MODELO DE GESTIÓN PARA LA ATENCIÓN Y RESPUESTA ANTE ATAQUES DE RANSOMWARE EN EL ÁREA DE NETWORKING

MANAGEMENT MODEL FOR ATTENTION AND RESPONSE TO RANSOMWARE ATTACKS IN THE NETWORKING AREA

Recibido/Received: 31/06/2024 **Aceptado/Accepted:** 30/08/2024

AUTORES

	Vanessa García Pineda. Docente tiempo completo e investigadora del Instituto Tecnológico Metropolitano. Ingeniera en Telecomunicaciones y Magíster en gestión de innovación tecnológica, cooperación y desarrollo regional.
Edison Andrés Zapata Ochoa. Docente e investigador del Instituto Tecnológico Metropolitano. Msc Automatización y Control.	**Juan Camilo Gallego Gómez.** Ingeniero Networking - Especialista en Ciberseguridad. Profesor e investigador del del Instituto Tecnológico Metropolitano.
Luis Alberto Flórez Laverde. Ingeniero de Telecomunicaciones, Magíster en gestión de innovación tecnológica, cooperación y desarrollo regional.	**Jackeline Andrea Macías Urrego.** Docente e investigadora del Instituto Tecnológico Metropolitano. Ingeniera de Telecomunicaciones, Magíster en gestión de innovación tecnológica, cooperación y desarrollo regional.

Semillero de Antenas y Comunicaciones Inalámbricas
Grupo de investigación Automática, Electrónica y Ciencias Computacionales
Ciencias Administrativas
Instituto Tecnológico Metropolitano – ITM

Para citar este artículo: García Pineda, V., Zapata Ochoa, E.A., Gallego Gómez, J.C., Flórez Laverde, L.A. y Macías Urrego, J.A. (2025). Modelo de gestión para la atención y respuesta ante ataques de ransomware en el área de networking. *Revista Sapientía, 17(33),* 25-39. Doi: 10.54278/sapientia.v17i33.263

RESUMEN

En la era actual de avances tecnológicos, el uso frecuente de servicios en la nube por parte de organizaciones y empresas ha brindado agilidad y comodidad a usuarios y colaboradores. Sin embargo, esta tendencia conlleva la exposición de datos tanto de usuarios como de organizaciones, haciéndolos vulnerables a ciberataques principalmente de ransomware, lo que ha despertado la creciente preocupación por la seguridad de los datos. En respuesta a esta amenaza, las organizaciones han reconocido la importancia de tomar medidas para proteger los datos y prevenir ataques cibernéticos. Este estudio propone un modelo de gestión para la respuesta ante ataques de ransomware en entornos de redes. La metodología se divide en dos fases: revisión de literatura, revisión y formulación del modelo. Los resultados identifican variables clave como técnicas de inteligencia artificial, modelos predictivos, y herramientas de monitoreo de seguridad. La discusión resalta la efectividad del modelo en la detección temprana y prevención de ataques, y la importancia de la capacitación del personal. A pesar de sus limitaciones, el modelo proporciona un marco robusto para mitigar riesgos y garantizar la continuidad operativa. Este estudio contribuye significativamente a la mejora de la ciberseguridad en redes organizacionales, ofreciendo un enfoque integral y adaptable frente a amenazas de ransomware.

PALABRAS CLAVE

Ataque cibernético, Ciberseguridad, Modelo de gestión, Ransomware, Redes de comunicaciones.

ABSTRACT

In the current era of technological advances, the frequent use of cloud services by organizations and companies has provided agility and convenience to users and collaborators. However, this trend entails the exposure of data of both users and organizations, making them vulnerable to cyber-attacks, mainly ransomware, which has raised growing concerns about data security. In response to this threat, organizations have recognized the importance of taking steps to protect data and prevent cyber-attacks. This study proposes a management model for responding to ransomware attacks in network environments. The methodology is divided into two phases: literature review, model review and formulation. The results identify key variables such as artificial intelligence techniques, predictive models, and security monitoring tools. The discussion highlights the effectiveness of the model in early detection and prevention of attacks, and the importance of staff training. Despite its limitations, the model provides a robust framework to mitigate risks and ensure operational continuity. This study contributes significantly to the improvement of cybersecurity in organizational networks, offering a comprehensive and adaptable approach to ransomware threats.

KEYWORDS

Cyber-attack, Cybersecurity, Management model, Ransomware, Communications networks

MARCO TEÓRICO

En los últimos años, el avance tecnológico ha llevado a las organizaciones y empresas a utilizar servicios en la nube con más frecuencia, con el fin de dar a sus usuarios y colaboradores agilidad y facilidad en el momento de adquirir y usar cualquier servicio. Lo anterior, implica que los datos tanto de los usuarios como de las organizaciones estén disponibles en la red, lo que los expone y los hace más vulnerables a ciberataques. Esto lleva a las organizaciones a pensar más en la protección de los datos de los usuarios. En este sentido, actualmente para las organizaciones es muy importante tomar medidas activas destinadas a salvaguardar la información confidencial tanto de los usuarios como de la propia empresa, así como a prevenir posibles ataques cibernéticos, dado que esto se ha vuelto fundamental en la gestión de cualquier organización (Oakley, 2020). De esta manera, se entiende un ciberataque como una acción maliciosa y premeditada por parte de un individuo o grupo con la intención de violar la seguridad del sistema informático de una organización (Kaspersky, 2023). Por lo general, el atacante busca obtener ganancias monetarias mediante la interrupción de la red, donde su principal meta es acceder a la información confidencial de la empresa. Al lograr obtener esta información, su intención principal suele ser presionar a la organización, ya sea para filtrarla, secuestrarla o llevar a cabo cualquier otra acción ilegal que pueda causar perjuicio a la empresa.

En diferentes sectores y a nivel mundial, los ciberataques han representado un desafío significativo. Por ejemplo, según reportes de la BBC en 2023, un grupo de ciberdelincuentes activos, potencialmente con base en Rusia, han puesto en jaque a varias organizaciones a nivel global mediante un extenso ataque cibernético. Este grupo, conocido como Clop, ha emitido una advertencia en la dark web dirigida a las empresas víctimas del ataque al software MOVEit. Este grupo notificaron que, de no establecer comunicación para negociar antes del 14 de junio, divulgarán los datos obtenidos. Más de 100,000 empleados de empresas como BBC, British Airways y Boots han sido alertados sobre la posible exposición de datos personales y financieros (Tidy, 2023).

En Colombia, se han reportado varios incidentes de ciberataques que han impactado diversos sectores, incluyendo salud, entidades públicas y empresas privadas como Nutresa, EPM y Colsanitas. Esto se atribuye principalmente a la falta de preparación y conocimiento en el ámbito de la ciberseguridad (Osorio, 2022). Un método de ataque ampliamente utilizado en el país es el ransomware, cuyas primeras variantes datan de finales de la década de 1980 (Tandon & Nayyar, 2020). Esta táctica se basa en cifrar la información y amenazar con su exposición pública, exigiendo un pago generalmente en criptomonedas para desbloquear los datos o, de lo contrario, hacerlos públicos, lo que podría dañar la reputación de la empresa (IBM, 2022).

El ransomware se aprovecha de la dependencia cada vez mayor de las personas de la tecnología moderna y las aplicaciones. Constituye un nuevo modelo de negocio que se deriva de antiguos conceptos de extorsión. Este modelo explota la creciente necesidad y dependencia de las organizaciones e individuos de sus datos, negándoles acceso y solicitando un rescate a cambio de la restauración de dichos datos (Cybersecurity, 2016). Algunos ejemplos de ransomware mencionados por Kaspersky, (2022) incluyen WannaCry, CryptoLocker, NotPetya, Bad Rabbit y REvil: Revil, Ryuk.

Existen diversas técnicas y amenazas adicionales que pueden comprometer la seguridad de los sistemas informáticos de las organizaciones. Una de ellas es el Botnet, que consiste en una red de dispositivos infectados con software malicioso, usualmente un virus. Los atacantes pueden controlar un botnet como un grupo sin el conocimiento del propietario, con el objetivo de aumentar la magnitud de los ataques, como los de denegación de servicio distribuido (DDoS) para interrumpir las operaciones de las compañías (Kaspersky, 2023).

Otra amenaza común es el malware, una de las formas más sofisticadas de ataque en el ámbito cibernético. Un desafío clave en la detección y clasificación del malware radica en la alta variabilidad y similitud del código malicioso (Bu & Cho, 2023). Según Bu & Cho (2023), el malware opera comprometiendo las redes a través de vulnerabilidades, generalmente cuando un usuario hace clic en un enlace sospechoso o descarga un archivo adjunto de un correo electrónico, lo que resulta en la instalación de software malicioso. Una vez dentro del sistema, el malware puede llevar a cabo diversas acciones maliciosas, como bloquear el acceso a componentes clave de la red, robar información mediante la transmisión de datos del disco duro, alterar componentes críticos o llevar a cabo suplantación de identidad (phishing), entre otros (Red Hat, 2018).

Otro método de ataque es la denegación de servicio (DDoS), un ataque en el que un gran número de atacantes desde diversas ubicaciones lanzan

simultáneamente ataques contra un objetivo específico, abrumando la funcionalidad de los usuarios legítimos (Li et al., 2023). El objetivo de este tipo de ataque es saturar los sistemas, servidores o redes con tráfico para agotar los recursos y el ancho de banda, lo que impide que el sistema pueda procesar solicitudes legítimas. Además, los atacantes suelen utilizar múltiples dispositivos comprometidos para llevar a cabo el ataque (Li et al., 2023). Otro tipo de ataque es la inyección de lenguaje de consulta estructurado (SQL), en la cual un atacante inserta código malicioso en un servidor que utiliza SQL, obligando al servidor a revelar información confidencial que normalmente no compartiría. Esta técnica puede aprovecharse manipulando las solicitudes de DNS para exfiltrar datos de un sistema (CloudFlare, 2022).

Asimismo, los ataques de día cero representan una amenaza ya que ocurren antes de que el objetivo sea consciente de la vulnerabilidad existente. En este tipo de ataque, el perpetrador libera malware antes de que el desarrollador o proveedor pueda desarrollar un parche para corregir dicha vulnerabilidad, lo que expone a sistemas vulnerables (Gonzalez, 2023). Por otro lado, la tunelización de DNS utiliza el protocolo DNS para transmitir tráfico que no está relacionado con DNS a través del puerto 53. Este método permite enviar tráfico HTTP y de otros protocolos a través de DNS, lo que puede ser utilizado de forma maliciosa para ocultar datos de una conexión a Internet, manipulando las solicitudes de DNS para extraer información del sistema (CISCO, 2006).

La proliferación de sistemas de red y la rápida adopción de aplicaciones tecnológicas han impulsado un crecimiento exponencial de los delitos cibernéticos, que involucran tácticas como phishing, hacking y propagación de malware. Las técnicas empleadas en estos ciberataques pueden generar efectos no deseados que podrían reducir el número de víctimas dispuestas a pagar el rescate exigido por los atacantes. Para prevenir estas situaciones, proponen la utilización de estrategias como la optimización Water Moth Flame (WMFO) y el empleo de redes neuronales recurrentes profundas para identificar y contrarrestar el ransomware (Nalinipriya et al., 2022).

Por otro lado, la incorporación de la organización definida por software (SDN) supone una simplificación y centralización en la gestión de grandes redes empresariales. Los beneficios de la SDN incluyen la programabilidad del tráfico, la preparación y la capacidad de implementar estrategias personalizadas para supervisar y automatizar la red. Este enfoque permite a los administradores gestionar toda la empresa de manera cohesiva y eficiente, independientemente de la estructura de la red subyacente (Anand & Ganeshwari, 2022). Estudios detallados han analizado los patrones de ransomware y malware mediante estrategias SDN, destinadas a mitigar los riesgos asociados con estos tipos de ciberataques (Anand & Ganeshwari, 2022).

Los ciberataques son considerados el quinto riesgo más alto en 2021 y se han establecido como un desafío creciente tanto para empresas públicas como privadas. Se espera que la incidencia de ciberataques a dispositivos de IoT (Internet de las Cosas) se duplique para 2025, ya que la expansión de la tecnología ha llevado a una mayor conectividad de dispositivos, lo que resulta en un incremento de incidentes de seguridad. Se pronostica que más de la mitad de los datos generados y procesados por las empresas para 2025 se gestionarán en ambientes fuera de las infraestructuras tradicionales de centro de datos o nube (Duque, 2023). Los delincuentes cibernéticos se mantienen constantemente a la búsqueda de oportunidades para explotar vulnerabilidades en individuos y organizaciones, adaptando rápidamente nuevas técnicas y tácticas, así como colaborando estrechamente entre sí (Garcia-Holgado et al., 2018). Entre 2018 y 2022, una parte significativa de las organizaciones ha experimentado un aumento en la frecuencia de ataques recibidos en comparación con años anteriores (ISACA, 2022). Esta realidad ha despertado una creciente preocupación a nivel internacional, en particular en los países de América Latina y el Caribe (OAS, 2022).

En consecuencia, es esencial implementar estrategias que permitan prevenir y responder de manera efectiva a los ataques de ransomware en las redes corporativas. Esto implica llevar a cabo un análisis detallado del tráfico de red, que incluye la detección de protocolos como ARP, la inspección de encabezados de paquetes, el uso de honeypots y la verificación del SMB, entre otras medidas (Sibi Chakkaravarthy et al., 2020). Un enfoque integral que incorpore metodologías y procedimientos eficaces puede contribuir significativamente a mitigar el impacto de un ataque de ransomware, asegurando la continuidad operativa de las organizaciones y fortaleciendo su resiliencia frente a tales amenazas. Este enfoque también plantea la formulación de un modelo de gestión derivado de la categorización de factores identificados en la literatura, destinado a mejorar la preparación y respuesta ante ataques de ransomware en el ámbito de la red de sistemas informáticos.

Por último, los avances en tecnologías como Inteligencia Artificial (IA) y Big Data han abierto

nuevas posibilidades en la predicción de congestión de tráfico, dando lugar a diseños innovadores como antenas reconfigurables en frecuencia para redes móviles 5G, agentes inteligentes para la creación de perfiles de tráfico en tiempo real, detección de intrusiones basada en algoritmos de aprendizaje automático, modelado de amenazas a la privacidad en sistemas de búsqueda personalizados, y sistemas mejorados de detección de intrusiones basados en la red, entre otros (NISS, 2021). Estas herramientas han permitido desarrollar soluciones efectivas para mitigar ataques a las redes informáticas de las organizaciones, brindando una capa adicional de seguridad en un entorno cada vez más vulnerable a las amenazas cibernéticas.

METODOLOGÍA

A continuación, se describe el desarrollo y enfoque metodológico que se llevó cabo con el fin de determinar los factores que permiten brindar atención y respuesta ante ataques de ransomware en el área de networking. De esta manera se presentan a continuación los diferentes métodos y pasos propuestos para el alcance del objetivo de la investigación:

Fase 1 - Revisión de Literatura

Las revisiones de literatura constituyen una forma de investigación observacional que sintetiza los resultados de múltiples estudios primarios. Su propósito fundamental es resumir la información disponible sobre un tema específico y determinar las variables clave y causales que respaldan la investigación (García Pineda & Macías Urrego, 2021). Para llevar a cabo una revisión de literatura exhaustiva, se seguirán los siguientes cinco pasos propuestos por Beltrán (2005):

- Formular una pregunta de investigación clara que responda al propósito de la investigación. En este caso, la pregunta sería: " ¿Qué factores son necesarios para definir un modelo de gestión que permita la atención y respuesta ante ataques de ransomware en el área de networking?".

- Establecer los criterios de inclusión y exclusión de los estudios. Únicamente se considerarán los artículos que se centren específicamente en ciberseguridad y networking.

- Definir la estrategia de búsqueda. Se seleccionarán bases de datos que incluyan revistas de todos los campos del conocimiento y de todas las regiones. Además, se desarrollarán ecuaciones de búsqueda adecuadas para cada base de datos.

- Registrar los datos y evaluar los documentos seleccionados. Los artículos se elegirán conforme a la cantidad de citaciones, su relación con las ciencias computacionales, seguridad e ingenierías, y la relevancia del contenido en lo que respecta al área de networking.

- Interpretar y presentar los resultados. Se analizarán los resultados de acuerdo con los criterios de inclusión y exclusión, y la información se organizará en una base de datos en Excel siguiendo categorías específicas para su posterior análisis y aplicación.

Fase 2 - Formulación

Después de completar cada una de las fases previamente mencionadas, se avanzará hacia la formulación de un modelo a partir de la información recopilada a través de los factores y estrategias que permitan la atención y respuesta ante ataques de ransomware en el área de networking". Esto se llevará a cabo siguiendo los pasos siguientes:

- Identificación de los resultados obtenidos en todas las etapas previas.
- Evaluación y debate de los resultados.
- Análisis en profundidad de los resultados.
- Formulación de una un modelo que permita la gestión ante ataques de ransomware a partir de los factores, recomendaciones variables y características encontradas que se pueden aplicar en el área de networking.

RESULTADOS

Fase 1 - Revisión Sistemática de Literatura

Siguiendo los criterios definidos para la estrategia de búsqueda, la ecuación de búsqueda empleada en Scopus es la siguiente:

TITLE (ransom* AND network*)

Con esta se obtienen 77 documentos, sin embargo, para cumplir con los criterios de inclusión y exclusión, se filtra por área de conocimiento, incluyendo solo documentos en las áreas de ingeniería, ciencias computacionales, y ciencias de la decisión, con lo que se obtienen 76 resultados.

Además, se incluyen solo los documentos correspondientes a los últimos 5 años, es decir a partir del 2019 y solo se tienen en cuenta documentos tipo artículos, con lo que los resultados se reducen a 27 documentos finales.

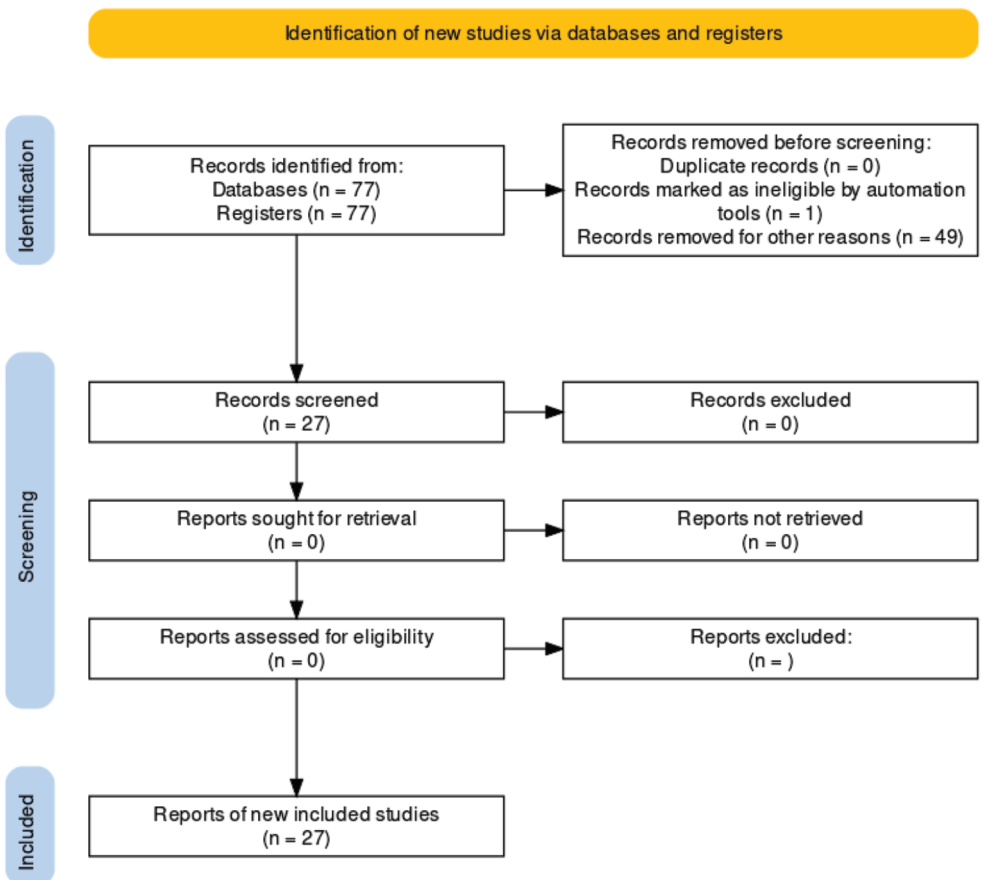
Estrategia de búsqueda:

A partir de los criterios definidos anteriormente, la estrategia de búsqueda queda finalmente de la siguiente manera:

TITLE (ransom* AND network*) AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "DECI"))

Esta estrategia también se limitó a que los términos o palabras clave buscadas se encontrarán específicamente en el título, lo cual permite que la búsqueda sea más refinada y reduce el sesgo en los resultados obtenidos. De esta manera, la metodología siguiendo la estructura PRISMA y estrategia de búsqueda se puede ver reflejada en la Figura 1.

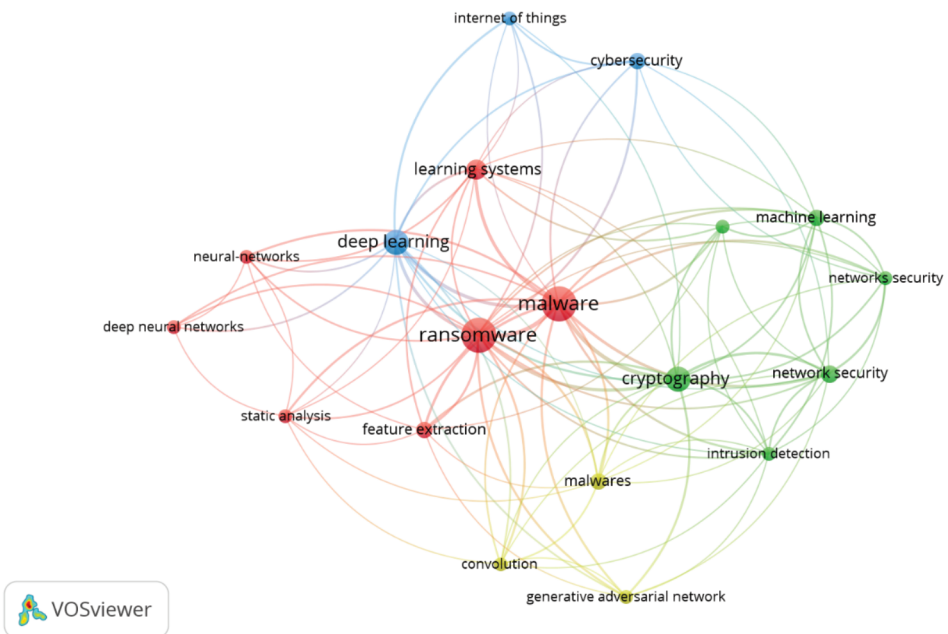
Figura 1. *Estructura de búsqueda*



A partir de estos resultados se analizan los 27 documentos y se analizan los términos clave, así como aquellas variables clave que permitirán la definición de un modelo de gestión que permita la atención y respuesta ante ataques de ransomware en el área de networking. Inicialmente, se analiza la red de palabras clave, lo que permite comprender cuales son los factores que posiblemente estén interactuando de la gestión en términos de ataques de ransomware y networking, esto permitirá comprender que variables se deben tener en cuenta en términos de tendencias para la definición del modelo, como se puede observar en la Figura 2.

Se puede observar que existe una fuerte relación entre los términos malware, ransomware, extracción de características análisis estadístico y redes neuronales. Un segundo clúster corresponde a los términos criptografía, seguridad en la red, detección de intrusión, y machine learning. El tercer clúster está compuesto por red adversarial generativa, malware y convolución y el último clúster lo componen internet de las cosas, ciberseguridad y deep learning.

Figura 2. *Co-ocurrencia de palabras clave*



Por otro lado, se observaron también las tendencias temáticas con el fin de definir el enfoque principal de las variables que harán parte del modelo, como se observa en la Figura 3. En esta figura se puede observar como el término neural es el más reciente surgiendo aproximadamente en el año 2023, seguido de convolucional que también surge en 2023, pero no con la misma fuerza que neural. El término 2022 surgió aproximadamente en el año 2021 siendo el más relevante seguidos de network y detección que tienen su fecha de aparición en el mismo año, los tres términos tienen su mayor relevancia en el año 2022.

Figura 3. *Términos tendencia de acuerdo con su año de mayor vigencia y aparición.*

Fase 2 - Formulación

En esta fase se realizó el análisis de las variables encontradas en los diferentes artículos, teniendo en cuenta la herramienta, tipo de ransomware y la variable de ataque. Para estas variables se encontraron las definiciones como se presenta en la Tabla 1.

Tabla 1. *Definición de variables propuestas para el diseño del modelo a partir de la revisión sistemática de literatura.*

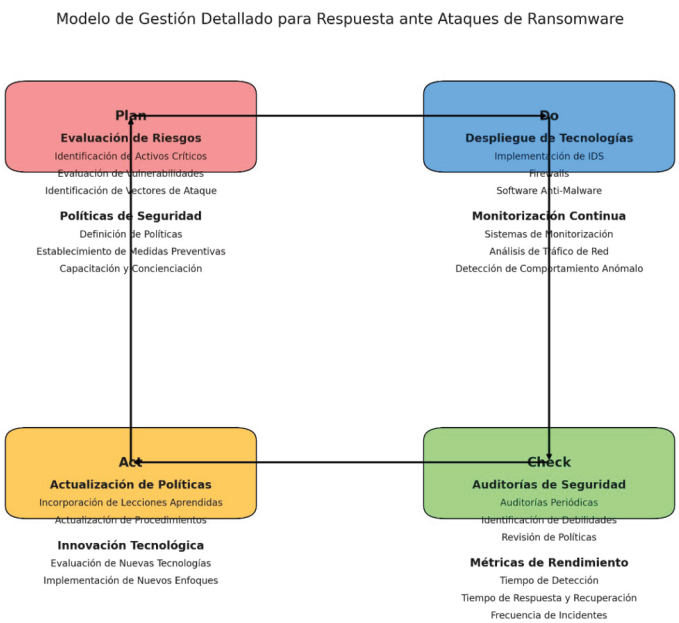
Nº	Tipo de Ransomware	Definición de Ransomware	Herramienta	Definición de Herramienta	Ataque	Ref.
1	Varios	Los autores mencionan que su segundo conjunto de datos incluye 1023 muestras de ransomware agrupadas en 25 familias activas y relevantes, tales como Cerber, Locky, TorrentLocker, TeslaCrypt, entre otros	Red neuronal convolucional Xception	Xception ColSeq	Detección preventiva	Moreira et al. (2023)
2	Malware	Tipo de malware que infecta a los usuarios y hace que sus archivos sean inaccesibles, exigiendo un rescate para su recuperación.	SINN-RD (Spline Interpolation envisioned Neural Network-based Ransomware Detection Scheme)	Mecanismo basado en la detección de tráfico de red utilizando un modelo de red neuronal artificial (ANN) que predice si el tráfico es malicioso o benigno	Detección preventiva	Singh et al. (2023)
3	Varios	Se mencionan diferentes tipos de ransomware entre los cuales están; TeslaCrypt, Petya, WannaCry, Pipeline y LockBit 2.0.	SwiftR	SwiftR está diseñado para detectar ransomware, distinguirlo de otro malware general y atribuirlo a familias de ransomware específicas	Identificación y atribución del ransomware	Karbab et al. (2023)

4	Varios	Se identificación diferentes tipos de ransomware entre los que se encuentran; Maze, Hive, y LockBit.	No se mencionan	Propuesta de modelo	No se indica	Cartwright & Cartwright (2023)
5	Crypto-ransomware	Malware que cifra los datos en el dispositivo de la víctima y demanda un rescate para proporcionar la clave de descifrado. Este tipo de ransomware se caracteriza por el uso de mecanismos criptográficos que hacen irreversible el ataque si no se dispone de la clave de descifrado.	Weighted Generative Adversarial Networks (wGANs)	La técnica de wGANs propuesta es utilizada para detectar el ransomware en su fase previa al cifrado, generando patrones sintéticos de comportamiento que permiten identificar las amenazas antes de que se realicen.	Detección preventiva	Urooj et al. (2024)
6	Crypto-ransomware y Locker ransomware	•Crypto-ransomware: Cifra los documentos clave en el sistema del usuario utilizando métodos de encriptación complicados y exige pagos, generalmente en criptomonedas, para descifrar las credenciales de las víctimas. •Locker ransomware: Muestra una pantalla de bloqueo que impide al usuario abrir su sistema y exige dinero para acceder nuevamente al ordenador.	Red Neuronal Convolucional de Grafos Óptimos (OGCNN-RWD)	Esta técnica utiliza algoritmos de optimización basados en el aprendizaje para la selección de subconjuntos de características y la clasificación del ransomware.	No se menciona	Khalid Alkahtani et al. (2023)
7	Crypto-ransomware	Cifra los archivos de los usuarios y solicita un rescate para recuperar el contenido cifrado.	Técnicas de aprendizaje automático	La herramienta propuesta detecta y bloquea la actividad de crypto-ransomware basada en el análisis del tráfico de archivos compartidos. Utiliza técnicas de aprendizaje automático para identificar patrones en el tráfico que delatan acciones de ransomware mientras se leen y sobrescriben archivos.	Monitoreo del tráfico de red entre clientes y servidores de archivos	Berrueta et al. (2022)
8	Ransomware en android	Ransomware es un tipo de malware que encripta los datos del usuario.	Red Neuronal Convolucional (CNN) basada en imágenes	Transforma un paquete de aplicación de Android (APK) en una imagen en escala de grises, utilizando técnicas de Procesamiento de Lenguaje Natural (NLP) y Hashing Difuso (Fuzzy Hashing) para representar el código descompilado del APK en un conjunto de hashes después del preprocesamiento con técnicas de NLP.	Clasificación y detección	Rodriguez-Bazan et al. (2023)

9	Varios	CC, FileDownload, HeartBeat, PartofHorizontalPortScan, Torii, Okiru, Mirai, y DDoS	No se proporcionan detalles	Modelo llamado AAA-ODBN (Artificial Algae Optimization with Optimal Deep Belief Network)	Se centra en la detección y categorización del ransomware en entornos IoT.	Al Duhayyim et al. (2023)
10	Varios	No se específica	Algoritmo de Red Generativa Adversarial (GAN)	Se utiliza para la predicción del comportamiento del ransomware.	Detección preventiva	Gazzan & Sheldon (2023)

A partir de los términos clave y las variables encontradas en la revisión de literatura es posible proponer el modelo de gestión basados en el estándar ISO 22301 que proporciona un marco para implementar un sistema BCM en empresas de todo tipo y tamaño, permitiendo una respuesta adecuada a incidentes significativos y reduciendo su impacto (ISO, 2019). Este estándar se centra en la identificación y protección de procesos críticos, facilitando la continuidad operativa incluso en condiciones desafiantes. La gestión de la continuidad del negocio se integra con la cultura organizativa, adoptando el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) para planificar, implementar, practicar y mejorar continuamente los procesos. De esta manera, en la Figura 4, se detallan los componentes del modelo.

Figura 4. *Modelo de gestión propuesto para ataques de ransomware.*



Este modelo está basado en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), incluye los criterios de la norma ISO 22301 y describe detalladamente los componentes y actividades asociadas a cada fase, las cuales se describen a continuación:

1. Planificación (Plan)

1.1. Análisis de Contexto y Evaluación de Riesgos

- Identificación de Activos Críticos: Identificar los activos críticos de la red, tales como servidores, bases de datos, y dispositivos de red.

- Evaluación de Riesgos: Realizar una evaluación detallada de los riesgos, identificando vulnerabilidades y posibles vectores de ataque de ransomware.

- Definición de Políticas de Seguridad: Establecer políticas de seguridad claras que incluyan medidas preventivas y de respuesta ante incidentes de ransomware.

1.2. Diseño de Estrategias de Prevención y Detección

- Implementación de Herramientas de Detección: Utilizar herramientas basadas en inteligencia artificial y machine learning, como redes neuronales convolucionales y algoritmos GAN (Generative Adversarial Networks), para la detección temprana de ransomware.

- Capacitación y Concienciación: Desarrollar programas de capacitación para empleados sobre buenas prácticas de seguridad y manejo de incidentes de ransomware.

2.Implementación (Do)

2.1. Desarrollo de Capacidades Operacionales

- Despliegue de Tecnologías de Seguridad: Implementar tecnologías avanzadas de detección y prevención, como sistemas de detección de intrusiones (IDS), firewalls, y software anti-malware.

- Monitorización Continua: Establecer sistemas de monitorización continua del tráfico de red y comportamiento anómalo utilizando técnicas de machine learning y análisis de tráfico de red.

2.2. Configuración y Prueba de Procedimientos de Respuesta

- Procedimientos de Respuesta a Incidentes: Desarrollar y documentar procedimientos detallados de respuesta ante incidentes, incluyendo roles y responsabilidades específicas.

- Simulacros de Incidentes: Realizar simulacros regulares de ataques de ransomware para evaluar la efectividad de los procedimientos y la preparación del equipo.

3. Verificación (Check)

3.1. Auditorías y Revisiones Periódicas

- Auditorías de Seguridad: Realizar auditorías de seguridad periódicas para identificar debilidades en la infraestructura de red y en las políticas de seguridad.

- Revisión de Incidentes: Analizar todos los incidentes de seguridad para identificar patrones y mejorar las estrategias de prevención y respuesta.

3.2. Evaluación de la Eficacia del Modelo

- Métricas de Rendimiento: Establecer métricas de rendimiento para evaluar la eficacia del modelo de gestión, como el tiempo de detección de ransomware, el tiempo de respuesta y recuperación, y la reducción en la frecuencia de incidentes.

4.Mejora Continua (Act)

4.1. Actualización de Políticas y Procedimientos

- Incorporación de Lecciones Aprendidas: Actualizar políticas y procedimientos basados en lecciones aprendidas de incidentes previos y auditorías de seguridad.

- Innovación Tecnológica: Evaluar e incorporar nuevas tecnologías y enfoques de detección y prevención de ransomware.

4.2. Fomento de una Cultura de Seguridad

- Fomento de la Concienciación: Continuar con programas de formación y concienciación para mantener al personal actualizado sobre las mejores prácticas de seguridad.

- Promoción de una Cultura de Seguridad: Integrar la seguridad en la cultura organizacional, promoviendo una actitud proactiva hacia la gestión de riesgos y la respuesta a incidentes.

De esta manera, el uso de tecnologías avanzadas de inteligencia artificial y aprendizaje automático, como las redes neuronales convolucionales y los algoritmos GAN, ha permitido desarrollar capacidades de detección temprana y prevención de ransomware, lo cual es crucial para minimizar el impacto de estos ataques. La implementación de un enfoque basado en el ciclo PDCA y los estándares de la norma ISO 22301 proporciona un marco estructurado para la gestión de la seguridad y la continuidad del negocio. Este enfoque asegura que las organizaciones no solo estén preparadas para prevenir ataques, sino que también tengan procedimientos robustos para responder y recuperarse eficazmente.

Los hallazgos de este estudio están alineados con investigaciones previas que subrayan la importancia de la inteligencia artificial y el aprendizaje automático en la detección de ransomware. Por ejemplo, Anand & Ganeshwari (2022) propusieron el uso de estrategias SDN para mitigar riesgos de ransomware, destacando la relevancia de técnicas avanzadas para la gestión de

redes. Asimismo, Nalinipriya et al. (2022) propusieron la optimización Water Moth Flame (WMFO) y el uso de redes neuronales recurrentes profundas para la detección de ransomware, lo cual coincide con nuestro enfoque en la utilización de algoritmos avanzados para la prevención de ataques.

La revisión de literatura también reveló que la capacitación y la concienciación del personal son fundamentales para la efectividad de cualquier estrategia de seguridad, un aspecto resaltado por Sibi Chakkaravarthy et al. (2020). Esta investigación reafirma que la formación continua y la sensibilización del personal son cruciales para reducir las vulnerabilidades humanas que pueden ser explotadas por los ciberdelincuentes. A pesar de los resultados presentados, este estudio no contempla la variabilidad de los entornos organizacionales. Cada organización tiene una infraestructura de red y un nivel de madurez en ciberseguridad diferente, lo cual puede afectar la aplicabilidad universal del modelo propuesto. Además, la rápida evolución de las amenazas cibernéticas implica que las estrategias de detección y prevención deben ser continuamente actualizadas y adaptadas a nuevas técnicas de ataque.

Otra limitación es la dependencia de datos históricos y patrones conocidos para el entrenamiento de los modelos de inteligencia artificial. Si bien estos modelos son eficaces para detectar ataques basados en patrones previamente identificados, pueden no ser tan efectivos contra nuevas variantes de ransomware que utilizan técnicas completamente innovadoras. Esto subraya la necesidad de una vigilancia constante y la actualización regular de los algoritmos de detección. Como línea de investigación y trabajos futuros podrían centrarse en la integración de tecnologías emergentes como blockchain para fortalecer la seguridad y la resiliencia de las redes contra ataques de ransomware. El blockchain puede proporcionar una capa adicional de seguridad mediante la descentralización y la inmutabilidad de los datos, lo cual podría dificultar la ejecución de ataques exitosos.

También se recomienda explorar la combinación de diferentes técnicas de detección y prevención, como la inteligencia artificial junto con métodos tradicionales de ciberseguridad, para desarrollar un enfoque más robusto y holístico. La colaboración con expertos en ciberseguridad y la participación en foros de intercambio de información sobre amenazas también pueden mejorar significativamente la capacidad de las organizaciones para defenderse contra ransomware y otros tipos de ciberataques.

CONCLUSIONES

La revisión de literatura ha revelado que términos como "redes neuronales convolucionales", "machine learning" y "detección de intrusión" son recurrentes y claves en la investigación actual sobre ciberseguridad. Estos términos indican que las tecnologías basadas en inteligencia artificial son fundamentales para la detección y prevención de ransomware. En el modelo de gestión propuesto, estas tecnologías pueden integrarse como componentes críticos en la fase de implementación. Por ejemplo, la implementación de redes neuronales convolucionales puede mejorar significativamente la capacidad de monitoreo continuo del tráfico de red y la identificación de patrones anómalos, mientras que los algoritmos de machine learning pueden ser utilizados para analizar grandes volúmenes de datos y predecir posibles ataques antes de que ocurran.

Otra variable clave identificada en la literatura es la utilización de técnicas de criptografía y redes generativas adversariales (GAN) para la generación de patrones sintéticos que pueden identificar ransomware en sus etapas iniciales. Estas técnicas son particularmente útiles en la detección preventiva, ya que permiten simular ataques y estudiar sus comportamientos sin comprometer los sistemas reales. Integrar estas técnicas en el modelo de gestión implicaría desarrollar capacidades avanzadas para la simulación y análisis de amenazas en la fase de planificación y diseño de estrategias de prevención. Además, la criptografía puede ser aplicada para asegurar los datos críticos y minimizar el impacto en caso de un ataque exitoso, añadiendo una capa de seguridad adicional en la infraestructura de red de la organización.

Por otro lado, la capacitación continua y la concienciación del personal sobre buenas prácticas de seguridad y manejo de incidentes son fundamentales para la efectividad del modelo de gestión propuesto. Los empleados a menudo representan el eslabón más débil en la cadena de seguridad, y su formación adecuada puede prevenir muchos incidentes de seguridad. Este estudio subraya que una cultura organizacional proactiva en ciberseguridad, complementada con programas de capacitación regulares, es esencial para mitigar las vulnerabilidades humanas explotadas por los ciberataques.

A pesar de las fortalezas del modelo, es esencial reconocer la rápida evolución de las amenazas cibernéticas y la variabilidad de los entornos

organizacionales. El modelo debe ser adaptado continuamente para incorporar nuevas tecnologías y estrategias de detección y prevención. Además, es crucial realizar evaluaciones periódicas y auditorías de seguridad para identificar y corregir debilidades en la infraestructura de red y en las políticas de seguridad. La mejora continua, basada en lecciones aprendidas y avances tecnológicos, es vital para mantener la relevancia y efectividad del modelo frente a las amenazas emergentes.

CONTRIBUCIÓN DE AUTORÍAS

Investigación: Vanessa García Pineda, Edison Andrés Zapata Ochoa, Juan Camilo Gallego Gómez, Luis Alberto Flórez Laverde y Jackeline Andrea Macías Urrego

Redacción – borrador original: Vanessa García Pineda, Edison Andrés Zapata Ochoa, Juan Camilo Gallego Gómez, Luis Alberto Flórez Laverde y Jackeline Andrea Macías Urrego

Redacción – revisión y edición: Vanessa García Pineda, Edison Andrés Zapata Ochoa, Juan Camilo Gallego Gómez, Luis Alberto Flórez Laverde y Jackeline Andrea Macías Urrego

BIBLIOGRAFÍA

Al Duhayyim, M., G. Mohamed, H., Alrowais, F., N. Al-Wesabi, F., Mustafa Hilal, A., & Motwakel, A. (2023). Artificial Algae Optimization with Deep Belief Network Enabled Ransomware Detection in IoT Environment. Computer Systems Science and Engineering, 46(2), 1293–1310. https://doi.org/10.32604/csse.2023.035589

Anand, S., & Ganeshwari, A. (2022). Enhancing Security for IoT Devices using Software Defined Networking (SDN). 2022 International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 130–137. https://doi.org/10.1109/DISCOVER55800.2022.9974896

Beltrán, Ó. A. (2005). Revisiones sistemáticas de la literatura. Revista Colombiana de Gastroenterología, 20, 60–69.

Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. Expert Systems with Applications, 209(July). https://doi.org/10.1016/j.eswa.2022.118299

Bu, S.-J., & Cho, S.-B. (2023). Malware classification with disentangled representation learning of evolutionary triplet network. Neurocomputing, 552, 126534. https://doi.org/10.1016/j.neucom.2023.126534

Cartwright, A., & Cartwright, E. (2023). The Economics of Ransomware Attacks on Integrated Supply Chain Networks. Digital Threats: Research and Practice, 4(4), 1–14. https://doi.org/10.1145/3579647

CISCO. (2006). Configuración del Protocolo de tunelización de la capa 2 (L2TP) por IPSec. https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14122-24.html

CloudFlare. (2022). ¿Qué es la inyección de código SQL? https://www.cloudflare.com/es-es/learning/security/threats/sql-injection/

Cybersecurity, N. (2016). ICS-CERT MONITOR. October. https://www.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep-Oct2016_S508C.pdf

Duque, X. (2023). Ciberseguridad y estándares en el cuidado. El Tiempo. https://www.eltiempo.com/opinion/columnistas/ximena-duque/ciberseguridad-y-estandares-en-el-cuidado-columna-de-ximena-duque-765439

García Pineda, V., & Macías Urrego, J. A. (2021). Analysis of the Variables Leading to the Identification and Incorporation of Innovation Capabilities by Firms in the Colombian ICT Sector. Innovar, 32(84). https://doi.org/10.15446/innovar.v32n84.99867

Garcia-Holgado, A., Mena, J., Garcia-Penalvo, F. J., & Gonzalez, C. (2018). Inclusion of gender perspective in Computer Engineering careers: Elaboration of a questionnaire to assess the gender gap in tertiary education. 2018 IEEE Global Engineering Education Conference (EDUCON), 1547–1554. https://doi.org/10.1109/ EDUCON.2018.8363417

Gazzan, M., & Sheldon, F. T. (2023). An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behavior Prediction. Future Internet, 15(10), 318. https://doi.org/10.3390/fi15100318

Gonzalez, E. (2023). Fortinet alerta de ataques contra organizaciones gubernamentales aprovechando una vulnerabilidad de día cero. Bit Life Media. https://bitlifemedia.com/2023/01/fortinet-ataques-dia-cero/

IBM. (2022). ¿Qué es el ransomware? https://www.ibm.com/mx-es/topics/ransomware ISO. (2019). ISO 22301:2019 GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

Karbab, E. B., Debbabi, M., & Derhab, A. (2023). SwiftR: Cross-platform ransomware fingerprinting using hierarchical neural networks on hybrid features. Expert Systems with Applications, 225, 120017. https://doi.org/10.1016/j.eswa.2023.120017

Kaspersky. (2022). Ransomware Attacks and Types – How Encryption Trojans Differ. https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types Kaspersky. (2023). ¿Qué es un botnet? - Definición. https://latam.kaspersky.com/resource-center/threats/botnet-attacks

Khalid Alkahtani, H., Mahmood, K., Khalid, M., Othman, M., Al Duhayyim, M., Osman, A. E., Alneil, A. A., & Zamani, A. S. (2023). Optimal Graph Convolutional Neural Network-Based Ransomware Detection for Cybersecurity in IoT Environment. Applied Sciences, 13(8), 5167. https://doi.org/10.3390/app13085167

Li, Q., Huang, H., Li, R., Lv, J., Yuan, Z., Ma, L., Han, Y., & Jiang, Y. (2023). A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks, 233, 109895. https://doi.org/10.1016/j.comnet.2023.109895

Moreira, C. C., Moreira, D. C., & Sales Jr., C. de S. de. (2023). Improving ransomware detection based on portable executable header using xception convolutional neural network. Computers & Security, 130, 103265. https://doi.org/10.1016/j.cose.2023.103265

Nalinipriya, G., Balajee, M., Priya, C., & Rajan, C. (2022). Ransomware recognition in blockchain network using water moth flame optimization aware <scp>DRNN</scp>. Concurrency and Computation: Practice and Experience, 34(19). https://doi.org/10.1002/cpe.7047

NISS. (2021). 4th International Conference on Networking, Intelligent Systems and Security, NISS 2021. 4th International Conference on Networking, Intelligent Systems and Security, NISS 2021. https://scopus.bibliotecaitm.elogim.com/record/display.uri?eid=2-s2.0-85116889719&origin=resultslist&sort=plf-f&src=s&sid=dcd054c507aee22c3aa9c6a1c080c196&sot=a&sdt=a&s=TITLEABS%28ransomware+AND+networking%29&sl=36&sessionSearchId=dcd054c507aee22c3aa9c6a

Oakley, J. G. (2020). Cybersecurity for Space. Apress. https://doi.org/10.1007/978-1-4842-5732-6

Osorio, C. (2022). La precaria ciberseguridad de Colombia. https://elpais.com/america-colombia/2022-12-24/la-precaria-ciberseguridad-de-colombia.html

Red Hat. (2018). El concepto de la seguridad de la TI. https://www.redhat.com/es/topics/security

Rodriguez-Bazan, H., Sidorov, G., & Escamilla-Ambrosio, P. J. (2023). Android Ransomware Analysis Using Convolutional Neural Network and Fuzzy Hashing Features. IEEE Access, 11, 121724–121738. https://doi.org/10.1109/ACCESS.2023.3328314

García Pineda – Zapata Ochoa – Gallego Gómez – Flórez Laverde – Macías UrregoSibi Chakkaravarthy, S., Sangeetha, D., Cruz, M. V., Vaidehi, V., & Raman, B. (2020). Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access, 8, 169944–169956. https://doi.org/10.1109/ACCESS.2020.3023764

Singh, J., Sharma, K., Wazid, M., & Das, A. K. (2023). SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme. Computers and Electrical Engineering, 106, 108601. https://doi.org/10.1016/j.compeleceng.2023.108601

Tandon, A., & Nayyar, A. (2020). Data Management, Analytics and Innovation (N. Sharma, A. Chakrabarti, & V. E. Balas, Eds.; Vol. 1042). Springer Singapore. https://doi.org/10.1007/978-981-32-9949-8

Tidy, J. (2023). El masivo ciberataque que amenaza con revelar los datos de empleados de grandes empresas del mundo, incluyendo la BBC. BBC. https://www.bbc.com/mundo/noticias-65834916

Urooj, U., Al-Rimy, B. A. S., Zainal, A. B., Saeed, F., Abdelmaboud, A., & Nagmeldin, W. (2024). Addressing Behavioral Drift in Ransomware Early Detection Through Weighted Generative Adversarial Networks. IEEE Access, 12, 3910–3925. https://doi.org/10.1109/ACCESS.2023.3348451