cualquier persona y no va tener rechazo porque es algo normal en la sociedad, otro de los principios es la autoridad, este básicamente se aplica por que las personas tienen a ser persuadidas cuando sienten que es una autoridad la que les está hablando y ordenando, de la misma manera la simpatía es un principio fundamental ya que a partir del cual se puede lograr isopraxismo toda vez que la persona es más propensa a realizar una actividad cuando la persona del otro lado le parece más simpática u agradable y por último la escasez el cual va de la mano con la necesidad de las personas generándoles sensaciones de insolvencia y demás, Los anteriores principios son elementales para el desarrollo de la ingeniería social, en razón a que una persona experta en la utilización de los mismos puede lograr conseguir la información necesaria para llevar a cabo un ataque,

4.1.4 ESCUELAS DE LA INTELIGENCIA ARTIFICIAL: a lo largo de la historia se han formado las bases y los principios de la inteligencia artificial, basándose principalmente en dos escuelas expuestas a continuación:

4.1.4.1 **Inteligencia artificial convencional**: Esta escuela es de tipo simbólico deductiva, y se basa en la aplicación del análisis formal con la presencia de la estadística de acuerdo con los comportamientos del ser humano es decir, es ejecutada con base a la experiencia y el aprendizaje de las personas, porques se fundamenta en el razonamiento basado en casos y sistemas expertos que provienen de un conocimiento previo; de la misma manera este tipo de escuela incorpora la IA basada en comportamientos que permiten predecir y autorregularse, lo anterior con el fin de tomar las decisiones más acertadas de acuerdo con el problema planteado como si lo realizara un ser humano experto.

4.1.4.2 **Inteligencia artificial computacional**: por otro lado, tenemos este tipo de inteligencia artificial que se basa en el simbolismo inductivo, y su aprendizaje está basado de manera interactiva basado en datos empíricos y diferentes principios en los cuales se basa el comportamiento de la naturaleza humana por eso se utilizan métodos para lograr un aprendizaje lógico y coherente.

5 MARCO CONCEPTUAL

Ingeniería social: consiste básicamente en el acto de manipular a una persona o varias personas utilizando diferentes técnicas psicológicas y habilidades sociales para cumplir metas específicas ya sea de manera presencial o remota. Cuya finalidad es la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo físico o activo de información), pudiendo ser o no del interés de la persona objetivo, por tal razón el objetivo primordial es la obtención de activos en provecho propio o de un tercero a finde causar afectaciones principalmente en los sistemas informáticos"[15].

Ingeniería Social No Presencial: En esta actividad el ingeniero social no se involucra de forma presencial, sino que se comunica mediante voz, de forma digital o comunicación escrita por medio físico con el objetivo.

La ingeniería social no presencial se divide en 3 tipos:

Comunicación por voz: conocido como Vishing, técnica en el que se busca manipular al objetivo solo usando la voz, para esta técnica se requiere elaborar un guion o ser espontaneo si se tiene experiencia y facilidad de realizarlo.

Comunicación por medios digitales: en este tipo de comunicación se realiza solo utilizando los medios digitales, como, por ejemplo, correos electrónicos, redes sociales, chat entre otros.

Comunicación escrita por medios físicos: este tipo de técnica se busca manipular al objetivo con regalos o cartas físicas.

Ingeniería Social Presencial: El ingeniero social se involucre e interactúe con el objetivo cara a cara; para realizar este tipo de trabajo de forma exitosa se debe de conocer la mayor cantidad posible de información sobre el objetivo en combinación de técnicas, como, por ejemplo, la elaboración de un buen "pretexting" (es el acto de crear y utilizar una identidad y/o escenario con el objetivo de obtener algo, en la mayoría de casos es conseguir información confidencial), también es necesario saber utilizar la lectura del lenguaje corporal, establecer confianza, saber empatizar, ser persuasivo, etc[16].

---

[15] Ingeniería Social: Corrompiendo la mente humana | Revista. Seguridad. Unam.mx [en línea], 2018. [Consulta: 31 octubre 2022]. Disponible en:https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana.

[16] TAHIRI DIKOVEC, 2019. Ingeniería Social: el arte de la manipulación humana - Tahiri Dikovec. Tahiri Dikovec [en línea]. [Consulta: 31 octubre 2022]. Disponible en: https://tahiridikovec.com/ingenieria-social-el-arte-de-la-manipulacion-humana/#:~:text=Como%20he%20comentado%2C%20la%20ingenier%C3%ADa,se%20comunican%20directamente%20entre%20s%C3%AD..

Inteligencia Artificial: “La inteligencia artificial es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear.

La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos.

Los sistemas de IA son capaces de adaptar su comportamiento en cierta medida, analizar los efectos de acciones previas y de trabajar de manera autónoma”[17].

Machine Learning: Se trata de una disciplina científica involucrado directamente con la Inteligencia Artificial que su único fin es la creación de sistemas que tienen la capacidad de aprender de manera automática. Lo que significa que está en la capacidad de reconocer patrones inmersos en millones de datos, facultad que le permite predecir diferentes comportamientos, lo que conllevan a una evolución a lo largo del tiempo, ya que el sistema mejora por sí solo, sin la intervención del ser humano que visto desde un sentido crítico es bueno pero que al analizarlo en detalle podrá traer consecuencias no muy buenas para la humanidad.

Aprendizaje automático: Dentro de los tipos de inteligencia artificial y de acuerdo con threepoints contamos con el aprendizaje automático el cual es uno de los tipos de inteligencia artificial, con el que más estamos familiarizados, el cual se basa en la capacidad que un software o dispositivo tiene de aprender por su cuenta. El aprendizaje automático sigue tres pasos fundamentales, como cualquier otro método: aprendizaje, entrenamiento y resultados[18].

Aprendizaje profundo: El mismo portal en internet menciona que existe un segundo tipo de inteligencia artificial denominado, aprendizaje profundo que es un tipo de aprendizaje que va más allá del automático, ya que engloba y procesa más datos e información al mismo tiempo, por lo que podemos apreciar su aplicación en el área de la Big Data[19].

Redes neuronales: Por otro lado, existen las denominadas Las redes neuronales, es un tipo de inteligencia artificial que intenta imitar el comportamiento de las

[17] ES, Q., 2020. ¿Qué es la inteligencia artificial y cómo se usa? | Noticias | Parlamento Europeo. Europa.eu [en línea]. [Consulta: 31 octubre 2022]. Disponible en: https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa.

[18] ¿Cuáles son los tipos de inteligencia artificial que existen? Three Points [en línea], 2022. [Consulta: 15 noviembre 2022]. Disponible en: https://www.threepoints.com/blog/tipos-de-inteligencia-artificial.

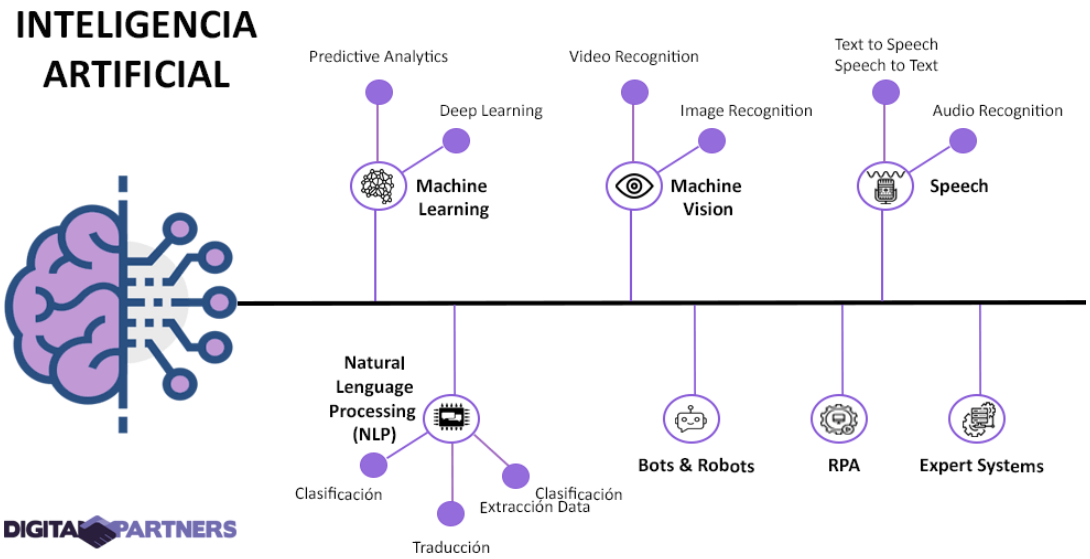
[19] Ibid

neuronas del ser humano. A partir de una red de neuronas artificiales, se crea un sistema por el que reciben y procesan datos. Las Redes Neuronales Artificiales (RNA) están formadas por millones de neuronas artificiales trabajando de manera coordinada, con capacidad de operar con acciones de aprendizaje[20].

Sistema experto: Por ultimo existe el sistema experto, el cual funciona a partir de una lógica racional que intenta imitar a un humano con dominio de una materia concreta[21].

Según la misma inteligencia artificial, esta se clasifica de la siguiente manera:

Figura. 1 clasificación de la inteligencia artificial



Fuente: DIGITALPARTNERS, 2022.

IA Basada en la Similitud Humana:

IA Débil o Estrecha (Weak AI o Narrow AI): Este tipo de IA se centra en tareas específicas y está diseñada para realizar una tarea en particular, como el reconocimiento de voz o la recomendación de productos en línea. No tiene conciencia ni comprensión real y no puede realizar tareas fuera de su dominio.

[20] Ibid
[21] ibid

IA Fuerte o General (Strong AI o AGI - Artificial General Intelligence): Se refiere a una IA que posee una inteligencia comparable a la humana y la capacidad de comprender y realizar tareas en cualquier dominio. La IA fuerte todavía es un objetivo en desarrollo y no se ha alcanzado plenamente.

IA Basada en Funcionalidad:

IA Reactiva: Estos sistemas toman decisiones basadas en patrones predefinidos y no tienen la capacidad de aprender o adaptarse. Son adecuados para tareas específicas y no pueden realizar actividades fuera de su programación inicial.

IA Basada en Aprendizaje (Machine Learning - ML): Los sistemas de aprendizaje automático utilizan algoritmos y datos para aprender y mejorar su rendimiento en tareas específicas con el tiempo. Esto incluye subtipos como el aprendizaje supervisado, no supervisado y por refuerzo.

IA Basada en Razonamiento:

IA Simbólica o Lógica: Estos sistemas utilizan lógica formal y reglas para el razonamiento y la toma de decisiones. Son eficaces en tareas que involucran reglas y relaciones lógicas.

IA Conexionista o Redes Neuronales Artificiales: Estos sistemas imitan el funcionamiento de las redes neuronales en el cerebro humano. Son efectivos en tareas como el procesamiento de lenguaje natural y el reconocimiento de patrones.

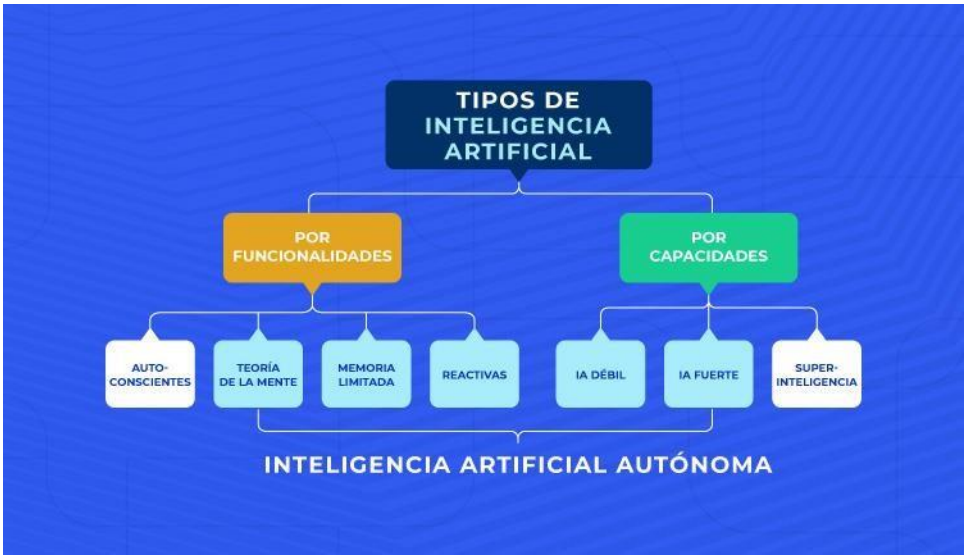
IA Basada en Comportamiento:

IA Biorrobótica: Este enfoque combina la robótica con la inteligencia artificial para crear robots que pueden imitar el comportamiento de los seres vivos.

IA Evolutiva: Utiliza algoritmos evolutivos para crear sistemas de IA que evolucionan y se adaptan con el tiempo.

Por su parte los tipos de inteligencia artificial que existen en la actualidad se describen a continuación:

Figura. 2 tipos de inteligencia artificial



Fuente: Guía de Inteligencia Artificial Autónoma: El futuro de la IA. Algotive.ai, 2022

1. Procesamiento de Lenguaje Natural (NLP): Se enfoca en la comprensión y generación del lenguaje humano, lo que permite a las máquinas interactuar con humanos en su propio idioma.

2. Visión por Computadora: Implica el análisis y procesamiento de imágenes y videos para tareas como reconocimiento facial, detección de objetos y visión artificial.

3. Aprendizaje Automático (Machine Learning): Incluye técnicas como el aprendizaje supervisado, no supervisado y por refuerzo para permitir a las máquinas aprender de los datos y tomar decisiones basadas en patrones.

4. Robótica: Combina la IA con la ingeniería para crear robots que pueden realizar tareas físicas y cognitivas.

5. IA en Juegos: Se utiliza para desarrollar programas de juego capaces de competir con humanos en juegos complejos como el ajedrez o el Go.

6. IA en Ciencias de Datos: Ayuda en el análisis y la interpretación de grandes conjuntos de datos para tomar decisiones informadas.

7. IA en Sistemas de Recomendación: Utilizada en aplicaciones como recomendaciones de películas, música o productos en línea.

8. IA en Conducción Autónoma: Desarrolla sistemas de vehículos autónomos capaces de conducir de manera segura sin intervención humana.

6 MARCO HISTÓRICO

A lo largo de la historia el hombre siempre ha tenido la necesidad o curiosidad de inventar seres inertes o maquinas con la capacidad de remplazar al ser humano, obtenido importantes desarrollos para la humanidad, pero no fue sino hasta el siglo (V) A.C que el Aristófanes poeta griego que invento una máquina que podía pensar y escribir poesía, obviamente para la época era ficción y engaño, pero a partir de allí influyo en el pensamiento humano, continuando a lo largo de la historia intentando crear cosas que pueden pensar por si solas para remplazar las tareas cotidianas realizadas por las personas.

Sin embargo, la primera vez que se acuño e termino de "inteligencia artificial", sucedió en el año de 1956 ,en donde de acuerdo con la UNESCO considero que "la inteligencia artificial (IA) es una disciplina científica que nació el Dartmouth College, en Hanover (Estados Unidos), durante un curso de verano organizado por cuatro investigadores estadounidenses: John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon. Desde entonces, la expresión "inteligencia artificial"[22], que al principio fue inventada probablemente para llamar la atención, se ha vuelto tan popular que hoy día todos saben de qué se trata, no sin esto considerar que para la época

Por su parte otras aproximaciones de "inteligencia artificial" surgen en el año de 1958 cuando Rosenblatt presenta el perceptrón, que se trataba del primer modelo de una neurona artificial, la cual era capaz de llevar a cabo un proceso de aprendizaje a partir de los datos de un problema de clasificación o regresión concreto hasta dar una respuesta al mismo, seguidamente hacia el año de 1968, Hart publica el algoritmo de búsqueda A*, que básicamente se trataba de un algoritmo de búsqueda que dado un problema, considera las posibles soluciones como puntos en un espacio apropiado y explora, a partir de un estado inicial, los posibles caminos que llevan a algunas de estas soluciones, después de otros descubrimiento y aplicaciones contemporáneas, la inteligencia artificial comenzó a declinar en los años 70 a lo que se le denomino el invierno de la inteligencia artificial en razón a que muchas empresas y empezaron a perder confianza en los resultados, ya para los años 80 comienza con la reactivación con avances importantes como las redes neuronales artificiales redescubrimiento y aplicación del algoritmo de retro propagación para el aprendizaje de redes neuronales multicapa tecnologías que fueron utilizadas en la guerra fría, hacia el año de 1989 se conoce por primera vez el termino de Big Data en la cual era esencial la inteligencia artificial para la extracción de datos en grandes volúmenes de información hasta como en día sucede, ya hacia el año de 1997 el gigante multinacional Google lanza su buscador que inicio un crecimiento desenfrenado que conllevo a la compañía a

[22] HTTPS://PLUS.GOOGLE.COM/+UNESCO, 2018. Inteligencia artificial: entre el mito y la realidad. UNESCO [en línea]. [consulta: 29 octubre 2023]. Disponible en: https://es.unesco.org/courier/2018-3/inteligencia-artificial-mito-y-realidad.

implementar paradigma de programación MapReduce Map, basado en los principios de inteligencia artificial permitiendo mayor velocidad y grandes cantidades de datos.

Posterior a ello en el año 2003 se hace necesario la utilización de la inteligencia artificial para completar el genoma humano debido a las operaciones matemáticas complejas que se pueden desarrollar con este tipo de tecnología, así mismo en ese mismo año sucedió un hecho catastrófico sobre el trasbordador espacial Culombia que se estalló en el espacio, situación que condujo para acudir a la inteligencia artificial en especial para conocer el estado de un maquina en tiempo real mediante sensores que envían información a la central de procesamiento de datos, hacia el año 2011 no se pierde la idea de crear maquinas inteligentes y por en aparecer Watson máquina que es sometida a una serie de preguntas en las cuales se encuentra en la capacidad de dar respuestas acertadas.

Por último desde el año 2013 aparece el concepto de la ciencia de datos que hasta nuestros días sigue vigente, que se convierte en el pilar fundamental para la inteligencia artificial moderna dado que se encarga de la extracción de datos inteligentes a partir de datos disponibles en las miles y millones de bases de datos, sensores inteligentes, redes computacionales y en general todo el ecosistema digital de hoy en día.

En lo que respecta al desarrollo histórico sobre la ingeniería social tenemos que es un concepto moderno que surge paralelamente con el desarrollo tecnológico pero que comenzó a tener repercusiones a finales de los años 90 y que para la década del 2000 debido a competencia empresarial se utilizó como estrategias corporativas que rápidamente fue mutando hacia la ciberdelincuencia en donde lograron hacer uso de las mismas aprovechando distintas vulnerabilidades en los sistemas informáticos.

7 MARCO LEGAL

La presente monografía aborda la temática sobre la problemática referente al contexto que afecta la población en general como son los delitos informáticos, por ende, en nuestro país estos comportamientos son regulados a través de la siguiente normatividad.

Convenio de Budapest. El congreso de la república de Colombia a través de la ley 1928 de 2018, aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest, el cual crea el marco de referencia sobre ciberseguridad para ser adoptada por todos los países miembros en su legislación interna, y en el cual dispone de todos los parámetros sobre los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, convenio que fue realizado en el año 2001 en la ciudad de Budapest Hungría.

Ley 1273 de 2009. Debido al gran índice y aumento de la comisión de condutas que afectaban la información y los datos en el año 2009 el Congreso de la República de Colombia, mediante la ley 1273 de 2009 modifica el Código Penal, y crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, implementado los siguientes delitos Artículo 269A: Acceso abusivo a un sistema informático, Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, Artículo 269C: Interceptación de datos informáticos, Artículo 269D: Daño Informático, Artículo 269E: Uso de software malicioso, Artículo 269F: Violación de datos personales, Artículo 269G: Suplantación de sitios web para capturar datos personales, Artículo 269H: Circunstancias de agravación punitiva entre otros dedicados a la protección de la información y los datos, aspectos importantes de la presente monografía en razón a que los ataques de ingeniería social se constituyen en una conducta delictiva la cual es penalizada en nuestro país.

En la misma vía el legislador el profirió la ley estatutaria 1581 de 2012, por medio de la cual se dictan disposiciones generales para la protección de datos personales cuyo ámbito de aplicación serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada es así como la presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales[23].

[23] Ley 1581 de 2012 - Gestor Normativo. Funcionpublica.gov.co [en línea], 2022. [Consulta: 28 mayo 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

8 DESARROLLO DE LOS OBJETIVOS ESPECÍFICOS

8.1 DESARROLLO OBJETIVO NO. 1 VULNERABILIDADES, RIESGOS, AMENAZAS E IMPACTOS DE LOS ATAQUES REALIZADOS POR INGENIERÍA SOCIAL Y SUS DIFERENTES CONSECUENCIAS PARA LA INFORMACIÓN Y LOS DATOS DE MANERA PERSONAL O CORPORATIVO.

De acuerdo con los referentes teóricos de la presente monografía, se entiende que la ingeniería social, es el hecho de a través de diferentes técnicas y estrategias de engaño, lograr la manipulación conseguir información o implantar un mecanismo que permita vulnerar las seguridad perimetral del sistema ya sea a nivel gubernamental, corporativo, o individual, con el fin de obtener información confidencial de esa estructura tecnológica y lograr ejecutar un ataque del cual pueda obtener provecho para si o un tercero, o en muchos de los casos por obtener un reconocimiento a nivel de la sociedad.

Como se mencionó anteriormente la ingeniería social se da de manera presencial o no presencial en donde esta última es la de mayor frecuencia, utilizando los medios electrónicos como mecanismos de transmisión, por esta razón a continuación se realizará la relación de diferentes formas de reconocimiento en las cuales se presenta la ingeniería social no presencial de las cuales se describen a continuación.

Figura. 3 incremento de los ciberdelitos en Colombia.

Fuente. cámara colombiana de informática y telecomunicaciones

Como se observa en la figura antes expuesta llama la atención las cifras expuestas que reflejan el crecimiento de los delitos denominados informáticos o ciber delitos en los cuales, pasan a convertirse en un delito común para la sociedad y la justicia por lo que se hace necesario que la política criminal aborde esta problemática para evitar que continúe en crecimiento en contraste con el incremento del uso de las tecnologías para la vida diaria de los seres humanos.

5.2.1 Spam

En primera medida comenzaremos con el Spam, que por muchos autores es considerado no malicioso, sin embargo, de acuerdo con (KASPERSKY 2021) indica que se trata de “Spam es el equivalente electrónico del "correo basura"[24] que dejan en el felpudo o el buzón de tu casa. No obstante, el spam no es solo molesto. Puede ser peligroso, especialmente si forma parte de una estafa de phishing, en este sentido, muchas de redes criminales utilizan el Spam como medio de transmisión del código malicioso en razón a que el abundante tráfico de información conllevan a inducir a la víctima a acceder a acceder a las pretensiones del atacante para cometer inclusive las estafas, es por esta razón que como se indica en (RISK, E., 2021) que los “servidores de correo electrónico revisan de manera automática los mensajes que recibimos y los clasifican como spam para evitar el peligro. Pero hay que tener cuidado porque este sistema no es perfecto y a veces se cuelan mensajes que pueden dañar nuestro sistema o apropiarse de datos confidenciales”[25]; así las cosas el Spam no goza de muy buen reputación, en vista que diferentes análisis como los ya citados describen los peligros y consecuencias de no realizar un buen tratamiento de este tipo de mensajería a través de correo electrónico, esto no significa que en su totalidad el Spam sea del todo malo porque en una gran cantidad tiene fines comerciales que son molestos para los internautas y por eso se considera un correo “basura” debido a la importancia que le da el usuario.

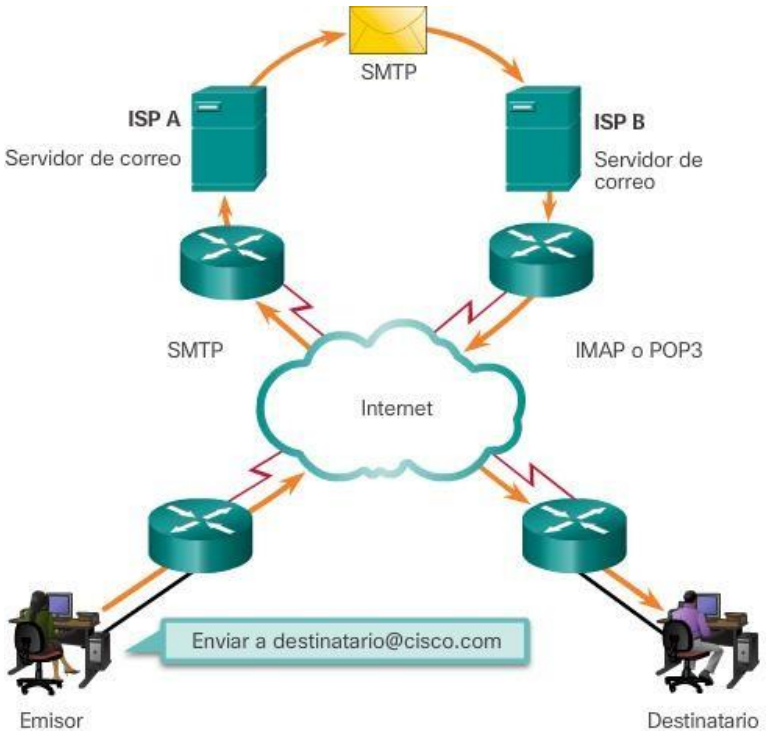
Con el transcurso del tiempo, empresas, trabajadores y consumidores no logran dimensionar el valor que representan los activos de información y se exponen a una perdida innecesaria de datos o de dinero. Los ciber delincuentes son conscientes de esta situación y mediante diversas técnicas buscan engañar a los usuarios para obtener un beneficio, generalmente económico entre ellos la utilización del Spam como herramienta para camuflar el phishing.

---

[24] KASPERSKY, 2021. Qué son el spam y las estafas de phishing - Definición. www.kaspersky.es [en línea]. [Consulta: 30 noviembre 2022]. Disponible en: https://www.kaspersky.es/resource-center/threats/spam-phishing.

[25] RISK, E., 2021. Blog de WTW España. WTW Update [en línea]. [Consulta: 30 noviembre 2022]. Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/eres-consciente-de-los-problemas-que-puede-generar-un-ingeniero-social-en-tu-empresa/.

Figura. 4 protocolo de funcionamiento del correo electrónico



Fuente. VER, 2017. Protocolos De Correo Electrónico. Interpolados [en línea].

Es así como hoy en día se han desarrollado diversos protocolos para evitar estos molestos mensajes y es por ello que se crean los sistemas Anti-Spam que trabajan de la siguiente manera

Anti-Spams de gran envergadura en servicios populares

Son los utilizados por sistemas populares en la nube, como el de Microsoft para sus dominios de Hotmail, Outlook, Live, Office 365, etc, o el de Google para Gmail, o el de Yahoo.m Si la idea es investigar estos casos en particular, recomendamos leer la nota Cómo evitar ser bloqueado por Hotmail, Gmail o Yahoo[26].

Anti-Spams Cloud

Son los utilizados en hostings de sitios web, servidores vps y otros servidores en la nube. Hay casos en que el dueño del sitio web y/o el web master tiene mayor

[26] WEB MATTER ARGENTINA, 2021. Por que hay emails que llegan a SPAM bandeja de correo no deseado? Como hacer para que lleguen a INBOX bandeja de entrada. Web-matter.com.ar [en línea].

incidencia en las configuraciones, mientras que en otros casos dependerá del proveedor del servicio de hosting.

Algunos componentes ejemplo de software para esta finalidad: SpamAssasin, Clamav, Firewalls como CSF o Fail2Ban, etc.

Anti-Spams del usuario final

Son los configurados por el propio usuario final de email. Ejemplo: Filtros dentro de un webmail, Reglas dentro de Outlook, listas blancas o negras de direcciones de email para preautorizar o no autorizar mensajes

Anti-Spams dentro de sistemas antivirus

Hoy en día cualquier solución de antivirus, sea de pc o de servidor, suele traer incorporada la posibilidad de utilizar un antispam de mensajes de email, como parte de la misma solución. Ejemplo: Avast, AVG, McAffee, Norton, etc Al indagar en cómo puede trabajar un ANTI-SPAM, se observa que tiene incorporados varios algoritmos de validación, en función a lo que se tenga que analizar del mensaje recibido:

Dirección de Email origen
Dominio origen y sus registros DNS asociados: spf, dkim, dmarc, reverso, etc
IP origen
Hostname origen
Asunto
Formato del mensaje
Links internos en el texto del mensaje
Textos internos en el mensaje que correspondan a direcciones de email
Textos internos en el mensaje que correspondan a dominios
Historial de cantidad de mensajes previos con ese email origen en la última media hora, hora, día, etc
Historial de mensajes previos con ese asunto
Historial de mensajes previos similares hacia el mismo destinatario
Historial de mensajes previos similares hacia otros destinatarios

Luego de aplicar el análisis y validación, se llega a un veredicto que puede determinar 3 posibilidades:

APROBADO OK → Llega a bandeja de Entrada

REPUTACIÓN DUDOSA → Llega a bandeja de SPAM, caso que analizaremos en esta nota

NO APROBADO → Rebota con bloqueo "duro"

5.1.2 Phishing

En primera medida se considera es pertinente conocer que es el Phishing para lo cual se trae a colación la definición realizada por (incibe 2020), en el cual describe a esta técnica como “el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico”[27] , en tal sentido se trata de una de las modalidades de ingeniería social mayormente conocidas por los ciberdelincuentes con el fin de obtener la información necesaria para perpetrar su ataque porque gracias a sus distintas técnicas orientadas a engañar al usuario final.

Figura. 5 circuito de ataque del phishing

Fuente: SOTO, C., 2021. Qué es el phishing, cómo funciona y cómo protegerte - Esferize. Esferize [en línea].

Como lo ilustra soto 2021 en la figura anteriormente expuesta el phishing principalmente se traduce en un objetivo y es lograr la consecución de dinero y es por ello que el vector de ataque ha sido creado con instrucciones para buscar información referente a datos bancarios, información de datos personales entre

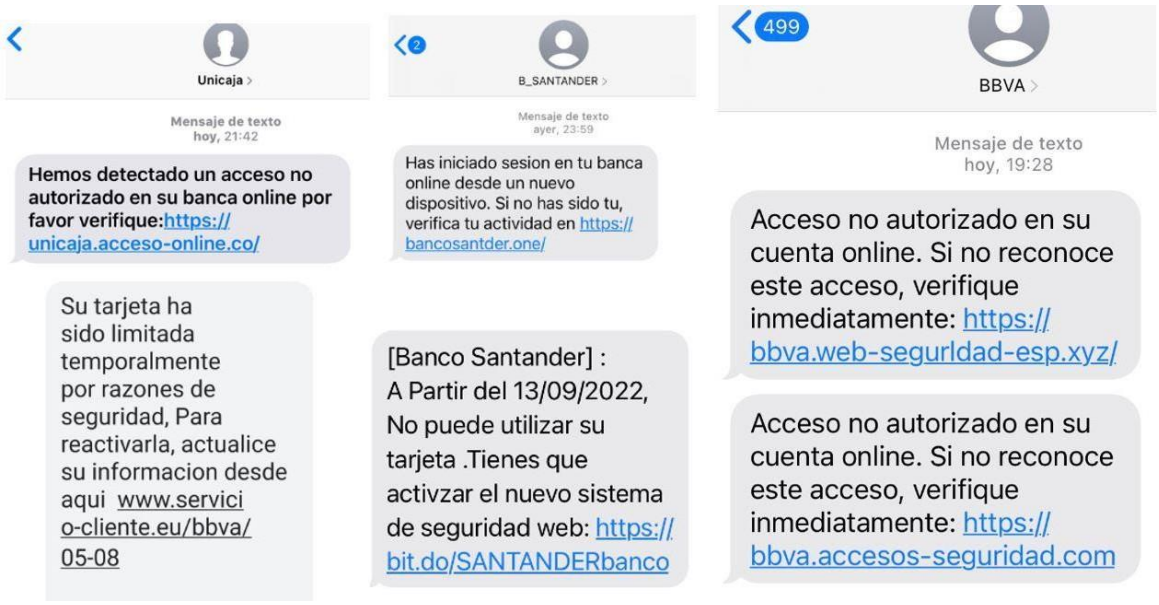
[27] Phishing. INCIBE [en línea], 2020. [Consulta: 1 diciembre 2022]. Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing.

otros con los cuales se genera un negocio del cual puede sacar provecho phisher enviando millones de correos, en donde muchas personas terminan haciendo clic abriendo la puerta para pedir información de datos personales.

5.1.3 Smishing

Esta técnica de ingeniería social que hace para del grupo del Phishing y se basa específicamente en la utilización de las mensajería instantánea SMS, en la cual buscan enviar información y enlaces para enviar enlaces en los que la víctima oprime al creer que proceden de una organización de confianza, pero con ello consigue dar apertura a la ejecución de un código malicioso que tiene una programación para ejecutar, en donde muchos de los casos se trata de el envió de información de manera oculta a un sitio web sen que el usuario se percate de lo que sucede en sus teléfono celular como la captura de sus contraseñas y datos sensibles.

Figura. 6 ejemplo de un ataque de smishing



Fuente: Kaspersky 2022

El circuito de ataque que se plantea en esta modalidad se basa principalmente a través de la mensajería SMS en el cual mediante llamativos y atractivos mensajes relacionados principalmente con ganar dinero de manera fácil o por razones políticas o idealistas.

5.1.4 Vishing

Se trata de otro método de engaño muy popular, en el cual se despliega todas las actividades que según (OSI, 2021) “es un tipo de fraude basado en la ingeniería social y en la suplantación de identidad. Se realiza a través de llamadas telefónicas, donde el atacante suplanta la identidad de una empresa, organización o incluso de una persona de confianza, con el fin de obtener información personal de sus víctimas”[28], aprovechando las debilidades psicológicas de la victimas como el miedo, confianza, desespero, codicia entre otros que conlleva a facilita la ejecución del ataque y obteniendo los resultados esperados.

5.1.5 Fake News y redes sociales

Esta modalidad consiste básicamente en la creación de noticias falsas, en las cuales busca ganar la curiosidad de la víctima a través de las redes sociales generando links o enlaces falsos que redirigen al visitante a sitios web o a descargas ocultas para iniciar otro tipo de ataque, este tipo de ingeniera social se basa en la versatilidad que tienen las redes sociales para difundir información siempre buscando captar la atención de las víctimas con avisos o eslogan llamativos y curiosos para buscar que la víctima caiga de una manera ingenua.

5.1.6 Impacto de los ataques por ingeniería social

Para analizar este aspecto es importante distinguir que el ataque por ingeniería social clasifica a tres tipos de víctimas, el primero de ellos es el sector gubernamental que se basa en las instituciones estatales y de los gobiernos a nivel mundial como por ejemplo organizaciones electorales, la seguridad y defensa del país, ámbito educativo del estado entre ostros que mantienen la estabilidad del estado pero que lograr vulnerar este tipo de organizaciones conllevaría a conseguir datos confidenciales que son muy bien pagos en la Deep Web o en el mercado negro, el otro sector que sufre bastante este tipo de ataques es el sector privado en especial la banca por tratarse de dinero constantemente son atacados para identificar vulnerabilidades que luego son explotadas con otro tipo de ataques pero que requiere de la ingeniería social para tener éxito y por ultimo tenemos el grupo individual o particular que se enfoca en la persona en específico y es ahí donde existe la mayor vulnerabilidad porque normalmente no se toman precauciones ya sea por falta de conocimiento o por la sofisticación del método de engaño

[28] ¿Qué es el vishing? | Oficina de Seguridad del Internauta. Www.osi.es [en línea], 2021. [Consulta: 1 diciembre 2022]. Disponible en: https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing.

Partiendo de los anterior, el impacto en los tres grupos clasificados como potenciales víctimas en la mayoría de los casos sufren afectaciones importantes para ello se describen de acuerdo a cada grupo.

En lo que respecta al sector gubernamental, las consecuencias y el impacto trascienden desde el nivel local, regional nacional y hasta trasnacional, porque dependiendo del nivel de acceso logrado y el tipo de información obtenida puede generar una desestabilización del gobierno en razón a que la información obtenida pude ser de gran utiliza para un sector de oposición o cibercriminales.

Para el segundo grupo, refiriéndonos a el sector privado las consciencias son bastantes complejas es por eso que (PETROSYAN, K., 2022) describe que “el impacto de la ingeniería social contra los negocios empieza con la reputación”[29] porque luego de que los socios comerciales se enteren de los sucedidos perderán la confianza en la entidad porque como afirma el mismo autor, “ la pérdida de datos por parte de la empresa ya es de por sí devastadora, pero pocas cosas son tan difíciles de recuperar como la buena fe que habías ganado con tus clientes”[30], además de ello las pérdidas económicas son realmente altas, debiendo asumir responsabilidades extracontractuales, así como inversiones futuras para adquirir nuevas infraestructuras tecnológicas y el contrato de profesionales para lograr la solución definitiva al evento el cual puede tardar tiempo que influye en la prestación del servicio de la entidad ya que se requiere una investigación rigurosa para detectar la vulnerabilidad afectada, por ejemplo conocer el nombre del funcionario que dio apretura al correo electrónico infectado. Dependiendo la gravedad y afectaciones ocurridas en el área privada puede conducir a la desaparición de la empresa, sin embargo este sector en especial la banca realiza inversiones en seguridad informática y capacitación a sus empleados sobre el manejo de la infraestructura tecnológica utilizada.

Donde muestran con mayor frecuencia los impactos, dado que es donde se idéntica la mayor vulnerabilidad del ecosistema digital tal y como lo segura (BBVA, 2022) “el factor humano se encuentra involucrado en la gran mayoría de brechas de seguridad producidas por ataques de ingeniería social. Estos ataques buscan ganarse la confianza de las personas no solo para que faciliten sus datos confidenciales, sino también para que permitan el acceso en remoto a sus equipos y/o descarguen aplicaciones o archivos maliciosos con apariencia de documentos y programas legítimos. Es decir, pretenden acceder como un caballo de Troya a los

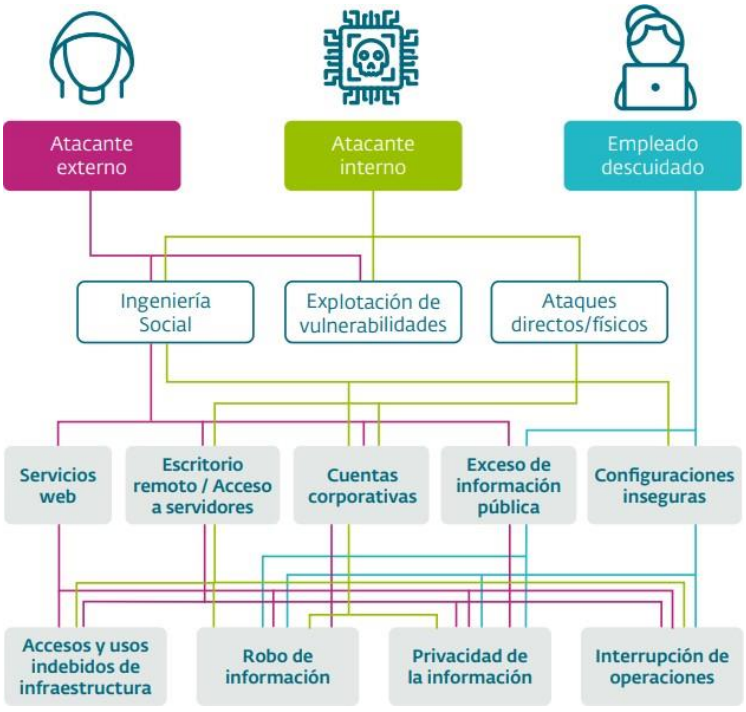
[29] PETROSYAN, K., 2022. EasyDMARC. EasyDMARC [en línea]. [Consulta: 30 noviembre 2022]. Disponible en: https://easydmarc.com/blog/es/como-puede-afectar-la-ingenieria-social-a-una-empresa-a-nivel-organizacional/#:~:text=Los%20efectos%20de%20la%20ingenier%C3%ADa,mala%20reputaci%C3%B3n%20para%20tu%20organizaci%C3%B3n..

[30] Ibid

dispositivos de las víctimas”[31], situación que conlleva a dificultar los controles por parte de la autorizades permitiendo que se presente en gran magnitud la ocurrencia de este tipo de ataques.

Sin embargo, paradójicamente existen diversos factores que contribuyen a que el ataque se satisfactorio porque no se puede esperar siempre que venga desde el otro lado, es por ello que el informe Security Report realizado por ESET para América Latina en 2020 en el cual aducen que “Desde el Laboratorio de Investigación de ESET elaboramos un diagrama con las vías más utilizadas en la ejecución de los ataques, según han identificado nuestras soluciones de seguridad en intentos dirigidos a nuestros clientes alrededor de Latinoamérica. Se ha tenido en consideración que, si bien muchas veces los ataques llegan desde fuera de la organización, es posible que ocurran dentro de la empresa, incluso por descuidos o malas prácticas de seguridad” esto conlleva a determinar que la protección a realizarse debe tener en cuenta todos los frentes y en especial el factor humano de inclusive los empleados de las organizaciones que son el eslabón más débil de la cadena en la ciberseguridad tal y como se muestra en la siguiente figura.

Figura. 7 vías para realización de un ataque de seguridad informática

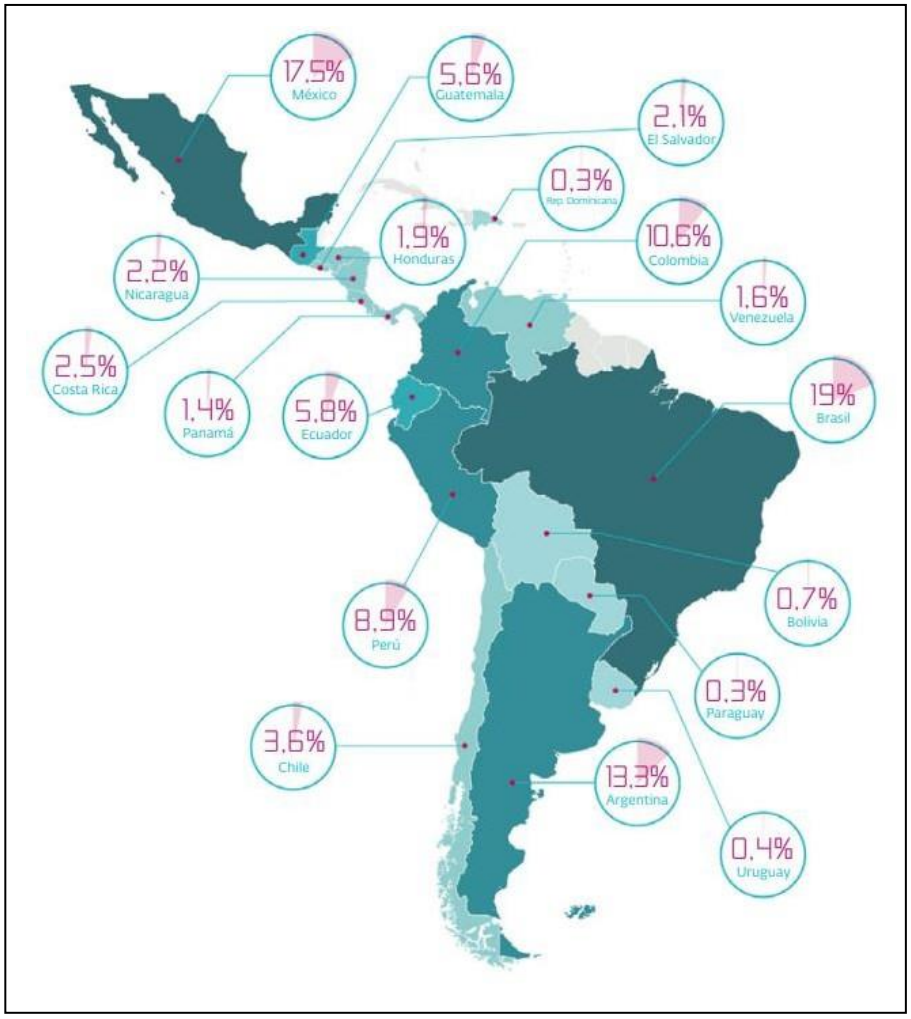


Fuente: ESET LATAM 2020

[31] BBVA ESPAÑA, 2022. Ingeniería social: el caballo de Troya de la ciberdelincuencia. Bbva.es [en línea]. [Consulta: 1 diciembre 2022]. Disponible en: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ingenieria-social-ciberdelincuencia.html.

El mismo informe determina que “cualquier caso, la ingeniería social y la explotación de vulnerabilidades siguen siendo los principales vectores que puede aprovechar un atacante para comprometer los diferentes servicios que una empresa utiliza. Una vez que logran el acceso, pueden llevar adelante distinto tipo de acciones maliciosas”[32].

Figura. 8 porcentaje en Latinoamérica de infección de malware



Fuente: ESET LATAM 2020

Independientemente del camino o del actor que esté detrás del incidente de seguridad, tanto la continuidad del negocio, como la reputación de la empresa, pueden verse afectadas, tendencia que sigue creciendo tal y como lo manifiesta organización especializada ESET en el ultimo reporte para el año 2022 en donde la ingeniería social ocupa “En segundo lugar, con el 17% de afirmaciones de los

[32] ESET Security Report, CAMBIOS EN EL PANORAMA DE SEGURIDAD 2020 LATAM 2020

encuestados, se encuentran los ataques de ingeniería social. No es de sorprender la ligera disminución con respecto al informe del año anterior, dado que el trabajo remoto dejó de ser una obligación para las corporaciones. Esto significa que cada vez menos interacciones entre colaboradores, como comunicaciones e invitaciones a reuniones, se realizan por medios digitales.

Es decir, los cibercriminales tienen una menor cantidad de temáticas para suplantar o engañar a sus víctimas en el ámbito corporativo, en comparación a años anteriores.

Sin embargo, y gracias al asentamiento del trabajo híbrido, engaños que utilicen como excusa herramientas, servicios o medios de comunicación introducidos por esta "nueva" modalidad laboral no desaparecerán. Más aún y para años posteriores, estas temáticas se sumarán a las usuales, tanto las que son atemporales como las basadas en temas de actualidad del momento.

8.2 DESARROLLO OBJETIVO NO. 2 DEFENSA PROACTIVA BASADA EN INTELIGENCIA ARTIFICIAL APLICADA COMO HERRAMIENTA DE ANTICIPACIÓN PARA PREVENIR EVENTOS DE INGENIERÍA SOCIAL.

Rincón Núñez, P. M. (2023) afirma que "Es cierto que la falta de conciencia sobre la importancia de los activos de información puede llevar a empresas, trabajadores y consumidores a exponerse a pérdidas innecesarias de datos o dinero. Los ciberdelincuentes aprovechan esta situación para llevar a cabo diversas técnicas de engaño y obtener beneficios económicos. Por esto, es importante que las empresas e individuos tomen medidas de seguridad cibernética para proteger sus activos de información y evitar ser víctimas de ataques cibernéticos. Algunas medidas que se pueden tomar incluyen el uso de contraseñas seguras, la actualización de software y sistemas, la realización de copias de seguridad de datos, la educación sobre técnicas de phishing y la implementación de políticas de seguridad cibernética en las empresas"[33].

En mismo sentido el autor plantea que "La información de personas o empresas que se encuentra pública en sitios de internet es la que más adelante les permite a los atacantes construir su estrategia de ataque, de alguna manera ganar la confianza de las víctimas y finalmente acceder a los datos confidenciales o simplemente engañar para obtener beneficio económico. De la investigación realizada se obtiene un conjunto de buenas prácticas y recomendaciones mediante las cuales es posible contribuir para la concienciación en seguridad de la información o para la elaboración de una guía que les permita a las personas tomar medidas de protección frente a este tipo de ataques"[34].

[33] Rincón Nuñez, P. M. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. InterSedes, 24(49), 120-150.

[34] Ibid

Por esta razón se hace necesario adoptar nuevas metodologías y estrategias para contrarrarrestar todo tipo de ataque en especial los relacionados con la ingeniería social; razón por la cual cobra importancia el termino de defensa proactiva y es por ello que Erick Erez Kreiner, presidente Five C y asesor senior del Israeli National Cyber Bureau afirma que ""No podemos modificar las tendencias, si uno navega, no puede cambiar el viento. Eso quiere decir que, si hay amenaza de ataque, tiene que haber tendencias de seguridad o defensa para contrarrestarla. Es necesario estar interceptando y atacando aun dentro de la propia red, pues uno la conoce mejor que el enemigo y sabe dónde puede esperarlo, en un sitio que él no se imaginaría que lo van a asaltar". Para ello, los ejércitos, las armadas, las fuerzas aéreas emplean armas que utilizan los hackers y esta es una tendencia de la tecnología desarrollada en el dominio civil, que pasa al militar y viceversa, agregó el estratega" básicamente esto significa que en materia de ciberseguridad no se puede estar esperando a que se presente el ataque para reaccionar, por lo contrario debemos y es anticipar a todas amenazas tanto desde afuera como de a dentro, y es de eso lo que se trata la defensa proactiva, pero para llevar a cabo este tipo de estrategia se requiere de contar con diversas técnicas y herramientas que funcionan bajo gran desempeño, que parta conseguirlo se basan en la utilización de la inteligencia artificial afirmando en que "sistemas proactivos le permiten mantenerse por delante de los delincuentes cibernéticos que intentan comprometer sus sistemas. El servicio proactivo combina el escaneo de red activo y pasivo para encontrar todos los sistemas en su red con inteligencia artificial y aprendizaje automático para buscar e identificar irregularidades en sus sistemas"[35] atlas cybersegurity 2018.

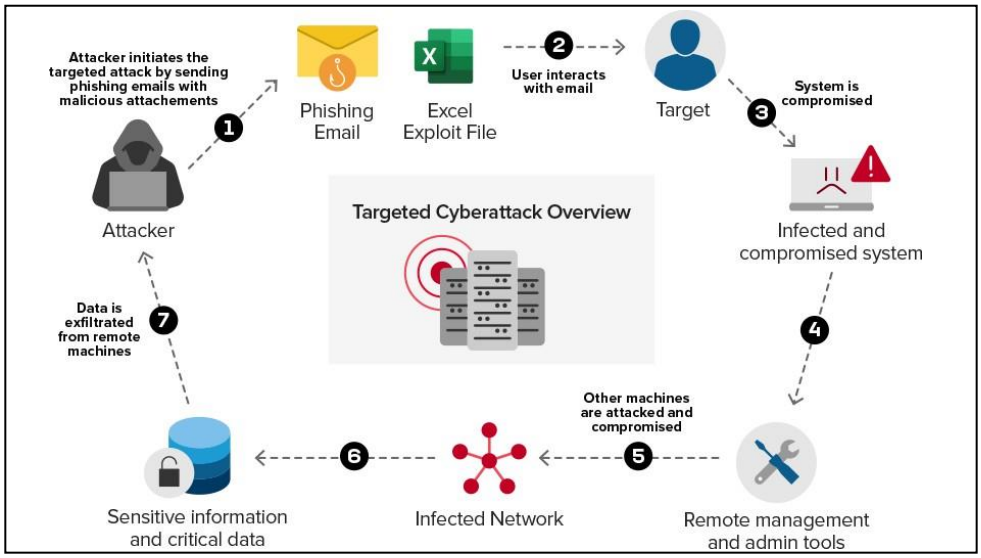
Con base en lo anterior se pude decir que, la defensa proactiva está íntimamente ligada con la inteligencia artificial puesto que una depende de la otra para su funcionamiento, lo que nos conduce a identificar que en resumidas cuentas la defensa proactiva realiza un aporte bastante significativo para contrarrestar las amenazas por ingeniería social, es por ello que Adela Colillo Jimenez 2022 menciona que "En su día a día, los profesionales de la ciberseguridad se ven desbordados por muchas tareas, por el exceso de datos que comentábamos anteriormente y por la falta de tiempo para desempeñar sus tareas, por lo que la IA les es de gran ayuda para detectar las amenazas, automatizar las respuestas y agilizar la defensa e investigación frente a otro tipo de ataques"[36], logrando que los profesionales en ciberseguridad se enfoquen mayormente en la planificación de estrategias y sea quien decide a partir de la información recolectada que tipo de

[35] Defensa Administrada Proactiva • Atlas Cybersecurity. Atlas Cybersecurity [en línea], 2018. [Consulta: 28 mayo 2023]. Disponible en: https://atlas-cybersecurity.com/es/service/proactive-managed-defense/.

[36] ADELA COLINO GIMENEZ, 2022. Realidades de la inteligencia artificial aplicada a la ciberseguridad - Artículo para Asociación @aslan. Asociación @aslan [en línea]. [Consulta: 28 mayo 2023]. Disponible en: https://aslan.es/realidades-de-la-inteligencia-artificial-aplicada-a-la-ciberseguridad/.

herramientas utiliza o métodos para prevenir vectores de ataque informático por ingeniería social “Se trata de un enorme avance en todos los sentidos, y su participación en las estrategias de ciberdefensa la iremos viendo, porque como dice Nick Bostrom, experto en IA de la universidad de Oxford, “Si la Inteligencia artificial termina siendo capaz de hacer todo o buena parte de nuestro trabajo intelectual mejor que nosotros, tendremos en nuestras manos el último invento que tendrá que realizar la Humanidad” reflexión planteada por la misma autora.

Figura. 9 ataques dirigidos utilizando ingeniería social



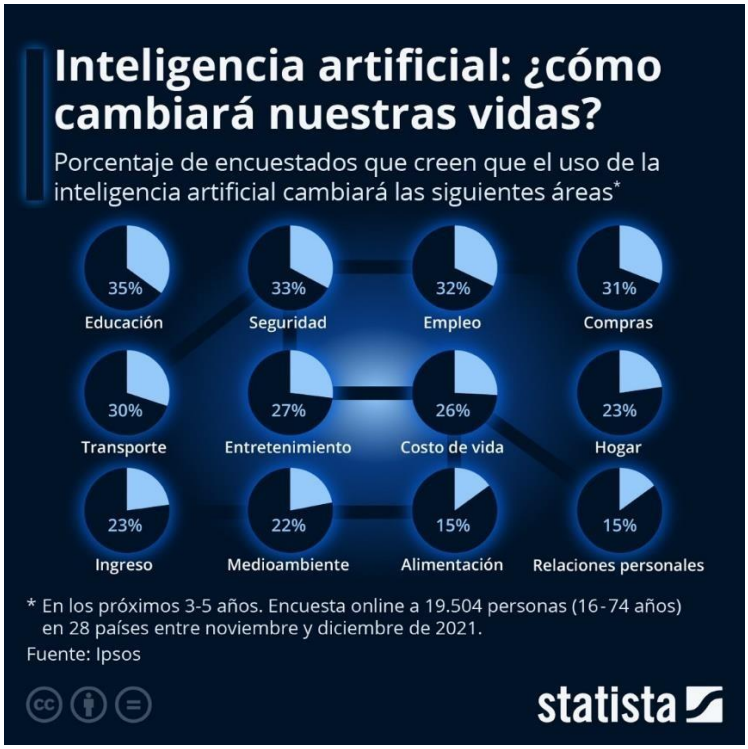
Fuente: Aditya Sood 2022

Se puede decir que el temino de seguridad proactiva, como lo indica aditya sood 2022 “se ha convertido en el enfoque necesario predominante. Mientras que los gobiernos son generalmente responsables de garantizar que las infraestructuras críticas (incluidos los portales web militares, los sitios web de las instituciones financieras, incluida la infraestructura SCADA) deben estar supervisadas y protegidas contra los ciberataques, las líneas entre la seguridad del sector público y privado se han vuelto mucho más matizadas. En términos generales, la seguridad de la infraestructura de red y de las aplicaciones desplegadas es fundamental para eludir los ataques a la red, como los de DDoS y los códigos maliciosos distribuidos a través de la conexión, para preservar la integridad de los recursos de la infraestructura sin afectar a la disponibilidad. Y, lo que es más importante, también es necesario proteger las aplicaciones críticas contra los ataques HTTP. Lo más importante es garantizar que la comunicación a través de Internet se mantenga sin interrupciones. Para ello, las organizaciones deben asegurarse de que su

infraestructura está dotada de mecanismos de seguridad para combatir los ciberataques” [37].

En conclusión con el abordaje de este segundo objetivo, nos permite inferir en la necesidad de mantener una seguridad proactiva para el entorno digital, para el cual es necesario hacer uso de la inteligencia artificial (AI), puesto que con ellos es posible realizar procedimientos como detectar amenazas más rápido, análisis en alto volumen sobre posible a ataques, aprendizaje constante sobre incidentes ocurridos, reducción de margen de error, enfrentar boots entre otras actividades que reemplazan a expertos en ciberseguridad que requieren pasar a un aspecto enfocado al control y operación de este tipo de herramientas.

Figura. 10 análisis del cambio de vida por la inclusión de la inteligencia artificial



Fuente: estatista 2023

Una de las principales conclusiones a la que nos lleva la gráfica anterior, realizada por María Melo con una encuesta mundial en el año 2021, destacando la seguridad como uno de los factores predominantes para cambiar las vidas; es pertinente reconocer que la ciberseguridad hace parte de ese gran componente de la

[37] La cambiante necesidad de ciberseguridad proactiva. F5.com [en línea], 2022. [Consulta: 28 mayo 2023]. Disponible en: https://www.f5.com/es_es/company/blog/the-evolving-need-of-proactive-cybersecurity.

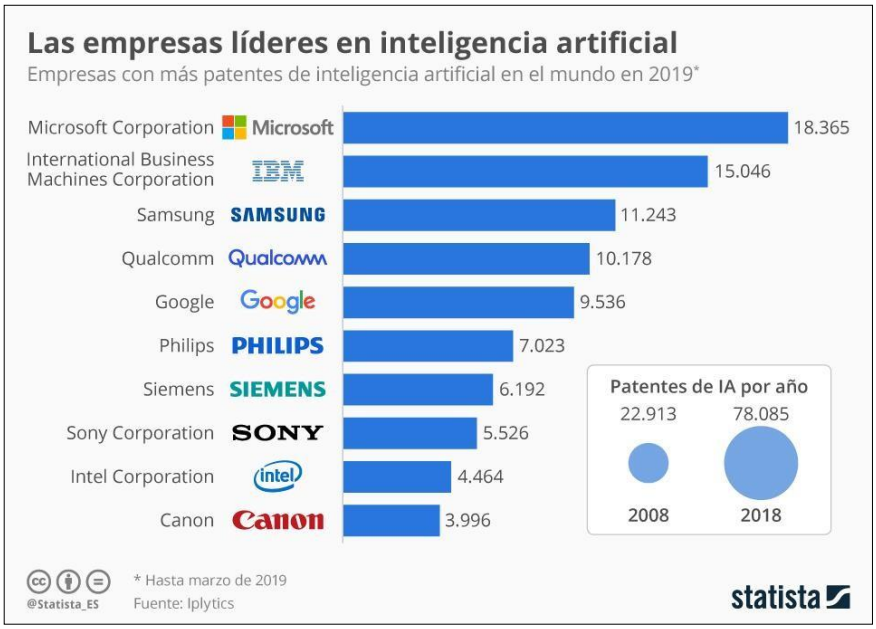
seguridad porque la necesidad de proteger los datos personales es cada día una prioridad mayor para la humanidad, así como mantener las infraestructuras tecnológicas funcionando correctamente, aspecto que no permite reflexión en que se deben mejorar los distintos controles y hacer uso eficiente de la inteligencia artificial para ayudar a contrarrestar este tipo de amenazas.

8.3 DESARROLLO OBJETIVO NO. 3 CARACTERÍSTICAS DE LA INTELIGENCIA ARTIFICIAL APLICADA EN PROCESOS DE PREVENCIÓN PARA ATAQUES DE INGENIERÍA SOCIAL

Dado que la inteligencia artificial se caracteriza por recoger y absorber información y datos, para posteriormente interpretar y aprender de los datos recolectados, que posteriormente ese conocimiento le permite ejecutar diferentes acciones traducidas en algoritmos que son predictivos con base en el aprendizaje logrado, de la misma manera la inteligencia artificial o IA en adelante posee múltiples bondades orientadas a facilitar operaciones sencillas y complejas para el ser humano debido a que gracias a sus fundamentos teóricos permiten inferir en áreas y campos de la vida moderna como la medicina, ingeniería, matemática, economía, tecnología, entre otras en las cuales sin dida alguna se ha vuelto un factor determinante en el desarrollo de la sociedad global.

Es así como como a partir de los diferentes tipos de IA, que existen en la actualidad como el aprendizaje automático que se encarga de aprender y entrenar resultados, por lo cual nos familiarizarnos con este tipo de inteligencia artificial dado que su aplicación principalmente se observa en video juegos y en boots de asistentes virtuales que hoy en día casi todas las empresas los utilizan es sus sitios web e incluso en la mensajería instantánea a nivel corporativo aplican este tipo de ingeniería social, de la misma manera la existe un tipo de IA que se dé denomina aprendizaje profundo el cual se orienta para analizar y comprender grandes volúmenes de datos como la BIG Data por ende su aplicación se basa en áreas como el reconocimiento facial, traducción de textos y la biometría entre otros, es por eso que grades compañía hoy en día la apuestan a la implementación de la inteligencia artificial para la fabricación de sus dispositivos y desarrollo de software como se ilustra en la Fig. 1 en la cual se evidencia como al año 2018, ya existía un auge y carrera desenfrenada por las grandes compañías para incorporar este tipo de desarrollo.

Figura. 11 Empresas lideres en inteligencia artificial.



Fuente: MORENO, G., 2019. Infografía: En 2018 se presentaron casi 80.000 patentes de inteligencia artificial.

Por otro lado, la inteligencia artificial se esta convirtiendo en una herramienta fundamental en el área de la ciberseguridad dado que muchos de los dispositivos físicos y lógicos que hoy en día son desarrollados, contienen en gran parte aspectos de la IA, ya que están programados para aprender de acuerdo con lo ataque sufridos y con esto implementar defensas, que puedan predecir futuros ataques, ya sea en las distintas modalidades en las que se cometen los ataques.

Una de estas modalidades es la ingeniería social, que se basa explícitamente en a través de maniobras presenciales como no presenciales para penetrar el sistema, principalmente basados en el arte de la manipulación y el engaño al ser humano en las diferentes modalidades conocidas de la ingeniería social, es por esta razón que la IA, se convierte en un aliado importante para combatir este tipo de vectores ya que por lo general siempre utilizan patrones de comportamiento y metodologías similares, esto le permite al sistema aprender y crear estrategias de defensa de manera automática evitando la ocurrencia del evento perjudicial.

En concordancia se busca explicar cómo las características de la inteligencia artificial permiten la prevención de la evitar la ocurrencia de ataques por ingeniería social, para tal fin es importante mencionar que la IA, posee diferentes características que permiten ser reconocida hoy en día como una herramienta fundamental en diversas áreas, y con las cuales se explicara su aporte para la prevención en la ingeniería social.

De acuerdo con cifras entregadas por WOOLF, M., 2022[38]. En 2021, la financiación total de los startups en IA alcanzó un récord de 18.000 millones de euros, mientas que ByteDance fue la mayor empresa de IA en 2021, con una valoración de más de 130.000 millones de euros. Sus algoritmos ofrecen contenidos personalizados a los usuarios de Tik Tok, entre otros, por otra parte IBM lidera la carrera actual del mercado de la IA, con una cuota de mercado global de más del 9%, en razón a que IBM era el mayor propietario de familias de patentes activas de aprendizaje automático (ML) y de IA en todo el mundo, con hasta 5.538 en propiedad hasta noviembre de 2020, se sigue considerando la ciberseguridad (52%) y la atención al cliente (48%) son los sectores más valorados de la IA.

Figura. 12 compañía líder en inteligencia artificial

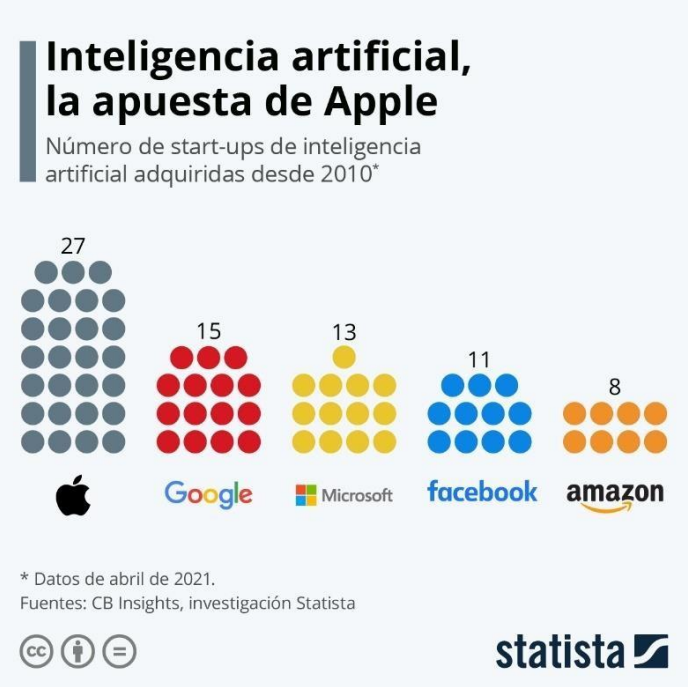
Fuente: WOOLF, M., 2022. 70+ Estadísticas sobre Inteligencia Artificial (IA) para 2022. Passport Photo Online [en línea].

La inteligencia artificial ha llamado la atención de los gigantes de la tecnología como se muestra en la gráfica de Statista, (Google, Amazon, Facebook, Apple y Microsoft) han estado tratando de conquistar el mercado de la inteligencia artificial durante la última década, puesto que conocen las bondades y ganancias que podrían generarle, pero también para proteger su infraestructura tecnológica robusta de grandes centros de datos requiere hacer uso de la inteligencia artificial

[38] WOOLF, M., 2022. 70+ Estadísticas sobre Inteligencia Artificial (IA) para 2022. Passport Photo Online [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://passport-photo.online/es-es/blog/estadisticas-sobre-inteligencia-artificial/#top-10-datos-sobre-inteligencia-artificial.

para detectar a tiempo cualquier tipo de intrusión que pueda llegar a realizar una afectación considerable, por ende la compra masiva de startups especializadas en el desarrollo de la inteligencia artificial ha impulsado la aplicación y utilización de la misma inclusive por parte de los usuarios finales con tan solos interactuar a través de un chat como chatgpt, que de acuerdo con Drew 2015 “es una herramienta que funciona interactuando de forma conversacional. El formato de diálogo hace posible que Chat GPT realice preguntas de seguimiento, admita errores, cuestione premisas incorrectas y rechace solicitudes inapropiadas. Chat GPT es un modelo hermano de Instruct GPT que está capacitado para seguir una instrucción en un aviso y proporcionar una respuesta detallada”[39].

Figura. 13 compra de startups de inteligencia artificial



Fuente: MÓNICA MENA ROA, 2021. Infografía: La gran inversión de los gigantes tecnológicos en inteligencia artificial. Statista Infografías [en línea].

5.1.1 Aplicación de la inteligencia artificial en gestión de información y eventos de seguridad (SIEM)

Para citar un ejemplo de utilización de inteligencia artificial por parte de las compañías tecnológicas, acudimos a los denominados SIEM que de acuerdo con

[39] DREW, 2015. ¿Qué es chat GPT? Wearedrew.co [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://blog.wearedrew.co/concepts/que-es-chat-gpt.

Pachón 2020[40] un SIEM (Security Information and Event Management), es una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas. Su objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información, por lo cual hoy en día existen múltiples soluciones SIEM desarrolladas por fabricantes en las cuales utilizan inteligencia artificial para realizar el monitoreo, generar alertas y realizar actuaciones para contrarrestar las amenazas, un líder en ese campo es Qradar del gigante IBM en el cual en su funcionalidad realiza actividades de aprendizaje autónomo como investiga automáticamente todas las anomalías e identifica comportamiento del ataque de alto riesgo, recopila pruebas en curso lo que facilita la actividad forense, guía a los analistas presentando una baraja de soluciones y adopta modelos para responder a ataques futuros mejorando la precisión y predicción del mismo.

5.1.2 Inteligencia artificial aplicada en antivirus

Se considera que la inteligencia artificial en la ciberseguridad comprende un gran conjunto de disciplinas entre ellas el aprendizaje automático y el aprendizaje profundo entre otros.

La inteligencia artificial se centra en el éxito, mientras que la precisión tiene menos peso. Por su parte el objetivo final es dar una respuesta natural a tareas complejas. Lo que consiste en una verdadera ejecución de la inteligencia artificial, por medio de la cual se toman decisiones reales e independientes, que a su vez están diseñados los algoritmos para encontrar la solución ideal en una situación, en lugar de solo la difícil conclusión lógica del conjunto de datos.

Como menciona Kaspersky 2022[41], es muy importante comprender el verdadero modo de funcionamiento de la IA moderna y sus disciplinas subyacentes. Dado que los sistemas autónomos no están muy extendidos, sobre todo en la esfera de la ciberseguridad. Su trabajo no requiere interferencia externa, y mucha gente suele

[40] PACHÓN, C., 2020. ¿Qué es SIEM en seguridad informática? Alcance e implementación. Nsit [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

[41] KASPERSKY, 2022. La IA y el aprendizaje automático en la ciberseguridad: cómo determinarán el futuro. latam.kaspersky.com [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity.

asociarlos con la IA, por lo que es muy fácil malinterpretar la operacionalización efectiva de la inteligencia artificial.

El papel ideal de la IA en la ciberseguridad es la interpretación de los patrones descubiertos por los algoritmos de aprendizaje automático, es por esta razón que hoy en día existe una nueva generación de antivirus que se denominan (AV) o (NGAV), los cuales revolucionan la tradicional actualización de firmas que lleva funcionando desde los últimos tiempo para dar paso a una modelos de operación de antivirus proactiva, que busca a partir de la inteligencia artificial generar predicciones sobre variantes de malware desconocidas e interpretar el modelo de operación del ataque para brindar las protecciones adecuadas al usuario final que puede ser a nivel corporativo empresarial o individual, ya que incorporan el machine learning para mantener de manera constante ya que se basa a partir de la tecnología cloud computing.

Figura. 14 Mejor antivirus de año 2022

Fuente: AV-TEST | Ensayos independientes de software antivirus. Av-test.org [en línea], 2022.

Según reportes del sitio especializado para ensayo de antivirus de manera independiente AV-TEST GmbH, que es el instituto de investigación independiente en materia de seguridad informática de Alemania, indica como se observa en la gráfica anterior un crecimiento de antivirus como (Ahnlab) remplazando a gigantes

que por años manejaron el monopolio global, pero esta tendencia tiene una explicación, que básicamente se basa en la inclusión de la ingeniería social para el funcionamiento del antivirus por eso a lo largo de los años venideros se apreciara una revolución con la llegada de nuevas compañías con experiencia en (IA).

Esta nueva generación de antivirus surge porque por años se lleva utilizando un modelo conocido y predictivo para los atacantes que ya conocen cuales son los alcances de los antivirus tradicionales y terminan por engañarlos como por ejemplo ataques basados en memoria, script de PowerShell, sesiones remotos, macros entre otros en donde el antivirus tradicional no está en la capacidad de logar detectar el ataque además porque requiere en mucha de las ocasiones la actualización de firmas y como ya todos sabemos no en un práctica habitual del usuario actualizar el antivirus; por lo contrario en la nueva generación con ayuda de la inteligencia artificial la operación del antivirus se basa a partir de eventos que rápidamente son analizados y cotejados con procesos y demás actores del sistema para identificar de manera temprana la ocurrencia de un ataque, vale la pena resaltar que esta nueva generación aún está en proceso de desarrollo que poco a poco se va perfeccionando para generar versiones estables para los usuarios.

9 CONCLUSIONES

A través del desarrollo de la presente monografía, fue posible dar respuesta al primer objetivo de la misma, que consistía en examinar las características de la inteligencia artificial, aplicada en procesos de prevención para ataques de seguridad informática realizados mediante la técnica de ingeniería social, que permitan la implementación como una herramienta moderna y alternativa en la seguridad informática, en donde una de las principales conclusiones a la cual se llega, es que, sin duda alguna el tema mundial del año 2023 y 2024, no es otro que la inteligencia artificial donde se derrumbaron diversos paradigmas de las capacidades de los ecosistemas digitales, como lo es de conocimiento público, en los últimos tiempos todo está asociado a la inteligencia artificial, pero algo muy claro es que no todo sistema automático es inteligencia artificial, es por ello que en el examen de las características de la inteligencia artificial orientada en el campo de la ciberseguridad, fue posible comprender que paradójicamente es una herramienta supremamente eficaz tanto del lado del atacante como del lado del de la víctima, es por ello que revisados diferentes referentes bibliográficos, sitios especializados y consultados expertos en el tema conllevan a determinar, que la inteligencia artificial llego para quedarse en la humanidad y sin duda alguna la aplicada a la ciberseguridad no es la excepción porque con las bondades que otorgan las redes neuronales, el aprendizaje autónomo, la capacidad de predicción y la facilidad para imitar el razonamiento humano, permiten adoptar estas cualidades para contrarrestar los ataques de seguridad informática, en especial los realizados con vectores como el de ingeniería social dado que son predecibles porque de manera común utilizan modalidades similares pero que son enviados a muchos usuarios y es de allí donde la inteligencia artificial IA, aprende y de inmediato expande la información a nivel mundial y además plantea las soluciones, llevando con ello mitigar las posibilidades que al ataque sea fructífero.

Dentro del estudio realizado en la pág. 47 se logró identificar, que la inversión que están realizando los gigantes de internet como Microsoft, Google, Amazon, IBM, Apple son incalculables, porque visionan su aplicabilidad en diferentes campos entre ellos la ciberseguridad, que también viene desarrollando múltiples estrategias de creación de dispositivos como firewall con inteligencia artificial, los SIEM entre otros, por el lado de la protección al usuario también se identificó que ya se dejaron de lado los antivirus convencionales para migrar a los antivirus NGAV basados en defensa proactiva con algoritmos de inteligencia artificial, en donde todas estas herramientas conllevan a comprender que la incidencia de la Inteligencia Artificial para contrarrestar los ataques de seguridad informática, es de manera definitiva y que a mediad que se siga desarrollando la IA se van a obtener mayor y mejores resultados, porque el presente documento es un referente bibliográfico para desarrollos fututos en los cuales se creen aplicaciones como por citar un ejemplo

en los cuales sea posible que antes de ingresar una llamada, un mensaje de texto o correo electrónico la inteligencia artificial de manera anticipativa detecte que se trata de un ataque de seguridad informática con el método de ingeniería social.

Como segunda conclusión a la cual llega, está ligada al desarrollo del segundo objetivo, en el cual se desarrolló una investigación por medio de una revisión sistemática de literatura y publicaciones las vulnerabilidades, riesgos, amenazas e impactos, de los ataques realizados por ingeniería social y sus diferentes consecuencias para la información y los datos de manera personal o corporativo; en donde es preciso argumentar, que la ingeniería social sigue siendo uno de los principales métodos de ataques de seguridad informática, así lo afirma diferentes fuentes consultada especializadas en el tema entre ellas Interpol, OEA, Europol, Caí Virtual de la Policía Nacional, Cámara Colombiana de informática, INCIBE, ESET Latinoamérica entre otras, en el cual se concluye principalmente que la ingeniera social se incrementó en los últimos tres años, a raíz de la pandemia que conllevo al teletrabajo, del cual la mayoría de organizaciones y personas del común no estaban preparadas a nivel de seguridad informática, para realizar con protección informática las actividades laborales, situación que fue aprovechada en gran magnitud por los ciberdelincuentes, que identificaron la facilidad para proferir ataques por ingeniería social, partiendo del principio que en las casas no se posee la infraestructura de red y controles de seguridad adecuados, con los que se contarían normalmente un una compañía empresarial.

Ciertamente fue posible comprender, que los circuitos de ataque por ingeniería social, incorporan varias modalidades entre ellas los más reconocidos, como el Phishing, Vishing, Smishing, Fack News, Malware, carta nigeriana entre otros, en donde claramente el fin primordial, se basa en buscar al eslabón más débil de la seguridad informática, que para este caso se trata del ser humano, interpretando las debilidades psicológicas de cada persona como la codicia, el dinero fácil, aprovechamiento de oportunidades, el hecho de conseguir riqueza de manera rápida, la curiosidad, ideologías, región, política entre otros que vemos a diario; situación que conlleva a que la ingeniería social este enfocada a tres grandes víctimas, la primera de ellas es del entorno gubernamental y su infraestructura, que se trata de explotar la seguridad y defensa del estado a través de sus instituciones, el segundo grupo está enfocado en lo particular o corporativo, allí está inmerso la banca, grandes y medianas empresas y demás infraestructuras atractivas para explotar, y por ultimo tenemos al usuario de manera individual, es decir cualquier la persona en su entorno privado, en la cual los ataques de ingeniería social están dirigidos a buscar afectar la integridad de los datos personales, para conseguir información intima con la que luego realizan estafas o chantaje; en definitiva estos ataques de seguridad informática abarcan un sin número de posibilidades, además por la facilidad de propagación que aplican con sus diferentes métodos de engaño,

es por ello que se concluye con la elaboración del presente documento académico, que se hace necesario, tomar medidas efectivas para contrarrestar el avancé de un fenómeno que cada día acrecienta dada la proliferación y avances de las tecnologías y la intercomunicación globalizada.

- Por último, nos centramos en describir el aporte que realiza la defensa proactiva basada en inteligencia artificial, como herramienta de anticipación, ante la ocurrencia de circuitos de ataque de seguridad informática, que incorporen la ingeniería social como método para afectar las dimensiones de la información y los datos, al tratarse del tercer objetivo de la monografía; que nos invita a comprender el contexto actual en ciberseguridad, en donde exige cambiar el paradigma de esperar el ataque de seguridad informática para reaccionar suponiendo que ya se tienen unos controles previamente instalados, de la misma manera a desistir de ser una seguridad reactiva, y considerar la implementación de seguridad proactiva que está basada por la anticipación a la ocurrencia de los eventos esto involucra una gran cantidad de recursos y actividades en donde muchas veces el experto en ciberseguridad no cuenta con el tiempo suficiente para ejecutarlas, y es allí cuando surge la inteligencia artificial herramienta auxiliar que se fundamenta en las capacidades BigData, la Probabilidad, la Estadística, y los nodos con algoritmos de Machine Learning, que están siendo incorporados en diferentes equipos y herramientas de seguridad informática, en donde a través de los mismos se puede efectuar la defensa proactiva, que de acuerdo con las fuentes consultadas permite reducir costos, intercambio de información, aprendizaje automático entre otras ventajas que llevadas al plano en defensa de los ataques por ingeniería social y facilita la prevención y ocurrencia de los mismos.

Como conclusión general, se generó un instrumento de consulta, que cuya finalidad es ayudar al desarrollo de la humanidad sentando bases para futuros estudios que permitan llevar a cabo investigaciones en las cuales se generen protecciones para la sociedad en general la cual es asediada por muchos peligros en el uso de las tecnologías y el internet como son los ataques por ingeniería social en donde la falta de capacitación a los usuarios sea compensada con la inteligencia artificial y logre brindar una protección total.

10 RECOMENDACIONES

Es preciso seguir ahondando en la investigación sobre la incidencia de la inteligencia artificial (AI) aplicada en la ciberseguridad, dado que es un campo que aun está en desarrollo constante en donde cada día se obtienen nuevos resultados, sin embargo, la IA moderna todavía no es capaz de interpretar los resultados como lo haría un ser humano. Esta área está en una fase de activo desarrollo, buscando adquirir algoritmos similares al pensamiento humano. Pero aún queda mucho camino por recorrer antes de que se cree una verdadera IA. Las máquinas aún tienen que aprender a replantearse situaciones usando conceptos abstractos. En otras palabras, este nivel de creatividad y pensamiento crítico no está tan cercano como los rumores sobre la IA quieren hacerte creer.

Se requiere generan mayor investigación relacionada con la Ingeniería Social, puesto que según las cifras aquí mencionadas indican que es un fenómeno en aumento dado principalmente por la proliferación de tecnologías y las formas en que las usa el ser humano, evidenciándose que conductas criminales se han trasladado de entornos físicos al mundo digital.

Continuar con la capacitación y concientización para derrumbar el paradigma que el eslabón más débil es la persona para ello desde los gobiernos debe existir políticas públicas orientadas al fortalecer y capacitar a todos los usuarios digitales con el fin de hacer el uso correcto de la tecnología minimizando los riesgos de ocurrencia de ataques.

Es muy importante la toma de conciencia de los seres humanos con referencia a la inteligencia artificial, porque este tipo de tecnologías está cambiando la formo de cómo se afrontan las situaciones del día a día, pero el desarrollo desmesurado podría conllevar a consecuencias si no se aplica regulaciones estatales en donde, la utilización de la IA sea beneficiosa para el ser humano y no conlleve a generar una esclavitud de la persona a requerir de ella para su supervivencia y dejar de lado el razonamiento que tanto caracteriza a la humanidad.

11 BIBLIOGRAFÍA

¿Cuáles son los tipos de inteligencia artificial que existen? Three Points [en línea], 2022. [Consulta: 15 noviembre 2022]. Disponible en: https://www.threepoints.com/blog/tipos-de-inteligencia-artificial.

¿Qué es el vishing? | Oficina de Seguridad del Internauta. Www.osi.es [en línea], 2021. [Consulta: 1 diciembre 2022]. Disponible en: https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing.
28 mayo 2023]. Disponible en: https://aslan.es/realidades-de-la-inteligencia-artificial-aplicada-a-la-ciberseguridad/.
28 mayo 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

ADELA COLINO GIMENEZ, 2022. Realidades de la inteligencia artificial aplicada a la ciberseguridad - Artículo para Asociación @aslan. Asociación @aslan [en línea]. [Consulta: ANÁLISIS FORENSE DIGITAL. Interpol.int [en línea], 2022. [Consulta: 7 octubre 2022]. Disponible en: https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital.

ANATOMÍA DE UN ATAQUE. Cisco [en línea], 2022. [Consulta: 7 octubre 2022]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html?dtid=osscdc000283.

Aproximación a la informática forense y el derecho informático: ámbito colombiano. ed. Medellín: Universidad Católica Luis Amigó, 2013. 215 p. ISBN 9789588399676

Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad.. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/bibliotecaueb/titulos/172144

ARROYO GUARDEÑO, DAVID - GAYOSO MARTÍNEZ, VÍCTOR - HERNÁNDEZ BARRÍA HUIDOBRO, C. ; ROSALES GUERRERO, S. Amenazados: seguridad e inseguridad en la web. ed. Santiago de Chile: Editorial ebooks Patagonia - Ediciones UM, 2021. 132 p. ISBN 9789566086055

BAUTISTA GARCÍA, FREDY. Tendencias del cibercrimen 2021 -2022 Nuevas amenazas al comercio electrónico, diciembre de 2021, vol 1, p 9-10. ISBN

BBVA ESPAÑA, 2022. Ingeniería social: el caballo de Troya de la ciberdelincuencia. Bbva.es [en línea]. [Consulta: 1 diciembre 2022]. Disponible en: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ingenieria-social-ciberdelincuencia.html.

BERNIK, I. Cybercrime and Cyber Warfare. ed. [S. l.]: Wiley, 2014. 176 p. ISBN 9781118898956
CENTRO CIBERNÉTICO POLICIAL. Policia.gov.co [en línea], 2022. [Consulta: 7 octubre 2022]. Disponible en: https://caivirtual.policia.gov.co/#mural.
Comisión Económica para América Latina y el Caribe (CEPAL), Tecnologías digitales para

un nuevo futuro (LC/TS.2021/43), Santiago, 2021

COSTAS SANTOS, J. Seguridad informática. ed. Madrid: RA-MA Editorial, 2015. 301 p. ISBN 9788499643137

CUATRECASAS MONFORTE, C. La inteligencia artificial como herramienta de investigación criminal: utilidades y riesgos potenciales de su uso jurisdiccional. 1. ed. [S. l.]: Wolters Kluwer España, 2022. 459 p. ISBN 9788419032560

CYBER CRIME | Federal Bureau of Investigation. Federal Bureau of Investigation [en línea], 2014. [Consulta: 7 octubre 2022]. Disponible en: https://www.fbi.gov/investigate/cyber.
Defensa Administrada Proactiva • Atlas Cybersecurity. Atlas Cybersecurity [en línea], 2018. [Consulta: 28 mayo 2023]. Disponible en: https://atlas-cybersecurity.com/es/service/proactive-managed-defense/.

DREW, 2015. ¿Qué es chat GPT? Wearedrew.co [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://blog.wearedrew.co/concepts/que-es-chat-gpt.

ENCINAS, LUIS. ¿Qué sabemos de? Ciberseguridad. Madrid. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. 144 p. ISBN 9788400107147

ES, Q., 2020. ¿Qué es la inteligencia artificial y cómo se usa? | Noticias | Parlamento Europeo. Europa.eu [en línea]. [Consulta: 31 octubre 2022]. Disponible en: https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa.

ESET Security Report, CAMBIOS EN EL PANORAMA DE SEGURIDAD 2020 LATAM 2020
FLORES SALGADO, L. Derecho informático. ed. México D.F: Grupo Editorial Patria, 2015. 241 p. ISBN 9786074388695

GARRIDO, Á. Los avances de la inteligencia artificial. ed. Madrid: Dykinson, 2020. 215 p. ISBN 9788413246604

INCIBE. Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. INCIBE [página web]. (9, mayo, 2019). [Consultado el 3, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse>.

Informe SAFE - Tendencias del Cibercrimen 2021 - 2022. Cámara Colombiana de informática. Etipo Tic Tac. Bogotá. 2022. Pag 27

Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. INCIBE [en línea], 2019. [Consulta: 19 marzo 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.

KARDOUDI, O., 2023. Expertos internacionales piden parar el desarrollo de la inteligencia artificial. elconfidencial.com [en línea]. [Consulta: 15 mayo 2023]. Disponible en: https://www.elconfidencial.com/tecnologia/novaceno/2023-03-29/inteligencia-artificial-chatgpt-regulacion-expertos_3601529/.

KASPERSKY, 2021. Maneras de evitar ataques de ingeniería social. www.kaspersky.es [en

línea]. [Consulta: 7 octubre 2022]. Disponible en: https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks.

KASPERSKY, 2022. La IA y el aprendizaje automático en la ciberseguridad: cómo determinarán el futuro. latam.kaspersky.com [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity.

KASPERSKY, 2022. La IA y el aprendizaje automático en la ciberseguridad: cómo determinarán el futuro. latam.kaspersky.com [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity.

KKIENERM, 2020. Cybercrime. Unodc.org [en línea]. [Consulta: 7 octubre 2022]. Disponible en: https://www.unodc.org/e4j/es/secondary/cybercrime.html.

La cambiante necesidad de ciberseguridad proactiva. F5.com [en línea], 2022. [Consulta: 28 mayo 2023]. Disponible en: https://www.f5.com/es_es/company/blog/the-evolving-need-of-proactive-cybersecurity.

LASSE ROUHIAINEN. Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro. ed Alienta Editorial Planeta. Barcelona. 2018. 22 p. ISBN : 978-84-17568-08-5
Ley 1581 de 2012 - Gestor Normativo. Funcionpublica.gov.co [en línea], 2022. [Consulta:

MAILLO FERNÁNDEZ, J. A. Sistemas seguros de acceso y transmisión de datos. ed. Paracuellos de Jarama, Madrid: RA-MA Editorial, 2017. 161 p. ISBN 9788499646954

MEDIA, D., 2019. La Inteligencia Artificial y su impacto en la Ciberseguridad. Itdigitalsecurity.es [en línea]. [Consulta: 7 octubre 2022]. Disponible en: https://www.itdigitalsecurity.es/opinion/2019/01/la-inteligencia-artificial-y-su-impacto-en-la-ciberseguridad.

MESA ELNESER, A. M. VÁSQUEZ SANTAMARÍA, J. E. ; LALINDE PULIDO, J. G. MESEGUER GONZÁLEZ, P. Y LÓPEZ DE MÁNTARAS BADIA. Inteligencia artificial. Madrid. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2017. 168 p. ISBN 9788400102340

MIRANDA GONÇALVES, R. ; PARTYK, A. Artificial intelligence and human rights. ed. Madrid: Dykinson, 2021. 489 p. ISBN 9788413778174

MORENO PÉREZ, A. Inseguridad informática y cibercrimen: rito y amenaza. ed. Buenos Aires: Editorial Seguridad y Defensa, 2012. 96 p. ISBN 9781512972825

PACHÓN, C., 2020. ¿Qué es SIEM en seguridad informática? Alcance e implementación. Nsit [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

PETROSYAN, K., 2022. EasyDMARC. EasyDMARC [en línea]. [Consulta: 30 noviembre 2022]. Disponible en: https://easydmarc.com/blog/es/como-puede-afectar-la-ingenieria-social-a-una-empresa-a-nivel-organizacional/#:~:text=Los%20efectos%20de%20la%20ingenier%C3%ADa,mala%20reputaci%C3%B3n%20para%20tu%20organizaci%C3%B3n..

Phishing. INCIBE [en línea], 2020. [Consulta: 1 diciembre 2022]. Disponible en:

https://www.incibe.es/aprendeciberseguridad/phishing.

RINCÓN NÚÑEZ, P. M. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. InterSedes, 24(49), 120-150.

RINCÓN NÚÑEZ, P. M. 2023. Ataques basados en ingeniería social en Colombia, buenasprácticas y recomendaciones para evitar el riesgo. InterSedes, 24(49), 120-150.

S. BISWAL, "Real-Time Intelligent Vishing Prediction and Awareness Model (RIVPAM)," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, pp. 1-2, doi: 10.1109/CyberSA52016.2021.9478240.

S. PATIL Y S. DHAGE, "Una descripción general metódica sobre la detección de phishing junto con una forma organizada de construir un marco anti-phishing", 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) , 2019, pp. 588-593 , doi: 10.1109/ICACCS.2019.8728356.

TAHIRI DIKOVEC, 2019. Ingeniería Social: el arte de la manipulación humana - Tahiri Dikovec. Tahiri Dikovec [en línea]. [Consulta: 31 octubre 2022]. Disponible en: https://tahiridikovec.com/ingenieria-social-el-arte-de-la-manipulacion-humana/#:~:text=Como%20he%20comentado%2C%20la%20ingenier%C3%ADa,se%20comunican%20directamente%20entre%20s%C3%AD..

TERRANIGMA, 2021. El uso de la inteligencia artificial en ciberdelincuencia y estafas. Platzi [en línea]. [Consulta: 7 octubre 2022]. Disponible en: https://platzi.com/blog/deepfakes/.

WEB MATTER ARGENTINA, 2021. Por que hay emails que llegan a SPAM bandeja de correo no deseado? Como hacer para que lleguen a INBOX bandeja de entrada. Web-matter.com.ar [en línea].

WOOLF, M., 2022. 70+ Estadísticas sobre Inteligencia Artificial (IA) para 2022. Passport Photo Online [en línea]. [Consulta: 20 marzo 2023]. Disponible en: https://passport-photo.online/es-es/blog/estadisticas-sobre-inteligencia-artificial/#top-10-datos-sobre-inteligencia-artificial.