Sebastián Gómez Sepúlveda, Juan Esteban Vélez Mazo (2024). Ciberseguridad aplicada a la gestión de datos en empresas de bienes y servicios: una revisión de literatura. Cuaderno Activa, 16, 109 a 121.

Cuaderno Activa
• REVISTA CIENTÍFICA DE LA FACULTAD DE INGENIERÍA •

Ciberseguridad aplicada a la gestión de datos en empresas de bienes y servicios: una revisión de literatura

Cybersecurity Applied to Data Management in Goods and Service Companies: a Literature Review

Sebastián Gómez Sepúlveda[1], Juan Esteban Vélez Mazo[2]

Tipo de Artículo: revisión de literatura.
Recibido: 13/11/2024. **Aprobado:** 12/12/2024. **Publicado:** 12/12/2024

Resumen: Este trabajo aborda la necesidad de utilizar encriptadores en empresas de bienes y servicios que enfrentan ciberataques cada vez más crecientes y sofisticados. Aunque la encriptación es clave para proteger la información, muchas organizaciones no invierten en estas herramientas hasta haber sido víctimas de un ataque significativo. El objetivo de esta investigación es evaluar el uso de encriptadores en entornos empresariales y cómo contribuyen a mitigar ataques como *phishing* o los DDoS, analizando tanto sus ventajas como sus limitaciones. Para ello, se realizó una Revisión Sistemática de la Literatura (RSL), seleccionando y analizando estudios que implementaron encriptación en entornos empresariales reales. El hallazgo principal de este trabajo indica que la probabilidad de que una empresa invierta en ciberseguridad aumenta a medida que incrementa la intensidad de los ciberataques. Esto sugiere que, en muchos casos, la inversión en encriptación y ciberseguridad ocurre solo después de un ataque, en lugar de ser una medida preventiva constante.

Palabras clave: criptografía; encriptador; ciberseguridad; hackeo; *phishing*.

Abstract: This work addresses the need for encryptors in service companies facing increasing and sophisticated cyberattacks. While encryption is

[1] *Autor correspondiente: Sebastian Gómez Sepúlveda. Mayor título: Estudiante de Ingeniería de Sistemas. Filiación institucional: Universidad Católica Luis Amigó. País: Colombia, Ciudad: Medellín. Correo electrónico: sebastian.gomezse@amigo.edu.co ORCID: https://orcid.org/0009-0005-2221-5015*

[2] *Autor correspondiente: Juan Esteban Vélez Mazo. Mayor título: Estudiante de Ingeniería de Sistemas. Filiación institucional: Universidad Católica Luis Amigó. País: Colombia, Ciudad: Medellín. Correo electrónico: juan.velezaz@amigo.edu.co ORCID: https://orcid.org/0009-0007-2774-4412*

key to protecting information, many organizations do not invest in these tools until they have been victims of a significant attack. The aim of this research is to evaluate the use of encryptors in businesses and how they help mitigate attacks such as phishing or DDoS, analyzing both their advantages and limitations. A Systematic Literature Review (SLR) was used, selecting and analyzing studies that implemented encryption in real business environments. The main finding indicates that the likelihood of companies investing in cybersecurity increases as cyberattacks grow in severity. This suggests that, in many cases, investment in encryption and cybersecurity occurs only after an attack, rather than being a constant preventive measure.

Keywords: cryptography; encryptor; cybersecurity; hacking; phishing.

I. Introducción

La ciberseguridad es un tema de vital importancia y utilidad en cualquier actividad desarrollada dentro de un sistema informático. Sin embargo, en muchos países en vías de desarrollo, este aspecto ha sido frecuentemente descuidado, dejando múltiples vulnerabilidades abiertas. La falta de atención a la ciberseguridad expone a empresas u organizaciones, a empleados y clientes al riesgo de sustracción de datos confidenciales, generando un entorno de incertidumbre e inseguridad.

La finalidad de este estudio es examinar y sistematizar el conocimiento existente sobre la ciberseguridad, indagando sobre cómo varios autores abordan los diversos componentes involucrados. Se busca identificar las estrategias más eficaces para difundir los beneficios que la ciberseguridad aporta en múltiples ámbitos, así como resaltar la información clave que todo individuo debería conocer para prevenir fallos y protegerse adecuadamente en el ambiente digital.

Inicialmente, se delimitó el tema de investigación. Se realizó un análisis detallado de la documentación disponible en bases de datos institucionales, utilizando términos clave estratégicos para identificar los documentos más relevantes. Posteriormente, se llevó a cabo una revisión minuciosa de los artículos seleccionados, evaluando su contenido en función de las preguntas planteadas. Este enfoque permitió obtener una visión integral del tema que, aunque no cuenta con una amplia documentación, proporcionó información valiosa.

El hallazgo principal de este trabajo fue confirmar que, a mayor intensidad de ciberataques, aumenta la probabilidad de que las organizaciones invirtieran en sistemas de ciberseguridad. Resultados evidencian que las empresas suelen esperar a ser blanco de un ataqune para realizar inversiones significativas en encriptación y seguridad informática.

II. Justificación de la revisión

La ciberseguridad depende en gran medida del uso de sistemas de cifrado de datos para garantizar la confidencialidad e integridad de la información. Entre los métodos tradicionales, el cifrado simétrico es ampliamente utilizado debido a su eficiencia y velocidad en el procesamiento de datos [1]. Por otro lado, el cifrado asimétrico emplea un par de claves para cifrar y descifrar información, lo que permite mejorar la seguridad en las comunicaciones y en la implementación de firmas digitales [2].

En Colombia, las empresas enfrentan desafíos significativos en materia de ciberseguridad, ya que el país se encuentra entre los diez más afectados por ataques de ransomware [3]. Informes recientes han señalado un aumento en los ciberataques dirigidos a sectores críticos, como el educativo, financiero y sanitario, lo que resalta la vulnerabilidad de las organizaciones frente a estas amenazas [4]. Además, muchas empresas colombianas carecen de personal especializado y recursos adecuados para mitigar estos riesgos, lo que agrava aún más la situación.

Las tendencias actuales en ciberseguridad incluyen la integración de inteligencia artificial y aprendizaje automático para mejorar los sistemas de cifrado y detección de amenazas [5]. Asimismo, la adopción de técnicas de encriptación basadas en blockchain

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 111 de 130

ha demostrado proporcionar mayor seguridad y transparencia en la gestión de datos [6]. Estos avances continúan transformando el panorama de la seguridad informática, abordando tanto los desafíos actuales como los futuros en la protección de la información.

III. Formulación de las preguntas de investigación

¿Cuáles son las principales vulnerabilidades de ciberseguridad en las empresas de bienes y servicios?

¿Cómo se han implementado los encriptadores de datos en el sector real?

¿Cuáles son las principales ventajas, desventajas y desafíos en el uso de encriptadores para garantizar la ciberseguridad en las empresas?

IV. Definiciones y conceptos básicos

A continuación, se presentan los conceptos o términos más relevantes en el campo de la ciberseguridad:

Ataques de Día Cero: son ataques que explotan vulnerabilidades de *software* que aún no han sido divulgadas públicamente ni tienen un parche o solución disponible [7].

BOUND DDoS: Distributed Denial-of-Service, (DDoS) es un delito cibernético en el que el atacante satura un servidor con tráfico de Internet para evitar que los usuarios accedan a servicios y sitios en línea conectados [8].

Denegación de servicio: consiste en sobrecargar un sistema con tráfico o solicitudes excesivas, impidiendo que los usuarios legítimos accedan a los servicios [9].

GDPR: el Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679) es una normativa con la que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE) [10].

Ingeniería Social: es una técnica que los hackers emplean para manipular a las personas y obtener información confidencial. A diferencia de otros métodos de ataque cibernético que se centran en las vulnerabilidades técnicas, la ingeniería social se dirige a la psicología humana [11].

ISO 27001: es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI) [12].

***Machine Learning*:** subconjunto de la inteligencia artificial que permite a los sistemas informáticos aprender de los datos, identificar patrones y tomar decisiones con mínima intervención humana [13].

Phishing: tipo de ciberataque que utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para engañar a las personas y hacer que compartan datos confidenciales, descarguen malware o se expongan de otro modo a la ciberdelincuencia [14].

Ransomware: es un tipo de *software* malicioso diseñado para cifrar los datos de la víctima y exigir un rescate a cambio de la clave de descifrado [15].

UNSW-NB15: es un conjunto de datos de intrusión de red [16].

V. Proceso de búsqueda de documentos

Palabras de búsqueda: cybersecurity vulnerabilities, information systems, security breaches, data encryption, applications of data encryption, advantages.

Cadenas o ecuaciones de búsqueda:

TITLE-ABS-KEY (("cybersecurity" AND "vulnerabilities" AND "information systems" AND " security breaches") AND NOT "biosecurity") AND PUBYEAR > 2019 AND PUBYEAR < 2025 AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")) AND (LIMIT-TO (EXACTKEYWORD, "Cyber Security") OR LIMIT-TO (EXACTKEYWORD, "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD, "Security Breaches") OR LIMIT-TO (EXACTKEYWORD, "Vulnerability")) AND (LIMIT-TO (PUBSTAGE, "final")) AND (LIMIT-TO (OA, "all"))

TITLE-ABS-KEY ("data encryption" AND "applications of data encryption") AND PUBYEAR > 2019 AND PUBYEAR < 2024 AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")) AND (LIMIT-TO (DOCTYPE, "ar")) AND (LIMIT-TO (EXACTKEYWORD, "Data Encryption") OR LIMIT-TO (EXACTKEYWORD,"Computer Networks") OR LIMIT-TO (EXACTKEYWORD, "Network Security") OR LIMIT-TO (EXACTKEYWORD, "Cryptography") OR LIMIT-TO (EXACTKEYWORD,"Encryption Technologies"))

TITLE-ABS-KEY ("cybersecurity" AND "data-encryption" AND "advantages") AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")) AND (LIMIT-TO (DOCTYPE, "ar")) AND (LIMIT-TO (EXACTKEYWORD, "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD, "Cryptography") OR LIMIT-TO (EXACTKEYWORD,"Data Encryption") OR LIMIT-TO (EXACTKEYWORD, "Cyber Security"))

Bases de datos empleadas: se utilizaron las siguientes bases de datos para la investigación: Science Direct, Web of Science y Google Academic.

Período de búsqueda: el periodo de búsqueda abarcó desde el año 2020 hasta el 2025.

Criterios de inclusión: que los artículos seleccionados se enfocarán en analizar los ataques presentados en empresas de servicios (*phishing*; DDoS, etc.).

Que los artículos hayan empleado un encriptador o encriptación real en sus empresas u organizaciones.

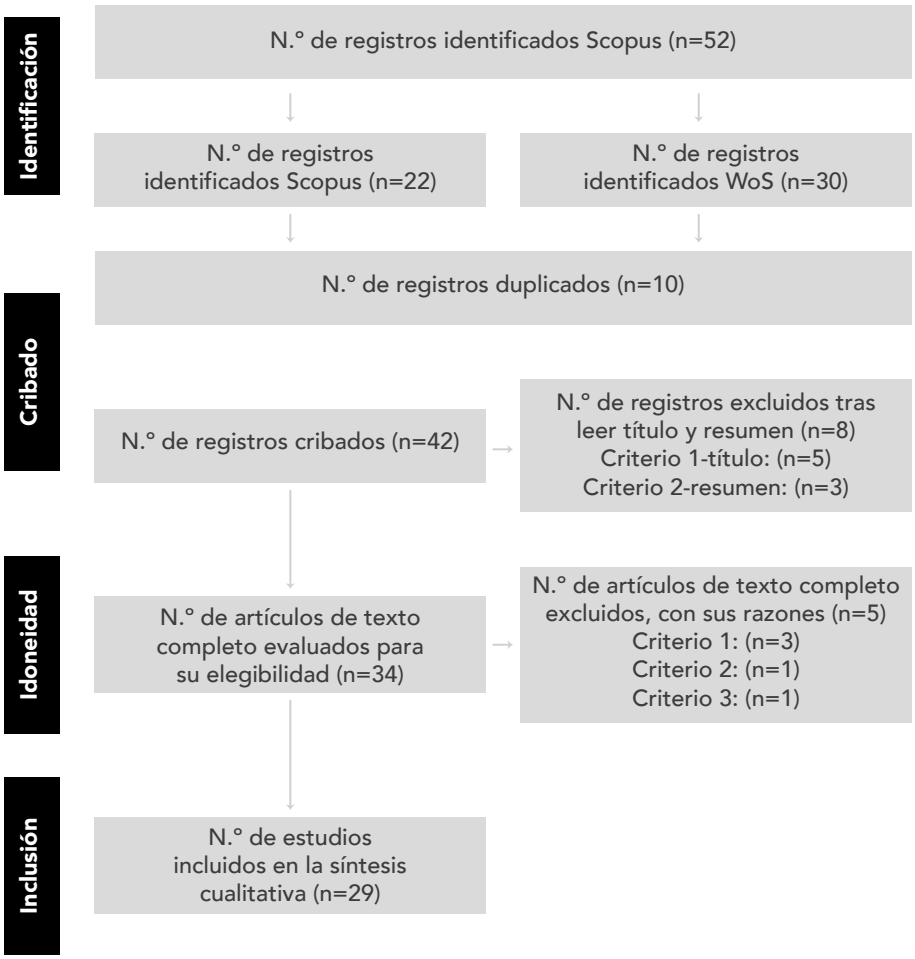
Que los artículos hayan señalado los puntos fuertes o débiles de los encriptadores al ser implementados en sus empresas u organizaciones.

Criterios de exclusión: los artículos que no se enfocaron en analizar ataques específicos (como *phishing* o DDoS) en empresas de servicios, sino que abordaron sobre ataques en sectores distintos (por ejemplo, bioseguridad) o describieron ataques sin detalles específicos aplicables a empresas de servicios. Los artículos que no emplearon ni implementaron encriptadores reales en sus entornos de estudio, sino que trabajaron desde una perspectiva teórica (simulaciones, estudios teóricos sin implementación en empresas) o usaron métodos alternativos de protección (como firewalls o autenticación multifactor sin encriptación).

Los artículos que no evaluaron ni discutieron puntos fuertes o débiles de la encriptación en contexto empresarial. En lugar de eso, se limitaron a describir la implementación básica de encriptadores sin mencionar su efectividad o analizar sólo aspectos técnicos sin impacto específico en la empresa.

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 113 de 130

Figura 1. flujograma Prisma 2020



Nota: fuente elaboración propia.

VI. Discusión

¿Cuáles son las principales vulnerabilidades de ciberseguridad en las empresas de bienes y servicios?

Para esta investigación se referencian las vulnerabilidades más comunes en las empresas, así como los ataques más comunes que realizan personas mal intencionadas o hackers para explotarlas.

El *phishing* es uno de los ataques informáticos más delicados, ya que proviene de la ingeniería social, la cual se encarga de atacar uno de los puntos débiles de cualquier organización: el usuario o trabajador. Estos ataques pueden desembocar en ataques automatizados, como la inyección de ransomware con el objetivo de secuestrar información [17].

La combinación del *phishing* con la falta de preparación de los trabajadores en las empresas genera se llega a una de las mayores vulnerabilidades: los ataques por correos electrónicos, dado que todas las empresas utilizan este medio y es la forma más sencilla de atacar. Los ataques basados en correo electrónico, que han crecido a un ritmo de más del

150% anual desde 2019, se están volviendo cada vez más comunes y han alcanzado niveles sin precedentes, con 4,7 millones de ataques registrados solo en 2022 [18].

Debido a esto, las empresas utilizan herramientas automatizadas para mitigar este tipo de ataques, pero estas también tienen vulnerabilidades, lo que significa que muchos correos electrónicos continúan evadiendo los sistemas automatizados, y un 85% sustancial de las violaciones de seguridad son atribuibles a las vulnerabilidades de los errores del usuario [18].

En este contexto, cuando se explotan vulnerabilidades, los hackers o ciberdelincuentes usan una técnica llamada ataque por denegación de servicio o DDoS que, aunque no es una vulnerabilidad en sí, es la forma más sencilla de detectar y explotar vulnerabilidades [19].

El *phishing*, la denegación de servicio, los Ataques de Día Cero, el ransomware y el acceso no autorizado a los sistemas de información son algunos ejemplos de vulneraciones. Cada uno de estos tipos tiene posibles consecuencias económicas y reputacionales para la empresa afectada. Entre ellos, uno de los más complejos es el Ataque de Día Cero, el cual causa una desestabilización de la empresa y, si el equipo T.I. no realiza una contingencia apropiada, podría causar grandes pérdidas [20].

Como se estableció al inicio de esta investigación, una de las vulnerabilidades más latentes, comunes o fáciles de explotar es la falta de conocimiento del empleado o usuario, ya que por medio de ellos pueden entrar a los sistemas de la empresa, especialmente si trabajan de forma remota. Al estar enlazados directamente con la red de la empresa, los empleados son más vulnerables y no comprenden lo delicado que puede ser que la entidad donde trabajan sea perjudicada por un error suyo [21].

Además, la investigación destaca nuevamente al usuario o empleado como una de las causas más probables de ataques una de las vulnerabilidades más comunes y peligrosas dentro de una empresa. En [22] señalan que el 34% de las organizaciones considera a los empleados desprevenidos como la mayor vulnerabilidad. La mayoría de ellos carece de conciencia sobre las amenazas y problemas de seguridad de la información.

Dado que esta investigación aborda no solo las TIC sino también el sector de bienes y servicios en general, Es definir y ejemplificar uno de los ataques más complejos: el Ransomware WannaCry. Este caso evidenció la gravedad del desconocimiento en las empresas de bienes y servicios y la necesidad de implementar normas para mitigar las vulnerabilidades como lo es la ISO 27001 [23].

Según la documentación, se puede considerar como vulnerabilidad el hecho de no darle importancia a los incidentes catalogados como de bajo impacto o gravedad, ya que estos podrían escalar y causar un problema mayor de alto riesgo, que supondría para la empresa pérdidas o fugas significativas [24].

También, en las empresas se encuentran vulnerabilidades originadas en el *software* que comúnmente se compra y se vende como seguro. Este es el caso de Windows uno de los sistemas operativos más usados en sus servidores y computadoras empresariales.

La documentación revela que existe una vulnerabilidad en "Wickr" que permite conseguir datos sensibles, como las contraseñas de los usuarios, por medio del algoritmo de validación: AES-GCM. Esto permitiría cambiar contraseñas por la fuerza, dejando expuestos los datos de los usuarios [25].

Para concluir y dejando en claro que el principal objetivo de un ciberdelincuente es atacar al usuario o trabajador, pues es la manera más fácil de acceder a la información sensible de personas y empresas, se encontró que en muchos casos no es el error humano en sí, sino el mal diseño de procesos lo que hace que el error humano y las violaciones de seguridad sean inevitables [26]. Esto demuestra que también es responsabilidad de los procesos que estas vulnerabilidades existan.

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 115 de 130

Ahora bien, una buena práctica podría ser el uso de factores de autenticación o un constante monitoreo de la red, sin dejar de lado al trabajador, ya que ciertos comportamientos pueden generar hábitos que crean vulnerabilidades importantes para la empresa [26].

Se evidenció que el usuario o trabajador es la principal víctima de los ciberdelincuentes para afectar a las empresas, con una tendencia mayoritaria a emplear ataques de ingeniería social. Sin embargo, hacen falta más estudios sobre el resto de numerosos ataques y vulnerabilidades en el campo de la ciberseguridad.

¿Cómo se han implementado los encriptadores de datos en el sector real?

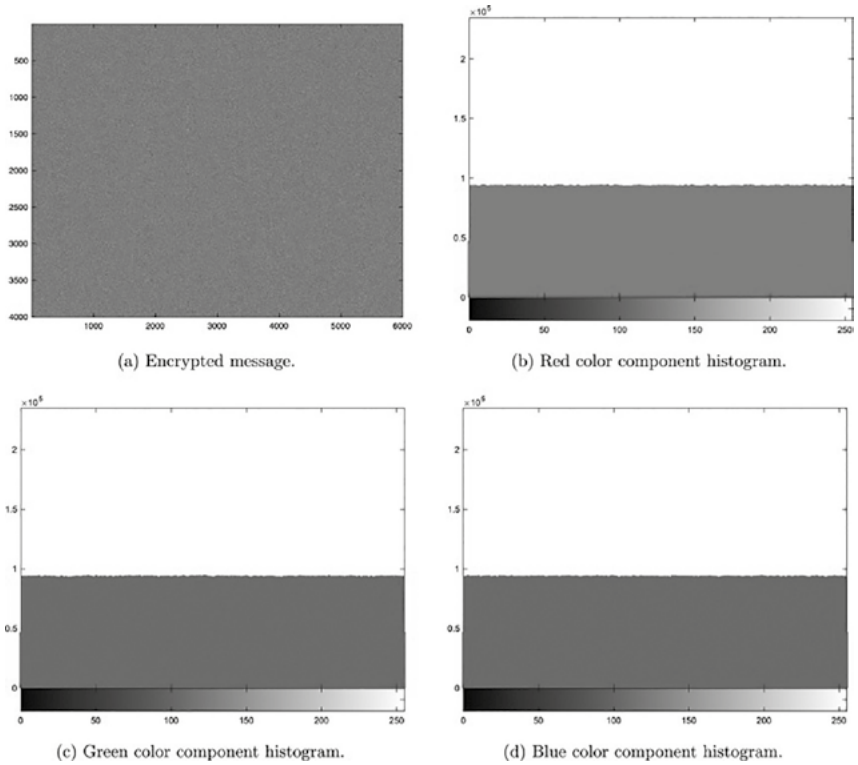
La implementación de encriptadores o cifradores de datos en el sector real ha incrementado en los últimos años aunque estas tecnologías o técnicas existen desde hace tiempo. Hay varios tipos de tecnologías de cifrado de datos, entre ellas los cifrados de enlaces y los cifrados de nodos. Estas dos tecnologías se usan en las herramientas denominadas encriptadores, y según la tecnología usan varios algoritmos para garantizar la seguridad de datos: Algoritmo DES (Data Encryption Standard), Algoritmo MD5 (Message-Digest Algorithm 5) y Algoritmo RSA (Rivest-Shamir-Adleman) [6].

Una de las técnicas implementadas en el sector es el cifrado de imágenes en color, presentado como una aplicación del método de sincronización. Este algoritmo permite descifrar datos sin pérdida, garantizando que solo usuarios autorizados puedan acceder a los datos originales, utilizando las teorías matemáticas del Derivado de Caputo y la Integral de Riemann-Liouville. De esta forma, la imagen se vuelve ilegible para terceros, pero al llegar al destinatario autorizado se recupera con todos sus detalles, preservando la seguridad de la información [27].

Figura 2. Mensaje

Nota: fuente O. Martínez-Fuentes et al. [27].

Figura 3. Mensaje encriptado



Nota: fuente O. Martínez-Fuentes et al. [27].

Figura 4. Mensaje descifrado

Nota: fuente O. Martínez-Fuentes et al. [27].

Actualmente, se utiliza un modelo de encriptación de imágenes diferente al anterior, de nombre: criptosistema híbrido (técnica de encriptación de módulos), que se basa principalmente en módulos S-box y PRN. Este sistema emplea un mecanismo de dos fases en una sola ronda sobre los datos de la imagen para generar su versión cifrada [28].

Ahora bien, al inicio se mencionaron algunos algoritmos utilizados en los cifrados; sin embargo, en el campo actual se usan otros, como el ANS, que consiste básicamente en comprimir los datos para agilizar su transporte. Este método presenta un bajo nivel de seguridad, lo cual se soluciona mediante el cifrado del flujo de bits comprimido. Sin embargo, requiere la implementación de dos algoritmos: uno para la compresión y otro para el cifrado [29].

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 117 de 130

De igual manera, se puede agregar otra mejora de seguridad para este protocolo: la Comp Crypt [29], que comprime y cifra los datos en un solo algoritmo, creando así un proceso más ágil [29].

Otro de los algoritmos de cifrado es el AES, un cifrado en bloques que divide los datos en diferentes secciones clave, posterior a su envío, para luego unirlas de una manera inversa y así proyectar el dato sin fallas [1].

En la actualidad, con la influencia de nuevas tecnologías como los sistemas de aprendizaje automático o *Machine Learning*, los cuales aprenden tareas específicas y manejan grandes volúmenes de información sensible, resulta crucial encriptar los datos en el momento en que son capturados por el programa, con el fin de evitar su robo [5].

Estas herramientas no se emplean exclusivamente en empresas de *software*. En el sector energético también se utilizan encriptadores para proteger las señales e información, y así prevenir ataques que puedan comprometer el suministro eléctrico [30].

El sector de la educación también está usando encriptadores para proteger los datos de los estudiantes y así garantizar su seguridad física y virtual, ya que en ellos puede haber información delicada no solo de los propios estudiantes, sino de sus familiares, lo cual representaría un robo con posibles implicaciones crecientes [31].

La encriptación de datos también está contribuyendo a impulsar empresas de manufacturación, ya que facilita su proceso de digitalización. Ofrece sugerencias efectivas para la transformación digital e introduce, en detalle, la arquitectura general y la estructura funcional del sistema de servicio. Al encriptar los datos del usuario yalmacenarlos de forma segura para análisis, es posibleofrecer una experiencia personalizada a cada usuario de la empresa [31].

Así pues, se pudo evidenciar que los encriptadores de datos están cada vez más presentes en todos los sectores empresariales y pueden brindar una gran seguridad en cualquier sector. No obstante la documentación e información al respecto sigue siendo muy limitada o meramente teórica.

¿Cuáles son las principales ventajas, desventajas y desafíos en el uso de encriptadores para garantizar la ciberseguridad en las empresas?

El uso de encriptadores en el ámbito empresarial brinda ventajas claras, como mayor protección de los datos y el cumplimiento de normativas. Sin embargo, su implementación puede resultar costosa y exige una gestión continua. Los organismos de normalización han comenzado a emitir directrices que exigen a las empresas adoptar medidas de seguridad acordes con los niveles requeridos para mitigar los altos riesgos asociados a ciberataques. Un ejemplo de ello es la norma ISO/SAE 21434 sobre ciberseguridad para vehículos de carretera [32].

El uso de sistemas de encriptación ligeros en la nube ofrece beneficios relevantes, al mejorar la seguridad de los datos mediante técnicas de cifrado optimizadas para dispositivos de baja potencia. Sin embargo, entre los desafíos destacan la gestión de claves y la necesidad de confiar en el proveedor de servicio lo que puede generar vulnerabilidades cuando los usuarios no controlan directamente la seguridad de su información [33].

Entre las ventajas del uso de encriptadores en entornos corporativos se encuentran la protección de información confidencial y la reducción de riesgos frente a accesos no autorizados, al transformar los datos en un formato ilegible sin las claves correspondientes Para enfrentar los desafíos asociados a la protección, transmisión y control de la información, algunos autores [34] proponen un sistema de cifrado basado en atributos de política de texto cifrado (CP-ABE). Esta solución no solo asegura la integridad de los datos, sino que también previene accesos no autorizados, protege la información transferida entre dispositivos y refuerza la seguridad en redes corporativas.

Igualmente, se identifican desafíos adicionales, como la necesidad de implementar medidas de autenticación y autorización, así como la integración

de la encriptación con otros sistemas de seguridad, como los firewalls. En el futuro, se recomienda realizar análisis periódicos de vulnerabilidades y encriptar los datos de forma sistemática para facilitar la detección temprana de vulnerabilidades y proteger los datos incluso si estos terminan en manos equivocadas [35].

Los encriptadores, por tanto, son herramientas clave para garantizar la ciberseguridad empresarial, al ofrecer una protección de los datos y preservar la integridad de las comunicaciones sensibles. No obstante, entre sus desventajas se encuentra el mantenimiento de estos sistemas. Como medida preventiva, se aconseja escaneos periódicos de vulnerabilidades y el cifrado de datos [36].

Una ventaja destacada es la evolución constante de los cifradores. Los modelos actuales incorporan mejoras sustanciales. Un caso ilustrativo es el uso de técnicas que transforman las características del tráfico de red en imágenes alfa de cuatro canales, las cuales se analizan mediante el modelo de aprendizaje profundo ResNet50 para la clasificación. Este enfoque logró una precisión del 99.8%, en la detección, superando a los modelos tradicionales en dos conjuntos de datos públicos: UNSW-NB15 y BOUND DDoS [37].

Las compañías priorizan la protección de la integridad y la privacidad de los datos, especialmente en entornos compartidos como la nube, donde los mecanismos de cifrado sin certificados permiten realizar auditorías sin comprometer la identidad del usuario. En los últimos años, muchas aplicaciones en la nube han permitido a los usuarios trabajar de forma colaborativa con datos compartidos. Por lo tanto, la auditoría de información entre múltiples usuarios ha cobrado creciente relevancia [2].

Las empresas se encuentran en un proceso constante de actualización, y gracias a estándares de seguridad como la norma ISO 27001 o el Reglamento General de Protección de Datos (GDPR), logran adaptarse a un entorno en el que los ataques cibernéticos también evolucionan continuamente. Estos ataques son cada vez más complejos, multivectoriales y de rápida evolución, lo que provoca graves interrupciones en los servicios críticos y compromete la continuidad operativa [4].

Sin embargo, también existen desventajas y desafíos, como la complejidad técnica y los costos asociados a la implementación de soluciones de cifrado avanzadas, así como la necesidad de cumplir con diversas normativas internacionales sobre ciberseguridad [38].

Si bien los métodos tradicionales, como el cifrado de datos, la seguridad del usuario y el uso de cortafuegos, se utilizan como medidas iniciales de protección, pero el uso de contraseñas débiles o las brechas en su gestión impiden evitar accesos no autorizados y comprometen la autenticación del usuario [39].

En síntesis, el uso de encriptadores en las empresas ofrece claras ventajas, especialmente en la protección de la integridad y la privacidad de los datos. Sin embargo, persisten desafíos técnicos y financieros en su implementación, como la gestión de claves y la dependencia de proveedores externos. Asimismo, se identifica un vacío en la literatura sobre el uso de cifradores en entornos corporativos, lo que revela la necesidad de más estudios en este campo.

VII. Conclusiones

A partir de esta revisión, se concluye que uno de los puntos más vulnerables las empresas es el factor humano, especialmente cuando los empleados trabajan de forma remota y carecen del conocimiento necesario para mitigar posibles ataques. A su vez, se evidencia que muchas organizaciones sólo toman medidas para reforzar su ciberseguridad después de haber sufrido incidentes, lo que conlleva fugas de información valiosa y pérdidas económicas significativas.

También se observa que la documentación disponible hasta ahora se ha centrado principalmente en el análisis de ataques ocurridos, descuidando el desarrollo de estrategias preventivas de mitigación. Esto representa una deficiencia importante en la literatura actual. Otras limitaciones detectadas

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 119 de 130

incluyen la escasa atención a enfoques preventivos, la baja inversión en programas de concienciación para los usuarios y la ausencia de soluciones criptográficas robustas ante amenazas emergentes, como los ataques cuánticos.

De igual forma, se concluye que el uso de cifradores de datos en el sector productivo real ha evolucionado significativamente para garantizar la protección de la información sensible frente a las amenazas cibernéticas. Empresas de sectores como energía, finanzas y salud, han adoptado algoritmos de cifrado avanzados como AES y RSA, para asegurar la integridad de sus transacciones y comunicaciones.

La ciberseguridad empresarial implica ventajas, desventajas y desafíos. Entre sus principales beneficios destaca la protección de datos y la integridad de las comunicaciones. La integración de sistemas de cifrado con otras soluciones de seguridad podría fortalecer de manera sustancial la postura defensiva de las organizaciones. En este sentido, los encriptadores desempeñan un papel fundamental en la protección de datos y en la reducción de riesgos frente a amenazas que puedan comprometer información importante y de gran valor.

Dado lo anterior, se recomienda que futuras investigaciones se orienten hacia el desarrollo de estrategias de seguridad proactivas, la implementación de metodologías de formación en ciberseguridad para los empleados y el estudio de nuevos algoritmos de cifrados resistentes a los avances de la computación cuántica.

VIII. Referencias

[1] Y. He, N. Ye, y R. Zhang, "Analysis of data encryption algorithms for telecommunication network-computer network communication security", Wirel. Commun. Mob. Comput., vol. 2021, n° 1, 2021. doi: 10.1155/2021/2295130.

[2] H. Yan, Y. Liu, Z. Zhang, y Q. Wang, "Efficient privacy-preserving certificateless public auditing of data in cloud storage", Secur. Commun. Netw., vol. 2021, n° 1, 2021. doi: 10.1155/2021/6639634.

[3] Prensario Hub. 2023. [En línea] Disponible en: https://www.prensariohub.com/colombia-entre-los-diez-paises-mas-atacados-por-ransomware/

[4] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, y U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures", Comput. Secur., vol. 128, 2023. doi: 10.1016/j.cose.2023.103139.

[5] S. Z. El Mestari, G. Lenzini, y H. Demirci, "Preserving data privacy in machine learning systems", Comput. Secur., vol. 137, 2024. doi: 10.1016/j.cose.2023.103605.

[6] L. Ding, Z. Wang, X. Wang, y D. Wu, "Security information transmission algorithms for IoT based on cloud computing", Comput. Commun., vol. 155, pp. 32–39, 2020. doi: 10.1016/j.comcom.2020.03.010.

[7] L. Ablon y A. Bogart, "Zero Days, Thousands of Nights", RAND, 2017. [En línea]. Disponible en: https://www.rand.org/pubs/research_reports/RR1751.html.

[8] Fortinet, "¿Qué es un ataque DDoS? Significado, definición y tipos", Fortinet. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/ddos-attack#:~:text=Ataque%20DDoS%20significa%20%22Ataque%20de,y%20sitios%20en%20línea%20conectados. [Accedido: 21-sep-2024].

[9] US Cybersecurity Institute, "Understanding Denial of Service (DoS) Attacks and Effective Prevention Strategies", 2024. [En línea]. Disponible en: https://www.uscsinstitute.org/cybersecurity-insights/resources/understanding-denial-of-service-dos-attacks-and-effective-prevention-strategies. [Accedido: 22-sep-2024].

[10] PowerData, "GDPR: Lo que debes saber sobre el reglamento general de protección de datos", PowerData. [En línea]. Disponible en: https://www.powerdata.es/gdpr-proteccion-datos. [Accedido: 22-sep-2024].

[11] CompTIA, "What is social engineering?", CompTIA. [En línea]. Disponible en: https://www.comptia.org/content/articles/what-is-social-engineering. [Accedido: 20-sep-2024].

[12] Global Suite Solutions, "¿Qué es la norma ISO 27001 y para qué sirve?", Global Suite Solutions. [En línea]. Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/. [Accedido: 23-sep-2024].

[13] California Institute of Technology, "What is Machine Learning?", [En línea]. Disponible en: https://pg-p.ctme.caltech.edu/blog/ai-ml/what-is-machine-learning. [Accedido: 22-sep-2024].

[14] M. Kosinski, "¿Qué es el phishing?", IBM, 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/phishing. [Accedido: 22-sep-2024].

[15] Cloud Security Alliance, "What is Ransomware", 2021. [En línea]. Disponible en: https://cloudsecurityalliance.org/blog/2021/11/28/what-is-ransomware. [Accedido: 22-sep-2024].

[16] "UNSW-NB15", Papers with Code. [En línea]. Disponible en: https://paperswithcode.com/dataset/unsw-nb15#:~:text=UNSW%2DNB15%20is%20a%20network,dataset%20contains%20raw%20network%20packets. [Accedido: 22-sep-2024].

[17] F. I. Arroyabe, C. F. A. Arranz, M. F. Arroyabe y J. C. Fernandez de Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019", Comput. Secur., vol. 124, 2023, doi: 10.1016/j.cose.2022.102954.

[18] N. Marshall, D. Sturman, y J. C. Auton, "Exploring the evidence for email phishing training: A scoping review", Comput. Secur., vol. 139, 2024, doi: 10.1016/j.cose.2023.103695.

[19] A. Nagurney y S. A. Shukla, "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability", Eur. J. Oper. Res., vol. 260, n° 2, pp. 588–600, 2017. doi: 10.1016/j.ejor.2016.12.034.

[20] M. F. A. Shaikh y M. Siponen, "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity", Comput. Secur., vol. 124, 2023. doi: 10.1016/j.cose.2022.102974.

[21] S. Vrhovec, I. Bernik, y B. Markelj, "Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign", Comput. Secur., vol. 125, 2023. doi: 10.1016/j.cose.2022.103038.

[22] K. Khando, S. Gao, S. M. Islam, y A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review", Comput. Secur., vol. 106, 2021. doi: 10.1016/j.cose.2021.102267.

[23] M. Mirtsch, K. Blind, C. Koch, y G. Dudek, "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective", Comput. Secur., vol. 109, 2021, doi: 10.1016/j.cose.2021.102383.

[24] C. M. Patterson, J. R. C. Nurse, y V. N. L. Franqueira, "'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents", Comput. Secur., vol. 139, 2024, doi: 10.1016/j.cose.2023.103699.

ISSN: 2027-8101 - e-ISSN: 2619-5232. Enero-Diciembre 2024 • Página 121 de 130

[25] G. Kim, S. Kang, U. Hur, y J. Kim, "A study on vulnerability of the WICKR login system in windows from a live forensics perspective", Comput. Secur., vol. 139, 2024. doi: 10.1016/j.cose.2023.103672.

[26] K. Mersinas, M. Bada, y S. Furnell, "Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions", Comput. Secur., vol. 148, 2025. doi: 10.1016/j.cose.2024.104025.

[27] O. Martínez-Fuentes, J. J. Montesinos-García, y J. F. Gómez-Aguilar, "Generalized synchronization of commensurate fractional-order chaotic systems: Applications in secure information transmission", Digit. Signal Process., vol. 126, 2022. doi: 10.1016/j.dsp.2022.103494.

[28] M. I. Haider, T. Shah, A. Ali, D. Shah, y I. Khalid, "An innovative approach towards image encryption by using novel PRNs and S-boxes modeling techniques", Math. Comput. Simul., vol. 209, pp. 153–168, 2023. doi: 10.1016/j.matcom.2023.01.036.

[29] S. Camtepe et al., "Compcrypt-Lightweight ANS-Based Compression and Encryption", IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 3859–3873, 2021. doi: 10.1109/TIFS.2021.3096026.

[30] C. Jost, M. Näslund, J. Mattson, y B. Smeets, "Cryptography in an all encrypted world", Ericsson Technol. Rev., vol. 92, n° 10, pp. 1–14, 2015.

[31] Y. Lin, "Digital transformation path for manufacturing enterprises using Internet of Things and data encryption technology", Sci. Program., vol. 2022, 2022, doi: 10.1155/2022/6862999.

[32] I. O. for Standardization, ISO/SAE 21434: 2021: Road Vehicles: Cybersecurity Engineering, ISO, 2021.

[33] S. Mohammed et al., "A new lightweight data security system for data security in the cloud computing", Meas. Sensors, vol. 29, 2023. doi: 10.1016/j.measen.2023.100856.

[34] P. K. Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, y V. J. Pillai, "Secure approach to sharing digitized medical data in a cloud environment", Data Sci. Manag., vol. 7, n° 2, pp. 108–118, 2024. doi: 10.1016/j.dsm.2023.12.001.

[35] T. Kaarlela, T. Niemi, T. Pitkäaho, y J. Harjula, "Retrofitting enables sustainability, Industry 4.0 connectivity, and improved usability", Adv. Ind. Manuf. Eng., vol. 9, 2024. doi: 10.1016/j.aime.2024.100146.

[36] A. Chidukwani, S. Zander, y P. Koutsakis, "Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications", Comput. Secur., vol. 145, 2024, doi: 10.1016/j.cose.2024.104026.

[37] Y. Yan, Y. Yang, F. Shen, M. Gao, y Y. Gu, "GDE model: A variable intrusion detection model for few-shot attack", J. King Saud Univ. Comput. Inf. Sci., vol. 35, n° 10, 2023. doi: 10.1016/j.jksuci.2023.101796.

[38] A. Mishra, Y. I. Alzoubi, M. J. Anwar, y A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations", Comput. Secur., vol. 120, 2022. doi: 10.1016/j.cose.2022.102820.

[39] H. Dalmaz, E. Erdal, y H. M. Ünver, "A new hybrid approach using GWO and MFO algorithms to detect network attack", CMES - Comput. Model. Eng. Sci., vol. 136, n° 2, pp. 1277–1314, 2023. doi: 10.32604/cmes.2023.025212.