Revista iraquí de informática y matemáticas

Revista Página de inicio:http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Hacia la Ciberseguridad Basada en Inteligencia Artificial: La Prácticas y formas de combate generadas por ChatGPT

Ciberdelincuencia

Maad M. Mijwil[1]*, Mohammad Aljanabi[2,4], ChatGPT[3]

[1]Departamento de Ingeniería de Técnicas Informáticas, Facultad de Ciencias Económicas de la Universidad de Bagdad, Bagdad, IRAQ
[2]Departamento de Informática, Facultad de Educación, Universidad de Aliraqia, Bagdad, IRAQ
[3]Open AI LLC, 3180 18th Street, San Francisco, CA 94110, EE. UU.
[4]Colegio universitario AlSalam, Irak

* Autor correspondiente: Maad M. Mijwil

DOI:https://doi.org/10.52866/ijcsm.2023.01.01.0019
Recibido en enero de 2023; Aceptado en enero de 2023; Disponible en línea en enero de 2023

ABSTRACTO: Hoy en día, la ciberseguridad se considera uno de los temas más destacados que circulan con frecuencia entre las empresas para proteger sus datos de las operaciones de piratería. La aparición del ciberespacio contribuyó al crecimiento de los sistemas electrónicos. Es un espacio digital virtual a través del cual se establece la interconexión entre ordenadores y smartphones conectados en el entorno del Internet de las Cosas. Este espacio es fundamental para construir un entorno digital seguro y libre de amenazas y delitos cibernéticos. Solo es posible hacer un entorno digital con la presencia del ciberespacio, que contiene tecnologías modernas que hacen que este entorno sea seguro y lejos de personas no autorizadas. La ciberseguridad tiene una amplia gama de desafíos y obstáculos en el desempeño, y es difícil para las empresas enfrentarlos. En este informe, Se estudiarán las prácticas más significativas, sensatas y buenas estrategias para frenar el ciberdelito y hacer un entorno digital que garantice la transferencia de datos entre dispositivos electrónicos de forma segura y sin la presencia de software malicioso. Este informe concluyó que los procedimientos que brinda la ciberseguridad son requeridos y deben ser cuidados y desarrollados.

Palabras clave: Ciberseguridad, Cibercrimen, Ciberespacio, Inteligencia Artificial, Digitalización, ChatGPT.

1. INTRODUCCIÓN

En los últimos años, el cibercrimen se ha convertido en uno de los puntos más cruciales que circulan entre empresas, organizaciones y particulares, por lo que se considera uno de los delitos más graves [1][2]. Estos delitos persiguen robar datos y cambiar el rumbo de las computadoras mediante la manipulación de sistemas y la modificación de programas de protección. El cibercrimen afecta tanto al rendimiento de los ordenadores como al estado psicológico de los usuarios, ya que el robo, alteración o borrado de datos es uno de los procedimientos más peligrosos a los que se enfrentan las empresas [3][4]. Por lo tanto, estas empresas buscan el uso de tecnologías modernas y avanzadas en el desarrollo de sus sistemas y la protección de los datos de sus clientes. Además, teniendo en cuenta todas las medidas cruciales para proteger las computadoras y el uso de especialistas en seguridad cibernética para crear un ciberespacio libre de brechas, así como el uso de técnicas de inteligencia artificial para diseñar las ventajas del ciberespacio y convertirlo en un excelente y sofisticado entorno digital [5-7]. El ciberespacio es un espacio digital que crea una forma para que las computadoras se conecten entre sí o con otros dispositivos electrónicos dentro del entorno de Internet de las cosas [8-10]. Utiliza técnicas de inteligencia artificial para proteger sus datos contra cualquier operación incorrecta [11-13]. La Figura 1 ilustra las amenazas cibernéticas que las instituciones pueden enfrentar en el entorno digital. Básicamente, el ciberespacio consta de tres capas, ya que cada capa está vinculada con la siguiente capa, que es la siguiente: El ciberespacio es un espacio digital que crea una forma para que las computadoras se conecten entre sí o con otros dispositivos electrónicos dentro del entorno de Internet de las cosas [8-10]. Utiliza técnicas de inteligencia artificial para proteger sus datos contra cualquier operación incorrecta [11-13]. La Figura 1 ilustra las amenazas cibernéticas que las instituciones pueden enfrentar en el entorno digital. Básicamente, el ciberespacio consta de tres capas, ya que cada capa está vinculada con la siguiente capa, que es la siguiente: El ciberespacio es un espacio digital que crea una forma para que las computadoras se conecten entre sí o con otros dispositivos electrónicos dentro del entorno de Internet de las cosas [8-10]. Utiliza técnicas de inteligencia artificial para proteger sus datos contra cualquier operación incorrecta [11-13]. La Figura 1 ilustra las amenazas cibernéticas que las instituciones pueden enfrentar en el entorno digital. Básicamente, el ciberespacio consta de tres capas, ya que cada capa está vinculada con la siguiente capa, que es la siguiente:

- **Capa fisica:**Contiene empresas, redes, computadoras, servidores y cosas conectadas a Internet. Este La capa es el área a la que las personas no autorizadas desean acceder y controlar.
- **Capa lógica:**Contiene aplicaciones, programas y protocolos que han sido proporcionados o equipados por partes especializadas y de confianza.
    - **Capa semilógica:**Contiene datos e información que no se permite ver ni transmitir excepto por personas autorizadas o de confianza.

* Autor para correspondencia: mr.maad.alnaimiy@baghdadcollege.edu.iq

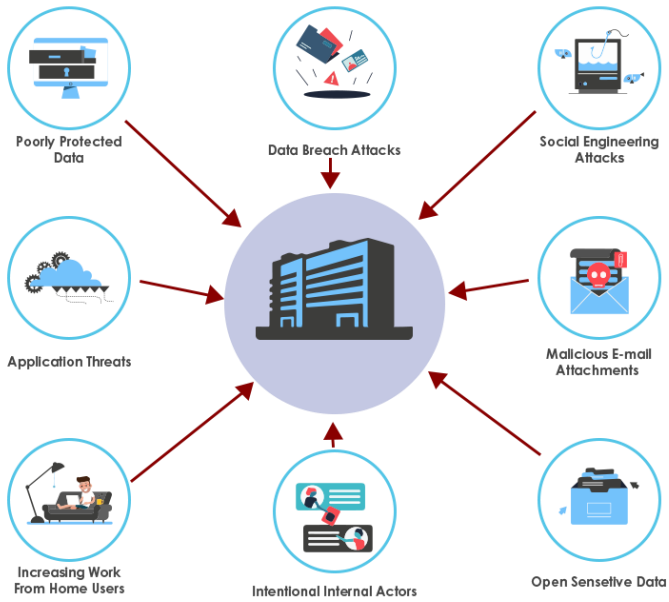

FIGURA 1.- Formas de amenazas cibernéticas [14].

Se debe tener en cuenta que el ciberespacio tiene un conjunto de características que se deben observar y cuidar para que no sean características negativas que afecten el funcionamiento del entorno digital. Como características más cruciales es que este espacio es complejo, amplio y de fácil acceso. Este espacio es donde se intercambian datos e información mediante el uso de prácticas correctas y seguras. Además, la característica más crucial de este espacio es que contiene tecnologías que detectan y controlan ciberataques complejos y determinan los procedimientos necesarios para eliminar estos ataques. El cibercrimen es un acto destructivo que afecta significativamente el funcionamiento del entorno digital mediante la manipulación de datos, el espionaje, la extorsión o la publicación de contenidos ilegales dirigidos a clientes o empresas [15][16]. El delito electrónico se considera una amenaza grave, debiendo buscarse rápidas resoluciones para el mismo en caso de ocurrencia y control de los sistemas informáticos. El cibercrimen busca comprometer la seguridad de las computadoras, teléfonos inteligentes, tabletas, consolas de juegos, redes y otras cosas conectadas a Internet [17-19]. El perpetrador de una amenaza cibernética puede ser una persona o un grupo de piratas informáticos. Las amenazas cibernéticas tienen grandes motivos en el espionaje militar, la extorsión para obtener dinero o información, la extorsión y el deterioro de la reputación de las personas, la venganza y el desafío. Por ello, en este artículo se repasarán las medidas más significativas que marca el ámbito de la ciberseguridad en la protección del entorno digital, como por ejemplo cómo se controlan los ordenadores y no se permite que se dañen o controlen. y se deben encontrar soluciones rápidas para el mismo en caso de su ocurrencia y control de los sistemas informáticos. El cibercrimen busca comprometer la seguridad de las computadoras, teléfonos inteligentes, tabletas, consolas de juegos, redes y otras cosas conectadas a Internet [17-19]. El perpetrador de una amenaza cibernética puede ser una persona o un grupo de piratas informáticos. Las amenazas cibernéticas tienen grandes motivos en el espionaje militar, la extorsión para obtener dinero o información, la extorsión y el deterioro de la reputación de las personas, la venganza y el desafío. Por ello, en este artículo se repasarán las medidas más significativas que marca el ámbito de la ciberseguridad en la protección del entorno digital, como por ejemplo cómo se controlan los ordenadores y no se permite que se dañen o controlen. y se deben encontrar soluciones rápidas para el mismo en caso de su ocurrencia y control de los sistemas informáticos. El cibercrimen busca comprometer la seguridad de las computadoras, teléfonos inteligentes, tabletas, consolas de juegos, redes y otras cosas conectadas a Internet [17-19]. El perpetrador de una amenaza cibernética puede ser una persona o un grupo de piratas informáticos. Las amenazas cibernéticas tienen grandes motivos en el espionaje militar, la extorsión para obtener dinero o información, la extorsión y el deterioro de la reputación de las personas, la venganza y el desafío. Por ello, en este artículo se repasarán las medidas más significativas que marca el ámbito de la ciberseguridad en la protección del entorno digital, como por ejemplo cómo se controlan los ordenadores y no se permite que se dañen o controlen. El cibercrimen busca comprometer la seguridad de las computadoras, teléfonos inteligentes, tabletas, consolas de juegos, re

2. PRÁCTICAS DE CIBERSEGURIDAD

La ciberseguridad es un conjunto de técnicas y enfoques que buscan proteger los sistemas y datos informáticos de los ciberataques y no permitir que software malicioso controle el funcionamiento del sistema informático. Se ocupa de proteger los sistemas sin lagunas, combatir el delito cibernético y establecer un entorno electrónico excelente. Además, la información debe estar protegida contra robo, vandalismo y acceso no autorizado, así como también protegida contra desastres naturales como polvo, humedad, etc. Las empresas buscan garantizar la integridad del proceso de transferencia de datos e información entre sistemas de dispositivos electrónicos sin la presencia de terceros no autorizados que trabajen para cambiar, modificar o eliminar datos. La confidencialidad debe existir en un proceso que busca hacer confidencial el proceso de transferencia de datos e información para evitar que personas no autorizadas accedan a estos datos mediante el uso de técnicas de inteligencia artificial que facilitan este proceso sin la presencia de ningún obstáculo y encriptarlo y transferirlo. a la parte requerida. Los sistemas informáticos se caracterizan por su capacidad de guardar datos o información sin cambiar su contenido excepto con la presencia de personas autorizadas, así como el no repudio, que es una propiedad para confirmar la realización de las tareas requeridas y no negar una transacción realizada. a cabo por uno de los participantes en el entorno digital. La ejecución de los sistemas informáticos se mide a través de un conjunto de elementos de seguridad eficaces. Se deben tener en cuenta los seis elementos básicos en el sistema de seguridad de la información informática, y se debe estudiar su influencia en las medidas de protección de datos (ver Figura 2). Además, los sistemas de seguridad de la información deben estar preparados para operar en todos los casos y bajo una ley desarrollada para combatir el ciberdelito con una gestión debidamente estructurada y organizada que incluya expertos en el manejo de sistemas de información.

La ciberseguridad se concentra en proteger el software y las aplicaciones de las vulnerabilidades, que se consideran puntos débiles, ya que permiten que se produzcan ciberataques. Los ciberdelincuentes se centran en las debilidades de los sistemas de información mediante el análisis de las prácticas de estos sistemas y el comportamiento de los usuarios para explotarlos al piratear estos sistemas. el phishing es

un tipo de operación fraudulenta a través del ciberespacio que busca obtener información influyente que beneficie a los ciberdelincuentes a través de mecanismos inteligentes con el objetivo de controlar sistemas y usuarios. La ciberseguridad enfrenta muchos desafíos en las prácticas laborales. Los especialistas organizan los sistemas de información en ciberseguridad, donde se establecen los estándares para su uso y las estrategias de conducción del trabajo. La falta de especialistas en ciberseguridad se considera uno de los obstáculos más importantes a los que se enfrentan las empresas, ya que solo es posible diseñar un entorno digital con un número suficiente de estos especialistas. Cuanto más significativo es el número de dispositivos conectados al Internet de las Cosas, más vulnerables son los ataques cibernéticos, las operaciones de espionaje y la penetración de las redes informáticas. Por lo tanto, las empresas deben contar con los preparativos adecuados y preparar las tecnologías necesarias para enfrentar la amenaza del ciberdelito. Además, no utilice aplicaciones o programas de sitios sin licencia o no oficiales, ya que estos sitios pueden ser motivo de operaciones de piratería. Las empresas deben utilizar ciertas estrategias para preservar los datos y la información y hacer copias de seguridad de los mismos de forma perfecta y precisa. Las contraseñas deben ser complejas y grandes y deben cambiarse cada seis meses o cada año para garantizar la seguridad de los sistemas informáticos. Cuando se utilizan procedimientos correctos y precisos y la cautela en el uso de los sitios web, se garantiza la seguridad del entorno electrónico y la satisfacción de empresas y clientes. El ámbito de la ciberseguridad contribuye a diseñar un entorno digital libre de lagunas y no permitir el acceso a este entorno a personas no autorizadas. Estos mecanismos solo se pueden lograr con técnicas de inteligencia artificial que juegan un papel influyente en cambiar y controlar los ataques cibernéticos [20-25]. Por lo tanto, la existencia de inteligencia artificial y medidas de ciberseguridad efectivas conducen al establecimiento de un entorno digital adecuado [26-31].

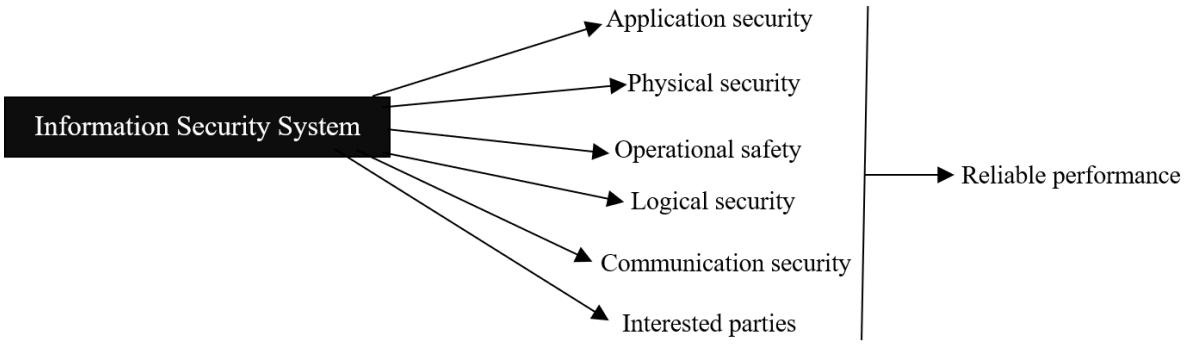

FIGURA 2.– Los seis elementos principales para medir la ejecución de un sistema de seguridad de la información.

3. LUCHA CONTRA EL DELITO CIBERNÉTICO (por ChatGPT)

La seguridad cibernética desempeña un papel fundamental en la lucha contra el delito cibernético al proteger los sistemas, las redes y los datos digitales del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados. El delito cibernético puede tomar muchas formas, incluyendo piratería, phishing, malware y ransomware, y puede tener graves consecuencias tanto para las personas como para las organizaciones. Para combatir el ciberdelito, las organizaciones deben implementar una estrategia integral de ciberseguridad que incluya:

- Evaluaciones regulares de seguridad: evalúe regularmente los sistemas y redes digitales de la organización para identificar vulnerabilidades y amenazas potenciales.
- Educación de los empleados: Brinde a los empleados capacitación sobre cómo identificar y prevenir los delitos cibernéticos, así como también sobre cómo responder a los incidentes de seguridad.
- Autenticación fuerte: use métodos de autenticación fuertes, como la autenticación multifactor, para evitar el acceso no autorizado a los sistemas y datos digitales.
- Seguridad de la red: implementar medidas de seguridad de la red, como firewalls y sistemas de detección de intrusos, para proteger contra accesos no autorizados y ataques.
- Plan de respuesta a incidentes: Desarrollar e implementar un plan de respuesta a incidentes para responder de manera rápida y efectiva a los incidentes de seguridad.
- Cifrado de datos: cifre datos confidenciales para protegerlos del acceso y la divulgación no autorizados.
- Inteligencia de amenazas de seguridad cibernética: Supervise continuamente el panorama de amenazas cibernéticas y manténgase informado sobre las últimas amenazas, tácticas y técnicas utilizadas por los ciberdelincuentes.
- Colaboración con las agencias de aplicación de la ley: La colaboración con las agencias de aplicación de la ley ayudar a localizar a los ciberdelincuentes y llevarlos ante la justicia.

Además de implementar estas medidas, las organizaciones también deben mantenerse informadas sobre las últimas tendencias y mejores prácticas de seguridad cibernética y estar preparadas para adaptar sus estrategias de seguridad según sea necesario para adelantarse a las amenazas emergentes. La ciberseguridad se refiere a la protección de los sistemas conectados a Internet, incluidos el hardware, el software y los datos, contra ataques, daños o acceso no autorizado. El ciberdelito, por otro lado, se refiere a la actividad delictiva que utiliza o tiene como objetivo

sistemas conectados a internet. Los ejemplos de delitos cibernéticos incluyen la piratería, el robo de identidad y la propagación de malware. La ciberseguridad efectiva implica el uso de una combinación de tecnologías, políticas y mejores prácticas para asegurar los sistemas y protegerlos contra el ciberdelito. Hay varios desafíos de seguridad cibernética en la protección del entorno digital, que incluyen:

- Amenazas avanzadas: los ciberdelincuentes son cada vez más sofisticados en sus métodos, por lo que es cada vez más difíciles de detectar y prevenir ataques.
- Falta de conciencia de seguridad: muchas personas y organizaciones carecen del conocimiento y la capacitación necesarios para protegerse de las ciberamenazas.
- Tecnología compleja y en constante cambio: el rápido ritmo del cambio tecnológico hace que sea difícil mantenerse al día con las nuevas vulnerabilidades y amenazas.
- Dependencia de proveedores externos: muchas organizaciones confían en proveedores externos para su infraestructura y servicios de TI, lo que crea riesgos de seguridad adicionales.
- Recursos limitados: muchas organizaciones tienen recursos y presupuesto limitados asignados a la ciberseguridad, lo que dificulta la implementación de medidas de seguridad adecuadas.
- Regulaciones insuficientes: la falta de estandarización y regulaciones uniformes dificulta la protección contra ataques cibernéticos en todas las industrias y países.
- IoT y dispositivos conectados: el creciente número de dispositivos IoT conectados a Internet crea nuevos vectores de ataque para que los ciberdelincuentes exploten.

Las reglas y regulaciones que rodean el delito cibernético pueden variar según la jurisdicción y el tipo específico de delito. En general, sin embargo, existen varias leyes internacionales, nacionales y estatales que abordan el delito cibernético. El Convenio sobre Ciberdelincuencia del Consejo de Europa es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas. Proporciona un marco para la cooperación entre las naciones en la investigación y el enjuiciamiento del delito cibernético. Estados Unidos tiene varias leyes federales que abordan diferentes tipos de ciberdelincuencia, como la Ley de Abuso y Fraude Informático, que penaliza el acceso no autorizado a las computadoras, y la Ley de Privacidad de las Comunicaciones Electrónicas, que aborda la vigilancia electrónica ilegal. Muchos países tienen sus propias leyes nacionales para abordar el ciberdelito, como el Reino Unido' s Ley de uso indebido de computadoras. Las organizaciones internacionales, como Interpol y Europol, también desempeñan un papel en la investigación y la lucha contra el ciberdelito al facilitar la cooperación entre las naciones. También vale la pena mencionar que muchas empresas y organizaciones tienen sus propios protocolos y políticas de seguridad cibernética para protegerse contra el delito cibernético, como planes de respuesta a incidentes, capacitación en concientización sobre seguridad y pruebas de penetración.

4. CONCLUSIONES

La ciberseguridad es un asunto importante ya que tiene la capacidad de hacer frente a las causas que amenazan la seguridad de la información. Sin embargo, los ataques cibernéticos representan una amenaza de diferentes maneras, y las contramedidas deben implementarse con conocimiento de las últimas tendencias. Dado que los métodos de los ciberataques evolucionan día a día, siempre es difícil tomar medidas integrales. En este sentido, este artículo contribuyó a presentar las prácticas y procedimientos más importantes que se deben tener en cuenta en su desempeño para proteger el entorno digital de ciberataques. Se deben utilizar métodos modernos para mejorar los mecanismos operados por las empresas mientras se educa a los empleados sobre la gravedad y las amenazas del ciberespacio. Aplicar estándares internacionales en la mejora de los mecanismos de protección del entorno digital. Esfuerzo constante para disponer de grupos especializados en ciberdefensa y ciberseguridad frente a ataques electrónicos y ciberdelitos. Crecer programas, aplicaciones y sistemas informáticos para poder hacer frente a todo tipo de ciberataques. Todas las empresas deben contar con mecanismos únicos para combatir los ataques cibernéticos utilizando tecnologías modernas y avanzadas basadas en inteligencia artificial para crear defensas contra el espionaje, el robo de datos y evitar la entrada de personas no autorizadas o software malicioso. Finalmente, se debe prestar atención al tema de la ciberseguridad y adaptarse al moderno y rápido crecimiento del ciberespacio a través de una estrategia integral para la prevención del ciberdelito. y sistemas informáticos para poder hacer frente a todo tipo de ciberataques. Todas las empresas deben contar con mecanismos únicos para combatir los ataques cibernéticos utilizando tecnologías modernas y avanzadas basadas en inteligencia artificial para crear defensas contra el espionaje, el robo de datos y evitar la entrada de personas no autorizadas o software malicioso. Finalmente, se debe prestar atención al tema de la ciberseguridad y adaptarse al moderno y rápido crecimiento del ciberespacio a través de una estrategia integral para la prevención del ciberdelito. y sistemas informáticos para poder hacer frente a todo tipo de ciberataques. Todas las empresas deben contar con mecanismos únicos para combatir los ataques cibernéticos utilizando tecnologías modernas y avanzadas basadas en inteligencia artificial para crear defensas contra el espionaje, el robo de datos y evitar la entrada de personas no autorizadas o software malicioso. Finalmente, se debe prestar atención al tema de la ciberseguridad y adaptarse al moderno y rápido crecimiento del ciberespacio a través de una estrategia integral para la prevención del ciberdelito.

REFERENCIAS

[1] Button M., Shepherd D., Blackbourn D., Sugiura L., Kapend R. y Wang V., “Evaluación de la gravedad del delito cibernético: el caso del delito de uso indebido de computadoras en el Reino Unido y la perspectiva de las víctimas ,”*Criminología y Justicia Criminal*, págs: 1-22, octubre de 2022.https://doi.org/10.1177/17488958221128128

[2] Alawida M., Omolara AE, Abiodun OI y Al-Rajab M., "Una mirada más profunda a los problemas de ciberseguridad a raíz de Covid-19: una encuesta"*Revista de la Universidad King Saud - Informática y Ciencias de la Información*, vol.34, no.10, pp:8176-8206, noviembre de 2022.https://doi.org/10.1016/j.jksuci.2022.08.003

[3] Lubis M. y Handayani DOD, "La relación de la protección de datos personales con la adicción a Internet: delitos cibernéticos, pornografía y actividad física reducida".*Procedia Informática*, vol.179, págs: 151-161, 2022. https://doi.org/10.1016/j.procs.2021.12.129

[4] Arpaci I. y Aslan O., "Desarrollo de una escala para medir la concienciación sobre delitos cibernéticos en las redes sociales"*Revista de sistemas de información informática*, págs: 1-11, julio de 2022.https://doi.org/10.1080/08874417.2022.2101160

[5] Mijwil MM, Doshi R., Hiran KK, Al-Mistarehi AH y Gök M., "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects,"*revista mesopotámica de ciberseguridad*, vol.2022, págs: 1-4, 2022. https://doi.org/10.58496/MJCS/2022/001

[6] Navas-Camargo F. y Castro CAA, "Cyberspace, Artificial Intelligence, and the Domain of War. Los desafíos éticos y los lineamientos propuestos por el Banco de Desarrollo de América Latina", en Seguridad y defensa: desafíos éticos y legales ante los conflictos actuales, pp: 37–55, marzo de 2022.https://doi.org/10.1007/978-3-030-95939-5_3

[7] Mijwil MM, Sadıkoğlu E., Cengiz E. y Candan H., "Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme," *Veri Bilimi*, vol.5, no.2 pp:97-105, diciembre 2022.

[8] Yang M. y Wang X., "Diseño de interacción del espacio de construcción de bienestar mediante el aprendizaje profundo y la tecnología de realidad virtual en el contexto de Internet de las cosas"*Comunicaciones inalámbricas y computación móvil*, vol.2022, no.6567431, pp:1- 10, junio 2022.https://doi.org/10.1155/2022/6567431

[9] Hu P., Chen W., He C., Li Y. y Ning H., "Software-Defined Edge Computing (SDEC): Principio, arquitectura del sistema IoT abierto, aplicaciones y desafíos"*Diario de Internet de las cosas de IEEE*, vol.7, no.7, pp:5934 - 5945, julio de 2020. https://doi.org/10.1109/JIOT.2019.2954528

[10] Roopa MS, Pattar S., Buyya R., Venugopal KR, Iyengar SS y Patnaik LM, "Internet social de las cosas (SIoT): fundamentos, áreas de interés, revisión sistemática y direcciones futuras"*Comunicaciones Informáticas*, vol.139, pp:32-57, mayo de 2019.https://doi.org/10.1016/j.comcom.2019.03.009

[11] Tao F., Akhtar MS y Jiayuan Z., "El futuro de la inteligencia artificial en la ciberseguridad: una encuesta completa"*Transacciones respaldadas por EAI sobre tecnologías creativas*, vol.8, no.28, pp:1-15, julio de 2021. https://doi.org/10.4108/eai.7-7-2021.170285

[12] Salem IE, Salman AM y Mijwil MM, "Una encuesta: funciones hash criptográficas para estampado digital" *Revista de la Universidad Southwest Jiaotong*, vol.54, no.6, pp.1-11, diciembre 2019. https://doi.org/10.35741/issn.0258-2724.54.6.2 .

[13] Salem IE, Mijwil MM, Abdulqader AW, Ismaeel MM, Alkhazraji A. y Alaabdin AMZ, "Introducción a las técnicas de minería de datos en ciberseguridad",*Revista mesopotámica de ciberseguridad*, vol.2022, pp:28-37, mayo de 2022.https://doi.org/10.58496/MJCS/2022/004

[14] ¿Por qué actualizar a Data Security Firewall?,https://www.gajshield.com/index.php/por-que-data-security-firewall

[15] Ali A., "Ciberespacio y crimen organizado: los nuevos desafíos del siglo XXI",*Revista internacional de investigación avanzada en humanidades*,vol2, no.1, pp:22-37, enero de 2022.https://doi.org/10.21608/IJAHR.2022.256386

[16] Bayramova A., Edwards DJ y Roberts C., "El papel de la tecnología Blockchain en el aumento de la resiliencia de la cadena de suministro ante el ciberdelito"*Edificios*, vol.11, no.7, pp:1-19, junio de 2021. https://doi.org/10.3390/buildings11070283

[17] Monteith S., Bauer M., Alda M., Geddes J., Whybrow PC y Glenn T., "Aumento del delito cibernético desde la pandemia: Preocupaciones por la psiquiatría"*Informes actuales de psiquiatría*, vol. 23, núm. 18, págs. 1-9, marzo de 2021. https://doi.org/10.1007/s11920-021-01228-w

[18] Al-Khater WA, Al-Maadeed S., Ahmed AA, Sadiq AS, Khan MK, "Revisión integral de las técnicas de detección de delitos cibernéticos",*Acceso IEEE*, págs: 137293 - 137311, julio de 2020. https://doi.org/10.1109/ACCESO.2020.3011259

[19] Narwal B., Mohapatra AK y Usmani KA, "Hacia una taxonomía de amenazas cibernéticas contra aplicaciones objetivo",*Revista de Estadística y Sistemas de Gestión*, vol.22, no.2, pp: 301-325, marzo de 2019. https://doi.org/10.1080/09720510.2019.1580907

[20] Aggarwal, K., Mijwil, MM, Sonia, Al-Mistarehi, AH., Alomari, S., Gök M., Alaabdin, AM y Abdulrhman, SH, "¿Ha comenzado el futuro? El crecimiento actual de la inteligencia artificial, el aprendizaje automático y el aprendizaje profundo",*Revista iraquí de informática y matemáticas*, vol.3, no.1, pp:115-123, enero de 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[21] Al Azzam SBN, "El algoritmo de inteligencia artificial para el cifrado de texto mediante esteganografía",*Revista mesopotámica de ciberseguridad*, vol.2020, págs: 18-27, 2020.https://doi.org/10.58496/MJCS/2022/003

[22]Mijwil MM, Salem IE e Ismaeel MM, "La importancia del aprendizaje automático y las técnicas de aprendizaje profundo en ciberseguridad: una revisión completa"*Revista iraquí de informática y matemáticas*, vol.4, no.1, En prensa, enero de 2023.https://doi.org/10.52866/ijcsm.2023.01.01.008

[23] Mijwil MM, Aggarwal K., Doshi R., Hiran KK y Gök M., "La distinción entre R-CNN y Fast R-CNN en el análisis de imágenes: una comparación de rendimiento"*Revista asiática de ciencias aplicadas*, vol.10, no.5, pp:429- 437, noviembre de 2022.https://doi.org/10.24203/ajas.v10i5.7064

[24] Muhammad T. y Ghafory H., "Detección de ataques de inyección SQL mediante algoritmo de aprendizaje automático" *revista mesopotámica de ciberseguridad*, vol.2022, págs: 5-17, 2022.https://doi.org/10.58496/MJCS/2022/002

[25] Mustaffa SNFNB y Farhan M., "Detección de ataques de inyección de datos falsos mediante el enfoque de aprendizaje automático"*Revista mesopotámica de ciberseguridad*, vol. 2022, págs.: 38–46, julio de 2022. https://doi.org/10.58496/MJCS/2022/005

[26]Mijwil MM, Filali Y., Aljanabi M., Bounabi M., Al-Shahwani H. y ChatGpt "El propósito de la ciberseguridad en la transformación digital de los servicios públicos y la protección del entorno digital",*revista mesopotámica de ciberseguridad*, vol.2022, págs: 1-5, 2022.

[27] Alwan AH y Kashmar AH, "Modelo FCNN para diagnóstico y análisis de criptosistema de clave simétrica", *Revista iraquí de informática y matemáticas*, vol. 4, núm. 1, págs. 53–61, noviembre de 2022. https://doi.org/10.52866/ijcsm.2023.01.01.006

[28]Mijwil, MM, "Detección de malware en el sistema operativo Android mediante técnicas de aprendizaje automático"*Ciencia de datos y aplicaciones*, vol.3, no.2, pp:5-9, 31 de diciembre de 2020.

[29]Mutar DS, "Detección de ataques de redes informáticas mediante tecnologías de agrupación en clústeres mejoradas"*revista asiática de ciencias aplicadas,*vol. 9, no.6, pp:392-396, diciembre 2021.https://doi.org/10.24203/ajas.v9i6.6839

[30] Alajanbi M., Ismail MA, Hasan RA y Sulaiman J., "Detección de intrusos: una revisión"*Revista mesopotámica de ciberseguridad*, vol.2021, pp:1-4, enero de 2021.https://doi.org/10.58496/MJCS/2021/001

[31] Aljanabi, M. ., Mohanad Ghazi, Ahmed Hussein Ali, Saad Abas Abed y ChatGpt. (2023). ChatGpt: posibilidades abiertas. Revista iraquí de informática y matemáticas, 4 (1), 62–64. https://doi.org/10.52866/ijcsm.2023.01.01.0018