Uso de *machine learning* en la prevención de amenazas de *ransomware* en bancos

Use of machine learning in the prevention of ransomware threats in banks

Vega Sierra, Jessica Alejandra[1] y Caicedo Rojas, Edisson Rafael[2]
Fundación Universitaria de San Gil - UNISANGIL
Facultad de Ciencias Naturales e Ingeniería, Programa de Ingeniería de Sistemas
Chiquinquirá, Colombia

jalejandravega@unisangil.edu.co
ercaicedo@unisangil.edu.co

Fecha de recepción: julio 13 de 2023
Fecha de aceptación: noviembre 29 de 2023

Resumen - En el siguiente artículo se presenta una revisión bibliográfica acerca de la aplicación de técnicas de *machine learning* para la prevención de amenazas de *ransomware* en entidades bancarias. En primer lugar, se describe la ciberseguridad y la protección de los datos en las organizaciones, así como, el concepto de Triada CID. También se introduce el concepto de *machine lea*rning, una tecnología de inteligencia artificial que se utiliza para identificar patrones en grandes cantidades de datos y hacer predicciones. Luego, se menciona el malware y los diferentes tipos que existen, como virus, spyware, *botnet*, troyanos, *rootkit*, adware, phishing, entre otros. Además, se define el *malware ransomware*. Finalmente, se explican las principales vulnerabilidades de seguridad que enfrentan los bancos, al igual que, se examinan algunas técnicas de *machine learning* utilizadas en la detección del *ransomware* y se destacan las políticas de prevención de incidentes de seguridad en los bancos, que garantizan la protección de la información para prevenir un ciberataque.

Palabras clave – Machine learning, ransomware, seguridad bancaria, seguridad de la información.

Abstract - The following article presents a bibliographical review about the application of Machine Learning techniques for the prevention of ransomware threats in banking entities. First, cybersecurity and data protection in organizations are described, as well as the concept of Triad CID. The concept of Machine Learning, an artificial intelligence technology used to identify patterns in large amounts of data and make predictions, is also introduced. Then, malware and the different types that exist are mentioned, such as viruses, spyware, botnets, Trojans, rootkits, adware, phishing, among others. Also, ransomware malware is defined. Finally, the main security vulnerabilities faced by banks are explained, as well as some Machine Learning techniques used in ransomware detection are examined and security incident prevention policies in banks are highlighted, which guarantee protection information to prevent a cyber attack.

Keywords - Machine learning, ransomware, banking security, information security.

[1] Ingeniero de Sistemas, UNISANGIL.
[2] Ingeniero de Sistemas. Magister en Ingeniería del Software y Sistemas Informáticos. Coordinador de Investigación, UNISANGIL Sede Chiquinquirá.

I. INTRODUCCIÓN

La inteligencia artificial (IA) está en constante avance. Esta disciplina se enfoca en crear máquinas y sistemas que sean capaces de realizar tareas que necesitan una inteligencia humana. El *machine le*arning es una rama de la IA que se caracteriza por la habilidad de los algoritmos para aprender de los datos, identificar patrones y hacer predicciones [1]. En este artículo se abordará la relevancia de la seguridad de la información en la era de la tecnología, y la manera en que el *machine le*arning puede contribuir en la protección de los datos.

Una amenaza para la seguridad de los datos confidenciales es el *malware*, debido a que los ciberdelincuentes buscan obtener ganancias económicas a través de actividades ilegales. La detección temprana de cualquier *malware* ayuda a mitigar el impacto que esto ocasiona para una organización. Existen diferentes categorías de malware como el *ransomware*, un software malicioso que roba la información de un sistema bloqueando o cifrando su contenido, con la intención de exigir un pago de rescate a la víctima [2].

Las organizaciones requieren la implementación de políticas de seguridad para reducir el riesgo de ciberataques, identificar las vulnerabilidades de los sistemas y establecer medidas. Las vulnerabilidades son fallas que pueden ser explotadas por los ciberdelincuentes para efectuar un ataque y comprometer la integridad, confidencialidad y disponibilidad de la información [3]. Las técnicas de *machine learning* son ampliamente utilizadas en la prevención del *ransomware* [4], entre ellas destacan: *Support Vector Machine* (SVM), *Naive Bayes Classifier* (NBC) y *Random* Forest [5], [6]. Estas técnicas son esenciales para evitar los falsos negativos y optimizar el rendimiento de la selección de características y la clasificación.

II. SEGURIDAD DE LA INFORMACIÓN

La ciberseguridad se centra en tomar medidas para la protección de infraestructura, software y hardware, desarrollando estrategias de contraataque, es un "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" [7]. Las políticas y procedimientos se documentan para implementar estrategias de seguridad en una organización [8], y así, evitar pérdidas económicas, inestabilidad social y aumento de la inseguridad virtual [9].

A. Triada CID

El Sistema de gestión de seguridad de la información (SGSI) unifica los criterios para la evaluación de los riesgos de ciberataques en las organizaciones, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información [10].

Confidencialidad: sólo los usuarios autorizados pueden acceder y modificar los datos.

Integridad: garantiza la exactitud y fiabilidad de la información, nadie debe modificar los datos, ya sea accidental o maliciosamente.

Disponibilidad: los usuarios autorizados acceden a los datos en cualquier momento [11].

B. Amenazas y ciberataques

En el entorno cibernético, las amenazas de un sistema inician con los errores o fallos de seguridad que son identificados y detectados por los cibercriminales [12]. Las principales ciberamenazas son ataques que buscan el robo de información sensible o confidencial [13], un ejemplo de ello, es el ciberataque que ocasionó la caída de la planta de energía de Ucrania en 2015, afectando a 225.000 clientes [14].

Según un estudio de la Asociación Colombiana de Ingenieros de Sistemas (ACIS), que realizó una encuesta en 2018 y 2019, concluyó que el 26 % de las organizaciones deben establecer mecanismos de ciberseguridad.

Actualmente, las organizaciones tienen políticas de seguridad, pero es inevitable que se presenten y se materialicen ataques cibernéticos. Como se muestra en la figura 1, el 62% de las empresas se recuperan de un incidente de seguridad en menos de un día, mientras que el 26% lo logra en menos de una hora, pero otras empresas pueden tardar dos o más días en recuperarse [15].

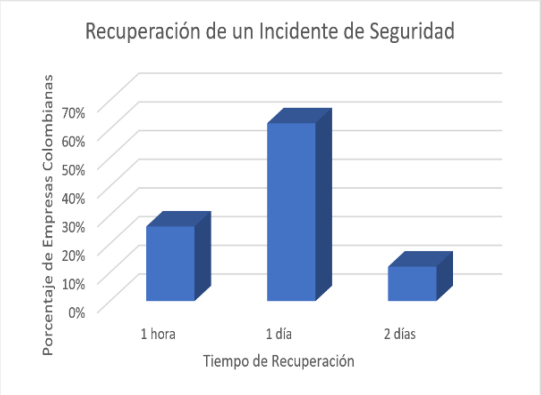

Fig. 1 Relación de las empresas colombianas con el tiempo de recuperación de un incidente de seguridad.

III. MACHINE LEARNING

La IA es una disciplina que tiene la finalidad de "elaborar máquinas y sistemas que puedan desempeñar tareas que requieren una inteligencia humana" [16]. Esta tecnología basada en redes neuronales se caracteriza por el aprendizaje automático y el aprendizaje profundo, los cuales son supervisados por un personal capacitado [16]. Su objetivo es representar la inteligencia del cerebro humano [17].

Machine learning es el proceso de aprendizaje automático que logra identificar patrones entre una cantidad de datos para hacer predicciones. En primer lugar, se ingresan los datos de entrada, luego la máquina aprende de estos datos, evaluándolos y categorizándolos, finalmente, la máquina proporciona salidas de solución al problema [18].

Los algoritmos son capaces de aprender de los datos guardados para optimizar de forma automática el rendimiento de algún proceso [19].

A. Modelos de aprendizaje automático

Se clasifican según el tipo de funcionamiento:

Aprendizaje supervisado: maneja un conjunto de datos previamente etiquetados, entrenando un modelo que asigne etiquetas a nuevos datos. El programador establece las etiquetas.

Aprendizaje reforzado: es utilizado en el análisis de regresión del aprendizaje supervisado, el modelo recibe retroalimentación en forma de calificaciones de precisión, que se emplean para maximizar una recompensa, es decir, el modelo aprende a través de un proceso de prueba y error.

No supervisado: permite procesar datos no estructurados, sin etiquetas y sin necesidad de programar una función de búsqueda. Se trabaja con datos de entrada sin clasificación previa. [20].

En la figura 2 se muestra el proceso de la construcción de un modelo de *machine learning*. Primero, se establecen los datos de ambas categorías, luego, se extraen las características de cada ejemplo de entrenamiento y se representa numéricamente cada muestra, después, en la etapa de entrenamiento, el sistema de aprendizaje automático reconoce patrones específicos en los datos para clasificarlos en alguna categoría, por último, se examina el sistema con datos que no fueron utilizados durante el entrenamiento para evaluar su precisión en la clasificación de nuevos datos [21].

Fig. 2 Proceso de la construcción de un modelo de machine learning [21].

B. Técnicas de machine learning en seguridad de la información

Las técnicas de *machine learning* son utilizadas para identificar y filtrar agentes maliciosos externos, como el filtrado de códigos, URLs, links y correos spam, con el propósito de prevenir infiltraciones externas, asimismo, ayudan a identificar los niveles de riesgo, establecer las vulnerabilidades informáticas y generar modelos clasificatorios y predictivos según los datos almacenados [22], [23].

Los métodos de detección de intrusiones, basados en *machine learning* son:

Sistema de detección de intrusiones (IDS): monitorea el tráfico de red en busca de actividades anormales para prevenir intrusiones en el sistema. Hay dos tipos de IDS: N-IDS, que protege la red, y H-IDS, que protege el host. Los IDS gratuitos como *ModSecurity* y *Snort* manejan reglas para detectar intrusiones, incluyendo inyecciones SQL y XSS [24].

Sistema de detección de intrusiones basado en firmas (SIDS): usa firmas para identificar patrones de ataques conocidos. Las firmas son almacenadas en una base de datos y se comparan con el tráfico de red para detectar posibles intrusiones.

Sistemas de detección de intrusiones basado en anomalías (AIDS): realiza la creación de un perfil normal del sistema utilizando técnicas de modelado, donde se almacenan las

actividades usuales. Luego, se compara este perfil con el comportamiento del sistema en tiempo real y se genera una alerta si no coinciden. Este método detecta nuevos ataques. [25].

Los algoritmos de aprendizaje automático se agrupan por similitud según su función:

1) Algoritmo de regresión: es un proceso de modelado iterativo de la relación entre diferentes variables, que busca minimizar el porcentaje de error en las predicciones.
2) Algoritmo basado en instancias: compara los nuevos datos con una base de datos de ejemplos usando medidas de similitud para hacer una predicción precisa.
3) algoritmo de regularización: simplifica los modelos que son demasiado complejos, para aumentar la capacidad de generalización.
4) Algoritmo de árbol de decisión: es un modelo de toma de decisiones que se construye con valores reales de las características de los datos, se ramifica hasta llegar a la decisión de predicción. Es rápido y preciso.
5) Algoritmo bayesiano: usa específicamente el Teorema de Bayes para resolver problemas de clasificación y regresión.
6) Algoritmo de agrupamiento: clustering, clasifica los datos según su similitud, basado en centroides o jerarquías, busca encontrar patrones intrínsecos en los datos para organizarlos.
7) Algoritmo de aprendizaje de reglas de asociación: encuentra las relaciones significativas entre las variables de un conjunto de datos, lo cual es útil para descubrir asociaciones en conjuntos con gran cantidad de datos multidimensionales.
8) Algoritmo de redes neuronales artificiales: está basado en la estructura o función de las redes neuronales del cerebro humano, se utiliza en problemas de regresión y clasificación. [26].
9) Algoritmo de k vecinos más cercanos: es supervisado y utiliza la distancia entre nodos para clasificar datos. Es conveniente para detectar amenazas en la red, debido a que utiliza condiciones de paquetes y registros de red [27].

IV. MALWARE Y SU CLASIFICACIÓN

El malware o software malicioso, es cualquier programa, software o aplicación informática que infecta y daña de diferentes maneras un sistema informático de forma intencional, consciente y sin la autorización de la víctima [28].

El malware es una amenaza para la seguridad de los datos confidenciales, porque los criminales pretenden obtener ganancias económicas sin importar las actividades ilegales que realicen. La detección oportuna de cualquier malware ayuda a reducir las consecuencias y el impacto que esto puede generar a una organización [29], [30].

Algunos tipos de malware son:

1) Gusano: se reproduce en ordenadores o en las redes, para infectar y destruir el sistema.
2) Spyware: es un malware espía que permanece oculto y captura los datos privados de la víctima para transmitir esta información a un receptor.
3) *Botnet:* también llamado “bot”, puede crear un botnet que infecta a un grupo de ordenadores, controlándolos de manera remota. [31].
4) *Virus:* se activa cuando la víctima lo ejecuta y realiza actividades destructivas en el dispositivo.
5) *Adware:* se instala sin autorización y hace publicidad a través de ventanas emergentes.
6) *Scareware y Crimeware:* intenta engañar a la víctima para convencerla de realizar un pago por tarjeta de crédito para extorsionarla.
7) *Troyanos:* son programas maliciosos que se muestran como algo inofensivo, por ejemplo, publicidad engañosa. Luego de ejecutarse, borran archivos o propagan gusanos por la red. [32].
8) Rootkit: se oculta en el sistema, puede dar acceso de administrador y controlar el sistema.
9) Backdoors: son accesos ocultos que puede tener un dispositivo. Vulneran el proceso de autenticación, accediendo a funciones del ordenador trabajando en segundo plano. [33].
10) Phishing: es una técnica fraudulenta que busca ganar la confianza de la víctima, falsificando la página web de una empresa, con la finalidad de que el receptor del correo electrónico masivo acceda a esta página y suministre las credenciales [34].

Cada tipo de malware se clasifica según la actividad maliciosa, es decir, el vector de ataque. En una organización es conveniente diferenciar cada uno de ellos, para establecer las acciones que se deben efectuar y detener específicamente un ataque [35].

V. RANSOMWARE

El ransomware es un malware que roba la información de un sistema, bloqueando un dispositivo o cifrando su contenido, con la intención de solicitar un pago por el rescate, en caso de que la víctima no acceda a estas peticiones, los ciberdelincuentes borran la información o la subastan en sitios de la darknet [36], [37].

A. Tipos básicos de Ransomware

Este ataque se clasifica en:

Cripto-Ransomware: encripta los archivos y datos de un sistema.
Locker-Ransomware: bloquea el computador u otro dispositivo, evitando que se pueda usar [38].

Las acciones que realiza este malware son: “Cifrado de archivos del disco duro del sistema, bloqueo de cuentas de usuario, bloqueo de programas, bloqueo administrador de tareas, muestra de un mensaje como medio de persuadir al usuario a realizar el pago” [39].

Los atacantes están implementando algoritmos más sofisticados para encriptar los archivos, ocultando el rastro, cambiando la forma de pago y efectuando ataques en la nube, asimismo, se estima que, en algunos años este tipo de ataque sea más destructivo, secuestrando sistemas asociados con infraestructuras críticas de una ciudad o nación [40].

B. Impacto de un ataque ransomware

Un ataque de tipo ransomware afecta la continuidad de negocio; debido a los incidentes relacionados con: la productividad, el costo económico por la pérdida de los activos financieros, la reputación de la empresa y las implicaciones legales por fuga de información confidencial.

En Colombia, este tipo de ataque puede generar pérdidas entre 300 y 5.000 millones de pesos. El 60% de las empresas pymes, no permanecen más de seis meses en el mercado después de sufrir un ciberataque de alto impacto.

Según la compañía internacional de seguridad informática Kaspersky, pagar por el rescate no asegura que los atacantes descifren los archivos, porque solo el 35% de las víctimas que pagan, logran restablecer toda la información, sin embargo, descifrar los archivos no garantiza que se haya eliminado la infección de malware [41], [42], [43].

C. Ransomware bancario

En febrero de 2016, un programa malicioso llamado "Xbot" atacó dispositivos Android en Australia y Rusia, encriptando archivos y robando datos bancarios en línea. Luego, en julio de ese mismo año, se mejoró el sistema del ransomware "Locky" que cifraba archivos incluso si la computadora objetivo no estaba línea. Se estima que este ransomware generó 209000 millones de dólares en los primeros tres meses de 2016 [44].

El troyano bancario para Android llamado "Android LokiBot" toma características de ransomware. Según los investigadores de seguridad de SfyLabs, este malware roba los datos financieros de la víctima, suplantando las aplicaciones bancarias para robar las credenciales y se convierte en ransomware en caso de que la víctima intente quitarle los privilegios de administrador [45].

En la tabla 1, se muestra la clasificación de malware bancario, teniendo en cuenta el listado de familias ransomware, es decir, cada malware tiene señalados con una x los comportamientos de acuerdo a la aplicabilidad. Los comportamientos son:
“1 Registro de teclas pulsadas
2 Captura de formularios
3 Capturas pantalla y grabación de video
4 Inyección campos de formulario fraudulentos
5 Inyección de páginas fraudulentas
6 Redirección de páginas bancarias
7 Registro de teclas pulsadas
8 Hombre-en-el-medio” [46]

En la Tabla 1 se presenta el comportamiento de malware bancario en relación con el listado de familias ransomware.

TABLA 1. COMPORTAMIENTOS DE MALWARE DE FAMILIAS RANSOMWARE [46]

MALWARE	Posibles comportamientos								
Comportamiento	1	2	3	4	5	6	7	8	Total
Cerberus	x	x	x	x		x	x	x	7
Teavtv.apk	x		x		x	x	x		5
Alien	x	x	x			x	x		5
Gustuff	x	x	x			x	x		5
Hydra	x	x	x			x	x		5
BlackRock	x	x	x	x		x	x		6

VI. PREVENCIÓN DE INCIDENTES DE SEGURIDAD EN BANCOS

A. Principales vulnerabilidades

Las vulnerabilidades son un fallo del sistema, entendido como un riesgo que puede permitir que un ciberdelincuente efectúe un ataque, y son causadas por: “fallos de diseño, errores de configuración o carencias de procedimientos” [47].

Los bancos pueden presentar vulnerabilidades como:
1) Poodle (Padding Oracle On Downgraded Legacy Encryption): es una vulnerabilidad en el diseño del SSLv3, descifra las conexiones seguras mediante la manipulación de la transmisión.
2) Cifrados inseguros: presentan debilidades en su diseño y pueden ser descifrados fácilmente por una persona no autorizada.
3) Firma de certificado insegura: es una vulnerabilidad en el algoritmo SHA1 (Secure Hash Algorithm), que permite ataques de colisión (dos entradas diferentes que producen el mismo valor) y posibilita falsificar la firma de un certificado válido.

4) No soporta FS (Forward Secrecy): carencia de FS, el cual garantiza que, si ocurre el robo de la llave maestra, los canales de comunicación anteriores estarán protegidos.

5) SSLv3: es un protocolo de comunicaciones antiguo, vulnerable y oficialmente obsoleto.

6) Protocolos modernos no habilitados: los protocolos de seguridad más recientes no están disponibles en el servidor. También pueden estar actualizados, pero tienen errores como: "Certificados que son caducados, falta de compatibilidad con indicación del nombre de servidor (SNI), certificado que se ha registrado con un nombre de sitio web incorrecto, problemas con la indexación, contenido diferente en HTTP y HTTPS". [48].

B. Ataques bancarios

Los principales ataques bancarios son:

1) Denegación de Servicio (DDoS): colapsa los servidores para dejar inaccesible un servicio, es realizado por bots que controla un ciberatacante, no roba información, pero genera pérdidas económicas.

2) *Códigos dañinos en Puntos de Ventas:* pueden interceptar datos, desviar transacciones o leer información de tarjetas de débito/crédito, ocurren en sistemas de socios como supermercados y son encubiertos con software inofensivo.

3) Watering Hole: infecta sistemas corporativos mediante búsquedas en línea, observando el comportamiento de los empleados en la web, es difícil de rastrear porque redirecciona IP específicas.

4) Explotación de vulnerabilidades: no se realizan actualizaciones y el ciberdelincuente aprovecha las vulnerabilidades para atacar el equipo.

5) Phishing: su objetivo es obtener los datos de la cartera de clientes, haciéndose pasar por una entidad financiera. Los medios utilizados son: "Correo electrónico, Formularios on-site, Fan pages". [49].

C. Técnicas de machine learning en la detección del ransomware

Las técnicas más utilizadas en la prevención del *ransomware* son:

1) Support Vector Machine (SVM) (lineal y no lineal: kernelizado): realiza la clasificación de múltiples clases para maximizar la separación entre ellas mediante vectores de soporte, y si no son linealmente separables, se utiliza el truco del kernel. Es utilizado en aplicaciones de detección de malware donde se busca evitar falsos negativos.

2) Naive Bayes Classifier (NBC): utiliza métodos de clasificación estadística basados en el teorema de Bayes que asume independencia entre las variables predictoras. Proporcionan modelos simples con buen rendimiento, permitiendo calcular la probabilidad posterior de que un evento ocurra, dadas algunas probabilidades anteriores, y son utilizados en la selección de características y clasificación.

3) Random Forest (bosque aleatorio): utiliza conjuntos de árboles de decisión combinados para que cada uno entrene con diferentes muestras de datos, luego, se combinan los resultados de los árboles, donde los errores se compensan y se obtiene una predicción precisa. Es útil en grandes conjuntos de características, como los datos de muestras de atributos de malware, reduce el tiempo de entrenamiento y mejora los tiempos de respuesta.

4) Árbol de decisión, con énfasis en el algoritmo J48: J48 es una herramienta de minería de datos gratuita que implementa el algoritmo C4.5 en Java para generar árboles de decisión. C4.5 usa la minimización de la entropía para clasificar estadísticamente los datos, donde la entropía representa la incertidumbre de las categorías en las muestras, por lo que cuanto mayor sea la entropía, mayor será la incertidumbre y más información se necesitará para clasificar. El algoritmo J48 optimiza el árbol de decisión al utilizar de manera eficiente los atributos de entrada.

5) Deep Neural Network (DNN): es una red neuronal artificial con múltiples capas ocultas que permite modelar relaciones complejas no lineales. Su función es procesar un conjunto de entradas y generar una salida para resolver problemas como la clasificación. El número de capas ocultas puede ser muy alto, lo que hace que el entrenamiento sea computacionalmente costoso. [5], [6].

D. Técnicas de prevención y políticas de seguridad

Las estrategias de seguridad que se pueden implementar son: "Estudio de ataques referentes al sector. Integración de un equipo de Pentesting. Realizar actualizaciones periódicas de todo el software. Utilización de herramientas como software SIEM y/o escáner de debilidades. Monitorizar toda la actividad dentro de la empresa" [49].

"La ISO 27001: 2013 es una norma internacional que proporciona políticas para garantizar la seguridad de la información, esta norma se puede aplicar a cualquier empresa u organización que tenga como prioridad proteger su información" [50].

La norma ISO 27035: 2011 proporciona las mejores prácticas y directrices en la gestión de incidentes de seguridad. El plan de respuesta se basa en: "Detección, notificación y evaluación. Respuesta ágil y rápida a incidentes, con controles preventivos y de respuesta (…). Notificación y anuncio de vulnerabilidades asociadas a los sistemas de manera proactiva (…). Aprendizaje y mejora continua del sistema" [51].

VII. CONCLUSIONES

La seguridad de la información es indispensable en el entorno cibernético, así como la aplicación de políticas y procedimientos de seguridad para prevenir pérdidas económicas y garantizar la protección de los datos. El

modelo de Triada CID unifica los criterios para evaluar los riesgos de ciberataques en las organizaciones. Las vulnerabilidades de seguridad son una realidad en cualquier organización, por eso se deben implementar estrategias de ciberseguridad para salvaguardar la información.

La IA ha permitido la aplicación de técnicas de *machine learning* en la seguridad de la información para identificar y filtrar agentes maliciosos, prevenir infiltraciones externas, identificar niveles de riesgo, establecer vulnerabilidades informáticas y generar modelos clasificatorios y predictivos. Las técnicas de *machine learning* como SVM, NBC y *random forest* se pueden implementar en los sistemas informáticos de los bancos para prevenir incidentes de seguridad relacionados con el *malware ransomware*, con el fin de detectar infiltraciones y amenazas de manera temprana, salvaguardando la información. Además, los bancos deben establecer medidas y políticas de seguridad actualizadas, así como capacitar a los empleados y clientes acerca de las mejores prácticas de seguridad.

REFERENCIAS

[1] F. Alvarez, "Machine Learning en la Detección de Fraudes de Comercio Electrónico aplicado a los Servicios Bancarios," 2020. https://dspace.palermo.edu/ojs/index.php/cyt/article/view/4310

[2] F. Bazante, L. Barona, Á. Valdivieso, and M. Hernández, "Indicadores para la Detección de Ataques Ransomware," 2019. https://www.proquest.com/openview/841aa93ba3c3df451268e843ef187b70/1?pq-origsite=gscholar&cbl=1006393

[3] L. Fernández, "Detección de Bonets y Ransomware en Redes de Datos mediante Técnicas de Aprendizaje Automático," 2019. https://digitum.um.es/digitum/bitstream/10201/73765/1/Lorenzo Fernández Maimó Tesis Doctoral s Art.pdf

[4] F. Bazante, "Análisis de Correlación Automática para Detección de Ataques Ransomware en Ambiente de Pruebas," 2019. https://bibdigital.epn.edu.ec/handle/15000/20121

[5] M. Amariles, S. Vallejo, and W. Úsuga, "Técnica de Machine Learning para la Prevención del Malware-Ransomware," 2021. https://dspace.tdea.edu.co/handle/tdea/2036

[6] O. Cumbicus, P. Ludeña, and L. Neyra, "Técnicas de Machine Learning para la Detección de Ransomware: Revisión Sistemática de Literatura," 2022. https://revistas.utb.edu.ec/index.php/sr/article/view/2684

[7] M. Ospina and P. Sanabria, "Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia," 2020. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lang=es

[8] Y. Llanten, S. Amador, and K. Márceles, "Validación de framework de ciberseguridad para la mitigación de amenazas," 2023. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292022000400200&lang=es

[9] R. Domínguez and R. Vera, "Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca," 2022. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692022000100021&lang=es

[10] D. Carvajal, A. Cardona, and F. Valencia, "Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana," 2019. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672019000100068&lang=es#fn1

[11] T. Martín, "Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001," 2021. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lang=es

[12] M. Álvarez and H. Montoya, "Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos," 2021. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-34612020000200279&lang=es

[13] J. Manuel, "Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad," 2019. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992019000200024&lang=es

[14] S. Quiroz, J. Zapata, and H. Vargas, "Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman," 2020. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-77992020000200243&lang=es

[15] R. Sabillón and J. Cano, "Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones," 2019. http://www.scielo.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200004&lang=es

[16] J. Estupiñán, M. Leyva, A. Peñafiel, and Y. Assafiri, "Inteligencia Artificial y Propiedad Intelectual," 2021. https://rus.ucf.edu.cu/index.php/rus/article/view/2490

[17] Y. Ocaña, L. Valenzuela, and L. Garro, "Inteligencia Artificial y sus Implicaciones en la Educación Superior," 2019. http://www.scielo.org.pe/scielo.php?pid=S2307-79992019000200021&script=sci_arttext

[18] W. Campos, R. Farina, and F. Florian, "Inteligência Artificial: Machine Learning na Gestão Empresarial," 2022. https://www.researchgate.net/publication/361525005_INTELIGENCIA_ARTIFICIAL_MACHINE_LEARNING_NA_GESTAO_EMPRESARIAL

[19] C. Ovalle, "Modelo Predictivo basado en Machine Learning para la Cadena de Suministro y su Influencia en la Gestión Logística de una Empresa de Venta de Autos," 2022. https://www.researchgate.net/publication/359709878_Modelo_predictivo_basado_en_Machine_Learning_para_la_Cadena_de_Suministro_y_su_influencia_en_la_gestion_logistica_de_una_empresa_de_venta_de_autos

[20] N. Amado, "El derecho de Autor en la Inteligencia Artificial de Machine Learning," 2020. https://www.researchgate.net/publication/347614188_El_derecho_de_autor_en_la_Inteligencia_Artificial_de_machine_learning

[21] J. Ortega, "Machine Learning para Proyectos de Seguridad," 2019. https://www.researchgate.net/publication/338823444_Machine_learning_para_proyectos_de_seguridad

[22] N. Luque and M. Ortega, "Análisis de Sistemas para Registros Médicos Electrónicos en Clínicas y su Enfoque al Machine Learning," 2020. http://repositorio.ucsp.edu.pe/bitstream/20.500.12590/16206/4/LUQUE_SUCASAIRE_NOE_MAC.pdf

[23] H. Villar and J. Castro, "Modelo de Evaluación de Riesgos Informáticos basado en Analítica de Datos para la Comunidad Educativa del Centro de Servicios y Gestión Empresarial del SENA Regional Antioquia," 2022. https://www.researchgate.net/publication/360869669_Modelo_de_evaluacion_de_riesgos_informaticos_basado_en_analitica_de_datos_para_la_comunidad_educativa_del_centro_de_servicios_y_gestion_empresarial_del_SENA_Regional_Antioquia#fullTextFileContent

[24] V. Macías, "Diseño de Sistema Prototipo para Análisis de Intrusiones con Técnicas de Machine Learning," 2020. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8213/Trabajo de Grado Victor_Macias_20200703.pdf?sequence=1

[25] N. Sotelo and L. León, "Machine Learning y Seguridad: Detección de Correos Falsos y Detección de Intrusos," 2020. https://repositorio.uniandes.edu.co/handle/1992/51480

[26] J. Correa, C. Henao, F. Henao, and D. García, "Análisis del Aporte del Aprendizaje de Máquinas a la Seguridad de la Información," 2021. https://publicaciones.americana.edu.co/index.php/inam/article/view/407

[27] H. Vargas, "Defensa contra Intrusos en Redes de Dispositivos IoT usando Técnicas de Blockchain y Machine Learning," 2020. https://repositorio.uniandes.edu.co/handle/1992/48617

[28] R. Garcia, "Seguridad Informatica y el malware," 2017. http://repository.unipiloto.edu.co/handle/20.500.12277/2641
[29] A. Silva and M. Pamplona, "On Deceiving Malware Classification with Section Injection," 2023. https://www.researchgate.net/publication/367177125_On_Deceiving_Malware_Classification_with_Section_Injection#fullTextFileContent
[30] L. González and R. Vasquez, "Clasificación de Malware mediante Redes Neuronales Artificiales," 2015. https://www.redalyc.org/pdf/342/34242142004.pdf
[31] D. Muena, "Malware para Dispositivos Móviles (Android)," 2018. https://premios.eset-la.com/universitario/pdf/malaware_para_dispositivos_moviles_android.pdf
[32] F. Gutierrez, C. Ortega, and M. Torres, "MalWare, más allá de los virus informáticos," 2014. https://pistaseducativas.celaya.tecnm.mx/index.php/pistas/article/view/1295
[33] A. Valencia and S. Galicia, "Detección de Malware con Modelo de Lenguaje y su Clasificación mediante SVM Language Model for Malware Detection and Classification based on SVM," 2016. https://www.researchgate.net/publication/314403708_Deteccion_de_malware_con_modelo_de_lenguaje_y_su_clasificacion_mediante_SVM_Language_Model_for_Malware_Detection_and_Classification_based_on_SVM
[34] M. Cueva and D. Alvarado, "Análisis de Certificados SSL/TLS Gratuitos y su Implementación como Mecanismo de Seguridad en Servidores de Aplicación.," 2017. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422017000100273&lang=es
[35] R. Rivera, "Detección y Clasificación de Malware con el Sistema de Análisis de Malware Cuckoo," 2018. https://www.researchgate.net/publication/349061289_Deteccion_y_Clasificacion_de_Malware_con_el_Sistema_de_Analisis_de_Malware_Cuckoo
[36] J. Márquez, "Cybersecurity and Internet of Things. Outlook for this Decade," 2022. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-55462022000301201&lang=es
[37] L. Duarte, J. Álvarez, and D. Preciado, "Evolución del fraude informático: una problemática en las organizaciones bancarias colombianas," 2021. https://dspace.tdea.edu.co/handle/tdea/2331
[38] F. Ávila, "Ransomware, una amenaza latente en Latinoamérica," 2023. https://revistas.ucr.ac.cr/index.php/intersedes/article/view/50765
[39] R. Rivera, "Análisis de características estáticas de ficheros ejecutables para la clasificación de Malware," 2014. https://www.researchgate.net/publication/349061489_Analisis_de_caracteristicas_estaticas_de_ficheros_ejecutables_para_la_clasificacion_de_Malware#fullTextFileContent
[40] J. Márquez, "Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas," 2023. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006&lang=es
[41] J. Pinzón, "Análisis del impacto de los ataques de Ransomware en las organizaciones colombianas como base de conocimiento para la determinación de nuevos mecanismos de protección y minimización de riesgos cibernéticos," 2021. https://repository.unad.edu.co/handle/10596/50093
[42] J. Márquez, "Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad," 2022. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934595
[43] L. Fiquitiva, "Análisis de los ataques tipo Ransomware realizados durante el Covid 19 a las Mipymes colombianas, por causa de vulnerabilidades presentes en las infraestructuras TI y en el proceso de transformación digital en las organizaciones," 2022. https://repository.unad.edu.co/handle/10596/50719
[44] A. Montañez, "El Ransomware y la Cultura de Seguridad," 2022. http://eprints.uanl.mx/23553/1/1080135883.pdf
[45] J. Pérez, "Estudio Monográfico Sobre La Amenaza Ransomware, Su Impacto En Las Organizaciones y Buenas Prácticas Para Su Prevención y Manejo," 2019. https://repository.unad.edu.co/handle/10596/42143
[46] O. Arango, "Detección de amenazas informáticas de tipo Malware Bancario o Ransomware Móvil hacia dispositivos Android, integrando IOC en una técnica semiautomatizada y con base en comportamientos analizados de incidentes," 2022. http://repositorio.itm.edu.co/handle/20.500.12622/5700
[47] E. Guaña and W. Aldaz, "Vulnerabilidad de Seguridad Informática en la Administración Zonal Norte 'Eugenio Espejo' a través del Phishing.," 2019. http://repositorio.uisrael.edu.ec/handle/47000/2301
[48] A. Zambrano and J. Suarez, "La seguridad de las Aplicaciones Bancarias y Dispositivos sin Contacto que permiten efectuar Pagos en Colombia," 2020. https://repository.unimilitar.edu.co/bitstream/handle/10654/36702/ZambranoLoaizaAngieCarolina-SuarezCastroJohanCamilo2020.pdf?sequence=1&isAllowed=y
[49] M. Moreno, "Estudio y puesta en Práctica de Elastic, Métricas y Visualizaciones para Seguridad Informática aplicado al Sector Bancario," 2020. https://crea.ujaen.es/bitstream/10953.1/18113/1/TFM_MorenoTorresMarcosDavid.pdf
[50] C. Astudillo and A. Cabrera, "Políticas de Gestión de Seguridad de la Información, fundamentadas en la Norma ISO/IEC 27001, Centro de Datos diseñado con el Estándar ANSI/TIA 942," 2019. https://dialnet.unirioja.es/servlet/articulo?codigo=7154279
[51] C. Ayala and E. López, "Diseño e Implementación de la ISO 27035 (Gestión de Incidentes de Seguridad de la Información) para el Área de Plataforma de Servicios de una Entidad del Estado Peruano," 2019. https://repositorio.utp.edu.pe/handle/20.500.12867/2477