

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 services companies: a literature review

Sebastian Gómez Sepúlveda ¹, Juan Esteban Vélez Mazo ²

Tipo de Artículo: revisión de literatura.

Recibido: 13/11/2024. Aprobado: 25/03/2025. Publicado: 00/00/0000

Resumen: Este trabajo aborda la necesidad de encriptadores en empresas de bienes y servicios, que enfrentan crecientes y sofisticados ciberataques. Aunque la encriptación es clave para proteger la información, muchas organizaciones no invierten en estas herramientas hasta que han sido víctimas de un ataque significativo. El objetivo de esta investigación es evaluar el uso de encriptadores en empresas y cómo estos ayudan a mitigar ataques como phishing o DDoS, analizando tanto sus ventajas como sus limitaciones. Para ello, se empleó 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 las empresas inviertan en ciberseguridad aumenta a medida que crece el nivel 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 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.

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>

I. Introducción

La ciberseguridad es un tema de vital importancia y utilidad en cualquier actividad que se desarrolle dentro de un sistema informático. Sin embargo, en muchos países en vías de desarrollo, este aspecto fue frecuentemente descuidado, lo que dejó abiertas múltiples vulnerabilidades. La ausencia en la atención de ciberseguridad pone en riesgo a las empresas u organizaciones, a los empleados y los clientes debido a la posibilidad de hurto de datos confidenciales, lo que genera un ambiente de presión e inseguridad.

La finalidad de este estudio es examinar y recolectar el saber existente en torno a la ciberseguridad, indagando en cómo varios autores tratan y detallan los diversos elementos involucrados en este asunto. Este estudio intenta determinar las estrategias más eficaces para transmitir los múltiples beneficios que la ciberseguridad brinda en varias actividades, además de resaltar los datos cruciales que cada individuo debería tener para prevenir fallos y estar protegido de manera adecuada en el ambiente digital.

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

El mayor hallazgo de este trabajo fue identificar que, a mayor nivel de ciberataques, aumentaba la probabilidad de que las organizaciones invirtieran en sistemas de ciberseguridad. A partir de nuestros resultados, pudimos confirmar que las organizaciones estuvieron sujetas a una gran variedad de ataques. Esto quiere decir que las empresas esperaron a que el nivel de los ataques a la información, o en los peores casos, fueran atacadas, para hacer una gran inversión en la ciberseguridad y en la encriptación de datos.

II. Justificación de la revisión

La ciberseguridad depende en gran medida del uso de cifradores 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 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 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 presenta 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 descubiertas públicamente ni tienen un parche o solución disponible [7].

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

Denegación de servicio: es sobrecargar un sistema con tráfico o solicitudes excesivas para que los usuarios legítimos no puedan acceder a los servicios [9].

GDPR: el Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679) es un reglamento con el 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 período 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.

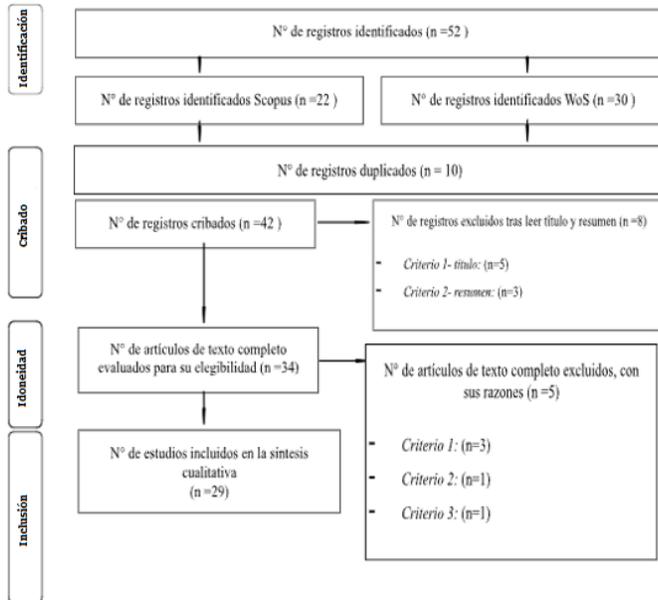
Criterios de exclusión: los artículos que no se enfocaron en analizar ataques específicos (como phishing o DDoS) en empresas de servicios, sino que hablaron sobre ataques en sectores distintos (por ejemplo, bioseguridad) o describieron ataques sin detalles específicos aplicables a empresas de servicios.

Los artículos que no emplearon ni implementaron encriptadores reales en sus entornos de estudio, sino

que trabajaron sólo en teoría (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 solo aspectos técnicos sin impacto específico en la empresa.

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 cuáles son esas vulnerabilidades más comunes en las empresas y también los ataques más comunes que hacen las personas mal intencionadas o hackers para explotar estas vulnerabilidades.

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

Combinando el phishing y la falta de preparación de los trabajadores de las empresas se llega a uno de los focos

más grandes en las vulnerabilidades como son los ataques por correos electrónicos, ya que, todas las empresas tienen correos 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].

Gracias a esto, las empresas están usando herramientas automatizadas para lograr mitigar este tipo de ataque, 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].

Dentro de este mundo podemos encontrar que, en el momento de explotar vulnerabilidades, los hackers o ciberdelincuentes usan una técnica llamada ataque por denegación de servicio o DOS que, si bien no es una vulnerabilidad, es la forma más sencilla de hallar vulnerabilidades y explotarlas [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. Cada uno de estos tipos de vulneraciones tiene posibles consecuencias económicas y reputacionales para la empresa afectada. De estos ejemplos uno de los más difíciles 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 hemos podido establecer 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 y más si estos están trabajando desde la virtualidad. Al estar enlazados directamente con la red de la empresa, el empleado es más vulnerable y no entiende lo delicado que podría ser que la entidad donde trabaja sea perjudicada por un error suyo [21].

Siguiendo con la investigación se encuentra que una vez más se debe llamar al usuario o al empleado como una de las causas más probables de ataques o una de las vulnerabilidades más comunes y peligrosas dentro de una empresa. En [22] señalan que el 34% de las organizaciones considera que los empleados desprevenidos son la mayor vulnerabilidad. La mayoría de los empleados carecen de conciencia sobre las amenazas y los problemas de seguridad de la información.

Ya que en esta investigación se habla no solo de TIC sino en general de bienes y servicios, es una buena práctica definir y ejemplificar uno de los ataques más

complicados: el Ransomware WannaCry. Este demostró lo delicado que es el desconocimiento en las empresas de bienes y servicios, demostrando que es necesario una serie de normas para mitigar las vulnerabilidades como lo es la ISO 27001 [23].

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

También, en las empresas podemos hallar vulnerabilidades que vienen desde el software que comúnmente se compra y se vende como seguro. Este es el caso de Windows uno de los sistemas operativos que más empresas usan en sus servidores y computadoras.

Revisando la documentación se encontró que hay una vulnerabilidad en "Wickr" lo cual permite conseguir datos sensibles como la contraseña de los usuarios por medio del algoritmo que usa para la validación: AES-GCM. Este permitiría el cambio de contraseña a la fuerza, dejando así los datos de los usuarios expuestos [25].

Para concluir y dejando en claro que el principal enfoque 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, al revisar la documentación 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]. Lo que demuestra que también es culpa de los procesos que estas vulnerabilidades se den.

Ahora, bien, una buena práctica podría ser el uso de factores de autenticación o un constante monitoreo de la red, aunque no dejando de lado al trabajador porque ciertos comportamientos de ellos pueden dar lugar a hábitos que generan vulnerabilidades importantes para la empresa [26].

Se pudo evidenciar que el usuario o trabajador son las víctimas principales de los ciberdelincuentes para lograr golpear a las empresas; con tendencia a usar ataques de ingeniería social en su mayoría. Falta un poco más de estudios en el resto de las infinidades de ataques y vulnerabilidades que hay en este mundo 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 se ha incrementado en los últimos años a pesar de que estas tecnologías o técnicas vienen de años atrás. Existen varios tipos de tecnologías de cifrado de datos, entre los que están: los cifrados de enlaces y los cifrados de nodos. Estas dos tecnologías

se usan en las herramientas llamadas encriptadores y dependiendo de las tecnologías usan varios algoritmos para una correcta seguridad de datos: Algoritmo DES (Data Encryption Standard), Algoritmo MD5 (Message-Digest Algorithm 5) y Algoritmo RSA (Rivest-Shamir-Adleman) [6].

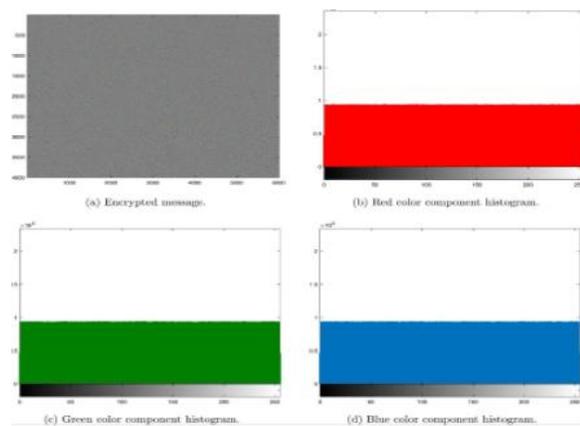
Una de las técnicas que se están implementando en el sector es el cifrado de imágenes en color, que se presenta como una aplicación al método de sincronización. El algoritmo permite descifrar datos sin pérdida garantizando que solo usuarios autorizados puedan acceder a los datos originales, usando las teorías matemáticas de Derivado de Caputo y la Integral de Riemann-Liouville, logrando así aplicar un algoritmo que vuelve la imagen formato ilegible, pero al llegar al destinatario autorizado logra retornar la imagen con todos los detalles, preservando así la seguridad de la información [27].

Figura 2. Mensaje



Nota: fuente elaboración propia.

Figura 3. Mensaje encriptado



Nota: fuente elaboración propia.

Figura 4. mensaje descifrado



Nota: fuente elaboración propia.

Actualmente, se está usando 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. Funciona empleando un mecanismo de dos fases en una sola ronda sobre los datos de la imagen para construir su versión cifrada [28].

Ahora bien, al inicio se mencionaron algunos algoritmos usados en los cifrados, aunque en el campo actual se usan otros como el ANS que básicamente es comprimir los datos para hacer el transporte más rápido. Este es muy poco seguro a lo cual se le da una solución sencilla usando cifrado del flujo de bits comprimido. Sin embargo, requiere dos algoritmos: uno para la compresión y el otro para el cifrado [29].

De igual manera, se puede agregar otra mejora de seguridad para este protocolo: la Compcrypt [29]; esta 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 unirlos 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, que se encargan de aprender ciertas tareas y contienen una cantidad grande de información delicada, es de suma importancia encriptar al momento que sea tomada por el programa para evitar robos de dichos datos [5].

Pero no solo en empresas de software se utilizan estas herramientas. En el sector energético se están usando encriptadores para proteger las señales e información de estas y así evitar ataques que comprometan la alimentación eléctrica [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 estos puede haber información delicada no solo de los estudiantes sino de sus familiares, lo cual sería un robo que podría ir escalando [31].

La encriptación de datos también está ayudando a impulsar empresas de manufacturación debido a que les ayuda en el proceso de digitalización. Brinda sugerencias efectivas para la transformación digital e introduce la arquitectura general y la estructura funcional del sistema de servicio en detalle. Al encriptar los datos del usuario y tenerlos de forma segura para analizarlos, se le puede ofrecer 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, pero aun así la documentación e información es muy limitada o es meramente teórica.

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

En cuanto a las ventajas, desventajas y desafíos del uso de encriptadores para la ciberseguridad en empresas, estos cifradores brindan mayor protección de datos y garantizan el cumplimiento normativo, pero su implementación puede ser costosa, además de requerir una gestión continua. Los organismos de normalización también han comenzado a emitir normas para garantizar que las empresas de estos dominios empleen medidas de seguridad que cumplan con los niveles requeridos para mitigar los altos riesgos de ciberataques, por ejemplo, la norma de ciberseguridad ISO/SAE 21434 para vehículos de carretera [32].

El uso de sistemas de encriptación ligeros en la nube presenta ventajas significativas al mejorar la seguridad de los datos mediante técnicas de cifrado optimizadas para dispositivos de baja potencia. Sin embargo, los desafíos incluyen la gestión de claves y la necesidad de confiar en el proveedor de servicios, lo que puede generar vulnerabilidades cuando los usuarios no pueden controlar directamente la seguridad de sus datos [33].

El uso de encriptadores para garantizar la seguridad en las empresas ofrece ventajas como la protección de la información confidencial y la reducción de riesgos ante accesos no autorizados, ya que transforma los datos a un formato ilegible sin las claves adecuadas. Para

abordar los desafíos de proteger, transmitir y controlar la información, los autores [34] proponen un sistema de cifrado basado en atributos de política de texto cifrado (CP-ABE). Sumado al aseguramiento de la integridad de los datos y la prevención de accesos no autorizados, protegiendo la información transferida entre dispositivos y garantizando la seguridad en redes corporativas.

Igualmente, también existen desafíos como la necesidad de implementar medidas de autenticación y autorización adicionales, como la integración de la encriptación con otros sistemas de seguridad: los firewalls. En el futuro, se recomienda realizar análisis periódicos de vulnerabilidades y encriptar los datos para permitir la detección temprana de vulnerabilidades y proteger los datos incluso si estos terminan en manos equivocadas [35].

Los encriptadores garantizan la ciberseguridad en las empresas y presentan varias ventajas, como la protección robusta de los datos y la integridad de las comunicaciones sensibles. No obstante, entre sus desventajas se encuentra el mantenimiento de estos sistemas. Para fortalecer la ciberseguridad contra ataques, se recomiendan escaneos periódicos de vulnerabilidades y cifrado de datos [36].

Una gran ventaja es que los cifradores de datos han ido evolucionando y se puede afirmar que cada vez se presentan modelos con mejoras. Transformaron las características del tráfico de red en imágenes alfa de cuatro canales y utilizaron el modelo de aprendizaje profundo ResNet50 para la clasificación; demostraron experimentalmente en dos conjuntos de datos disponibles públicamente: UNSW-NB15 y BOUN DDoS, que la precisión de detección fue del 99.8%, lo que fue mejor que el modelo de clasificación general para datos [37].

Las compañías incluyen la protección de la integridad y privacidad de los datos, especialmente en entornos compartidos como la nube, donde los mecanismos de cifrado sin certificados permiten auditorías sin comprometer la identidad del usuario. En los últimos años, muchas aplicaciones en la nube permitieron a los usuarios trabajar en coordinación con datos compartidos. Por lo tanto, la forma de auditar los datos compartidos entre múltiples usuarios atrajo mucha atención [2].

Las empresas están en constante actualización y con ayuda de estándares de seguridad como el ISO 27001 o el GDPR, las empresas logran renovarse ya que los ataques cibernéticos también están en constante actualización. Los ciberataques son cada vez más complejos, multivectoriales y evolucionan rápidamente, lo que provoca graves interrupciones en los servicios críticos y en la continuidad general del negocio [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].

Métodos tradicionales como el cifrado de datos, la seguridad del usuario y el uso de cortafuegos se utilizan como medidas de seguridad iniciales, pero las contraseñas débiles o las brechas de seguridad de las contraseñas no evitan el uso no autorizado y la autenticación del usuario falla [39].

Se logra evidenciar que el uso de encriptadores en las empresas presenta claras ventajas, como la protección de la integridad y privacidad de los datos. Sin embargo, existen desafíos técnicos y financieros en su implementación, como la gestión de claves y la dependencia de terceros. En la búsqueda también se logra evidenciar un vacío en el tema de cifradores en las empresas, puesto que hacen falta más estudios.

VII. Conclusiones

Por medio de esta revisión e investigación se puede concluir que uno de los focos o factores más débiles de las empresas es el trabajador y más si este trabaja a distancia y no tiene los conocimientos pertinentes para mitigar los posibles ataques. A su vez, también queda en evidencia que las empresas esperan a que les pasen ataques para tomar la decisión de engrosar su ciberseguridad dando como resultado fugas de información valiosa y pérdida de dinero.

También podemos concluir que la documentación hasta el momento se centra solo en ataques que ya sucedieron y no en estrategias de mitigación preventiva, lo que representa una deficiencia en la literatura actual. Además, se identifican otras limitaciones, como la falta de enfoques preventivos en seguridad, la escasa atención a la concienciación del usuario y la ausencia de soluciones criptográficas robustas ante posibles ataques cuánticos.

Podemos concluir que el uso de cifradores de datos en el sector real ha evolucionado significativamente para garantizar la protección de la información sensible frente a las amenazas cibernéticas. Empresas del sector energético, finanzas o salud, han adoptado algoritmos de cifrado avanzado como AES y RSA para asegurar transacciones y comunicaciones seguras.

La ciberseguridad en las empresas trae ventajas, desventajas y desafíos. Permite proteger los datos y la integridad de las comunicaciones. La integración de los cifradores con otros sistemas de seguridad podría fortalecer en gran medida la seguridad de las empresas. Estos encriptadores forman un papel muy importante en las compañías ya que estos contribuyen a la seguridad

de los datos y a la reducción de riesgos ante cualquier amenaza que pueda comprometer información importante y de gran valor.

Dado lo anterior, se recomienda que futuras investigaciones se enfoquen en el desarrollo de estrategias de seguridad proactivas, metodologías de capacitación en ciberseguridad para los empleados y el estudio de nuevos algoritmos de cifrado resistentes a 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/dd>

os-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/unswnb15#:~:text=UNSW%20NB15%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.

[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.