9 No.4 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.4.2025.e1116

# Ransomware attack prevention strategies: a systematic review

# Estrategias de prevención contra ataques de ransomware: una revisión sistemática

**Autores:**

Morales-Ramírez, Juan Roberto
UNIVERSIDAD CATÓLICA DE CUENCA
Maestrante
Azogues - Ecuador

juan.morales.90@est.ucacue.edu.ec

https://orcid.org/0009-0005-2895-090X

Criollo-Bonilla, Ronald Raúl
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutor del área de Ciberseguridad
Azogues - Ecuador

ronal.criollo@ucacue.edu.ec

https://orcid.org/0000-0001-7103-6869

Fechas de recepción: 13-Sep-2025 aceptación: 13-Oct-2025 publicación: 31-Dic-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

## Resumen

Hoy en día los ataques de tipo ransomware representa una de las amenazas más potenciales y peligrosas en el campo de la ciberseguridad, afectando a todo tipo de personas, empresas e instituciones secuestrando y poniendo en riesgo la accesibilidad y privacidad de la información. Por consiguiente, el presente trabajo investigativo tiene como objetivo realizar una revisión metódica de las estrategias que las entidades dedicadas a seguridad de la información ponen a consideración para contrarrestar los ataques de tipo ransomware; así mismo, evaluar la efectividad que tiene estos tipos de mitigación ante incidentes. Para llevar a cabo este artículo, se utilizó la metodología bibliográfica mediante la técnica de revisión documentos científicos; a partir de informes técnicos especializados y estrategias aplicadas por parte de empresas de seguridad informática se pudo comprender cómo se puede aplicar las medidas de protección. A través de documentos como IEEE Xplorer, artículos de Scopus, ScienceDirect, ENISA, NIST, entre otros se obtuvo un enfoque analítico de la aplicación de estrategias preventivas y cómo mitigar ante un ataque de esta índole. Como resultado de la información obtenida, se determinó algunas prácticas efectivas como las copias de seguridad, actualización de sistemas, autenticación, soluciones avanzadas y respuestas en endpoints. También se pudo reconocer que el factor humano juega un papel importante en la seguridad informática por lo que, su formación y atención en prácticas de ciberseguridad pueden llevar a una empresas o institución, fortalecer la seguridad mediante uso de políticas y herramientas que permitan reducir el impacto ante un ataque de tipo ransomware.

**Palabras claves:** ransomware; amenazas; mitigación; ciberseguridad; seguridad informática

## Abstract

Today, ransomware attacks represent one of the most potential and dangerous threats in the field of cybersecurity, affecting all types of individuals, businesses, and institutions by hijacking and jeopardizing the accessibility and privacy of information. Therefore, this research aims to conduct a methodical review of the strategies that information security organizations consider to counter ransomware attacks; it also evaluates the effectiveness of these types of mitigation measures against incidents. To prepare this article, we used a bibliographic methodology through the technique of reviewing scientific documents. Based on specialized technical reports and strategies applied by cybersecurity companies, we were able to understand how to apply protection measures. Through documents such as IEEE Xplorer, articles from Scopus, ScienceDirect, ENISA, NIST, and others, we obtained an analytical approach to the application of preventive strategies and how to mitigate an attack of this nature. As a result of the information obtained, we determined some effective practices such as backups, system updates, authentication, advanced solutions, and endpoint responses. It was also recognized that the human factor plays an important role in cybersecurity, so training and attention to cybersecurity practices can lead a company or institution to strengthen security through the use of policies and tools that can reduce the impact of a ransomware attack.

**Keywords:** ransomware; threats; mitigation; cybersecurity; computer security

## Introducción

En la actualidad, la ciberseguridad se ha transformado en un pilar esencial para el salvaguardo de la información y la prolongación operativa de las organizaciones (Alvarado, 2020). La evolución de las amenazas digitales ha llevado al desarrollo de múltiples mecanismos de defensa; sin embargo, uno de los ataques más considerables y con mayor impacto a nivel mundial es el ransomware (Veritas, 2024). Tal como lo menciona Cloudflare (2024), estos softwares de tipo maliciosos tienen como objetivo cifrar la información ya sea archivos como sistemas en su totalidad, impidiendo al dueño o responsable de los datos su acceso y pidiendo a cambio de su recuperación un costo por el rescate. Es ahí que los ataques ransomware es uno de los riesgos más potenciales para las empresas, instituciones y usuario final.

En concordancia con Aguirre (2022), los ataques de tipo ransomware ha tenido un repunte en los últimos años siendo así uno de los ataques con mayor impacto en las víctimas. En los primeros años donde salió a la luz estos tipos de amenazas, el ataque se camuflaba mediante el envío de correos electrónicos y usando la técnica del phishing llegaba a las posible víctimas al momento de descargar estos contenidos maliciosos; en la actualidad el ransomware ha evolucionado siendo más selectivos en sus víctimas y también estratégicos, en la cual ya los ataques van dirigido hacia las empresas que contengan alta disponibilidad económica y que tengan vulnerabilidades críticas. Este cambio de las estrategias de los atacantes ha dado lugar a variantes más avanzadas como el ransomware de doble extorsión, en el cual no únicamente se encriptan datos, también se extraen y intimidan con ser publicados si no se paga el rescate, incluso aquellos que cuentan con copias de seguridad pueden verse obligados a pagar para evitar la exposición.

Según Onofe (2022), el efecto del ransomware no se basa únicamente al secuestro de los datos o de la interrupción de las organizaciones. Sus consecuencias abarcan aspectos financieros, legales y reputacionales. Una vez que el ataque fue exitoso, se comienza a solicitar un pago por el rescate de la información, que su valor monetarios va desde los miles hasta los millos de dólares, haciendo muy atractivo su medio de ataque.

Además, la exposición de información confidencial puede derivar en sanciones regulatorias, demandas judiciales y desconfianza por parte de los usuarios y entes comerciales. En el caso

de infraestructuras críticas, como el sector energético, la salud o las telecomunicaciones, un ataque de ransomware puede provocar un potencial riesgo en las personas y la estabilidad de servicios esenciales para la sociedad (Agencia de Regulación y Control de las Telecomunicaciones, 2024).

Ante este panorama, la prevención del ransomware se ha convertido en una prioridad para los equipos de ciberseguridad y los responsables del control de riesgos de las empresas. A diferencia de otros tipos de amenazas cibernéticas, donde la detección y respuesta pueden ser suficientes para mitigar el impacto, en el caso del ransomware la prevención adquiere una importancia crítica,

Sin embargo, la tecnología por sí sola no es suficiente para frenar la propagación del ransomware. El accionar humano continúa siendo la pieza más vulnerable en el círculo de ciberseguridad, ya que la mayoría de los ataques exitosos tienen su origen en errores humanos, como la apertura de correos electrónicos fraudulentos o el uso de credenciales débiles. En este sentido, como lo menciona Alvarado (2020), es fundamental la capacitación constante de los empleados en buenas prácticas de seguridad, el fomento de una cultura enfocada en la precaución y la implementación de ejercicios de simulación de ataques; de esta manera, se convierte en estrategia claves para reducir el riesgo de infección.

## Material y métodos

Se aplicó la técnica documental se procedió a realizar la búsqueda en páginas indexadas y con gran rigor científico que permitan evaluar y contratar la información; se usaron operadores lógicos para la búsqueda exacta de la información y con objetivo de asegurar la calidad y veracidad de la información se escogió documentación científica de os últimos siete años comprendidos entre el 2018 hasta el 2025. Además, la documentación seleccionada como insumo para la investigación debe estar al menos revisada por pares; también se excluyó aquella documentación que contenía información redundante y con baja calidad académica.

Toda información recopilada, contratadas y verificada permitió comprender de mejor manera cómo los ataques de tipo ransomware se ha convertido en un medio de amenazas más selectivos por sus atacantes. También se ha comprendido su evolución y prácticas que

permitieron conocer su modo operandi y de esta manera saber cómo mitigarla. Otro aspecto fundamental es que las personas ya sean dueñas de su información o de una empresa, puedan realizar conocimientos mediante la educación continua de los sistemas de seguridad informática, la aplicación de autenticación dos factores y aplicar la seguridad en los puntos finales. Otro aspecto para considerar es el respaldo de la información segura y la capacidad que el usuario final conozca la necesidad de proteger la información. Sin duda alguna, estas buenas prácticas permiten formar una base sólida para la construcción de estrategias de seguridad y que éstas sean eficaces y cada una esté descargado mediante evidencias que sustente la novedad.

El presente análisis investigativo se ejecutó mediante un estudio documental y sistemático de la información literaria de acorte científico con el objetivo de identificar y analizar estrategias efectivas para el cuidado ante ataques de tipo ransomware. Para ello, se consultaron diversas bases de datos académicas y repositorios especializados ciberseguridad, tales como IEEE Xplorer, ACM Digital Library, Scopus, ScienceDirect, Web of Science y Google Scholar, así como informes técnicos emitidos por organismos internacionales como el National Institute of Standards and Technology (NIST), la European Union Agency for Cybersecurity (ENISA) y empresas reconocidas en seguridad informática como ESET, Karpersky, Symantec y Cloudflare.

## Resultados

Una vez obtenida y procesada la información, se pudo comprender de las estrategias de prevención que se puede aplicar para contrarrestar o mitigar los ataques de tipo ransomware. Al conocer su evolución y los métodos de propagación; se pudo identificar algunos aspectos para el manejo de buenas prácticas para garantizar la seguridad informática y la protección de la información. Aplicando su respectivo análisis de la información obtenida, se procede a recomendar la ejecución de buenas prácticas de seguridad efectiva, entre ellas:

1. **La evolución del ransomware y tendencias actuales:** Así como la tecnología va creciendo y evolucionando cada día de manera exponencial, los ataques de tipo ransomware también ha pasado por grandes cambios en los últimos años. En sus primeros años, solo se limitaba a cifrar los datos de la víctima y pedir un rescate

por su devolución o descifrar los datos. Hoy en día ya se escucha ataques de tiple extorsión en la cual, no solo le empresa se ve afectada, sino también con el acceso a la información, pueden llegar sus amenazas a clientes y socios comerciales. Es más, los ciberdelincuentes que día a día tratan que secuestrar la información, ya no le presta mucha atención al cifrado de archivos, optando ahora por la exfiltración y amenazas por la no divulgación de los datos pidiendo un valor a cambio por su liberación. La evolución del ransomware lo podemos observar en la tabla 1.

**Tabla 1**

*Evolución del ransomware*

| Año | Variante de Ransomware | Fuente |
|---|---|---|
| 2013 | CryptoLocker | Secureframe |
| 2014 | CryptoWall | |
| 2016 | Petya | |
| 2017 | WannaCry | |
| 2018 | Ryuk | |
| 2019 | Ryuk | |
| 2020 | BlackCat/ALPHV | |
| 2021 | LockBit 2.0 | |
| 2022 | LockBit 3.0 | |
| 2023 | LockBit | |

*Nota.* Estos datos fueron adoptados por (Karspersky, 2023)

2. **Métodos de infección y propagación del ransomware:** En la Tabla 2 se identificaron diversos métodos y propagación del ransomware. Los resultados del análisis revelan que los ataques de ransomware pueden ocurrir a través de múltiples vectores de infección.

**Tabla 2**

*Métodos de propagación de ransomware*

| Método de Infección | Descripción |
|---|---|

| | |
|---|---|
| Correos electrónicos de phishing | Envío de correos electrónicos fraudulentos que contienen enlaces o archivos adjuntos maliciosos. Al hacer clic, el ransomware se descarga e instala en el sistema de la víctima. |
| Explotación de vulnerabilidades | Aprovechamiento de fallas de seguridad en software desactualizado o sin parches para infiltrarse en el sistema y desplegar el ransomware. |
| Descargas maliciosas (drive-by-downloads) | Infección automática al visitor sitios web comprometidos que contienen código malicioso, sin necesidad de interacción por parte del usuario. |
| Dispositivos extraíbles infectados | Propagación del ransomware a través de dispositivos USB u otros medios extraíbles que, al conectarse a una computadora, ejecutan el código malicioso. |
| Ataques a RDP (Remote Desktop Protocol) | Acceso no autorizado a sistemas mediante la explotación de credenciales débiles o vulnerabilidades en servicios de escritorio remoto, permitiendo la instalación del ransomware. |
| Ingeniería social | Manipulación psicológica de las víctimas para que realicen acciones que comprometan la seguridad, como habilitar macros en documentos o desactivar medidas de seguridad. |
| Publicidad maliciosa (malvertising) | Inserción de anuncios infectados en sitios web legítimos que, al ser visualizados o |

| | |
|---|---|
| | clicados por el usuario, descargan e instalan el ransomware en el sistema. |
| Botnets y malware preinstalado | Distribución de ransomware a través de redes de bots o mediante software malicioso preinstalado en dispositivos antes de su venta. |

*Nota.* Datos de formas de cómo se propaga el ransomware de acuerdo con Cloudfare (2024).

3. **Estrategias de prevención contra el ransomware:** Como se puede observar en la Tabla 3, el estudio de la revisión sistemática permitió identificar un conjunto de estrategias de seguridad que han demostrado ser efectivas para prevenir ataques de ransomware. Entre las principales medidas preventivas se destacan:

**Tabla 3**

*Implementación de medidas de seguridad a las entidades afectadas*

| Medidas de Seguridad | Implementación | Descripción |
|---|---|---|
| Actualización de sistemas | 80% | Aplicación regular de actualizaciones de seguridad y soluciones de software para rectificar vulnerabilidades y prevenir la explotación por parte de atacantes. |
| Protocolos de respuesta | 75% | Establecimiento de planes de contingencia y recuperación ante incidentes para reducir el efecto ante un ataque de ransomware y restaurar operaciones rápidamente. |

| | | |
|---|---|---|
| Capacitación en ciberseguridad | 65% | Formación de usuarios en reconocimiento de amenazas como phishing, ingeniería social y buenas prácticas de seguridad informática |
| Autenticación de dos factores (2FA) | 70% | Implementación de mecanismos de autenticación multifactor para restringir accesos no autorizados y proteger credenciales de usuario. |
| Protección del correo electrónico | 72% | Uso de filtros de detección avanzados y análisis de correos electrónicos para prevenir ataques de tipo phishing y adjuntos maliciosos. |
| Seguridad en los puntos finales (endpoints) | 68% | Instalación de soluciones antimalware, control de aplicaciones y cifrado de discos duros para evitar infecciones en dispositivos individuales. |
| Copias de seguridad seguras | 77% | Implementación de backups inmutables y almacenamiento en ubicaciones seguras, con |

| | | |
|---|---|---|
| | | pruebas regulares de restauración. |
| Modelo de seguridad Zero Trust | 60% | Aplicación de controles de acceso estrictos, monitoreo de tráfico en la red y segmentación para evitar movimientos laterales del ransomware. |

*Nota.* Datos de la implementación de medidas de seguridad de acuerdo con Veam (2023)

4. **Uso incorrecto de la tecnología y riesgos asociados:** El análisis de este punto trajo como resultado que, el uso inoportuno de la tecnología aumenta los riesgos ante un ataque de tipo ransomware y otras amenazas cibernéticas. El déficit de conocimientos en seguridad informática, el acceso a sitios web inseguros y la instalación de software no verificado representan riesgos significativos. El uso no regulado de herramientas para eludir restricciones de red, como vpn no autorizada, proxies o software de tunneling como rayX, representan un riesgo significativo, ya que permite a los empleados o atacantes internos acceder a recursos en línea sin el monitoreo adecuado del departamento de TI. Esto facilita la descarga de software malicioso, el acceso a plataformas no seguras y la exfiltración de datos sin detección.
5. **Implementación de soluciones de seguridad avanzada:** Los hallazgos del estudio resaltan la necesidad de adoptar soluciones de seguridad avanzadas que permitan una detección y respuesta proactiva ante ataques de ransomware. Estas tecnologías fortalecen la posición de seguridad de una empresa y reducen significativamente el riesgo de infecciones y brechas de datos.

## Discusión

A partir de los resultados obtenidos en la presente investigación se determinó que las amenazas de tipo ransomware va creciendo de forma exponencial aprovechándose de los vacíos que tiene las personas sobre la cultura de la seguridad informática. La recopilación de

la información conlleva desde el año 2018 al año 2024; este estudio crítico y técnico mediante el método bibliográfico determinó algunas estrategias efectivas para la protección y mitigación de la información. Al encontrar soluciones documentadas, se procede a realizar la aplicación de buenas prácticas mediante procedimientos a seguir; no se puede seguir permitiendo que las empresas instituciones y usuarios finales continúen con conocimientos escasos en seguridad informática, contar con recursos tecnológicos y afinar una cultura de ciberseguridad.

El análisis documental permitió identificar las estrategias más recomendables para enfrentar un ataque de esta índole mediante la actualización periódica del software, uso de autenticación multifactor, la implementación de copias de seguridad dentro y fuera de la organización, aplicar software que permita dar soluciones de detección de amenazas y respuestas en endpoints. Todo este proceso va de la mano con el aporte humano, primero haciendo conciencia de la gravedad de este tipo de ataque por lo que su formación en seguridad informática es fundamental.

Esta investigación pretende establecer buenas prácticas sobre la aplicación de medidas de seguridad a través de las publicaciones revisadas y seleccionadas, resaltando la necesidad de aplicar mecanismos de capacitación para el recurso humano y la ejecución de guías de buenas prácticas accesible para todo puesto de trabajo y usuario final. En conclusión, se evidencia un papel importante en la seguridad de la información, identificar como funciona los ataques de tipo ransomware y combinar con herramientas tecnológicas que sea un apoyo para la seguridad informática.

## Conclusiones

Se concluye que los ataques de tipo ransomware es una de las amenazas con mayor impacto a nivel mundial por lo que el sector de la ciberseguridad le ha puesto mayor atención en los últimos años. La literatura obtenida y clasificada permitió identificar algunas estrategias que permitan prevenir este tipo de ataque.

Otro aspecto para considerar es comprender los mecanismos de mitigación que permita reducir el impacto de riesgo; puesto que, una vez que la información se haya puesto en compromiso, resulta difícil recupera de manera segura y confiable. Por ello entre los aspectos

estratégicos recomendable para este tipo de ataque son la constante actualización de software, el uso de autenticación multifactor; es oportuno a nivel de red, realizar una segmentación puesto que así se garantiza que toda la red no se vea comprometida, aplicar soluciones como sistemas EDR y modelos de seguridad Zero Trust.

Otro aspecto que la presente investigación resalta es la importancia de contar con el recurso humano capacitado en cuestión de seguridad informática; puesto que, la carencia de conocimiento al momento de saber cómo actuar frente a un ataque como el phishing, incrementará la vulnerabilidad ante estos ataques.

Por consiguiente, a parte del conocimiento, refuerzo continuo, es fundamental aplicar respaldos de seguridad; de esta manera que, si la información se vea comprometida, se pueda recuperar la información, sin depender del pago por el rescate. De esta manera se establecerá los correctos cimientos para la potenciación de la seguridad digital y la reducción del impacto por un ataque de tipo ransomware.

## Referencias bibliográficas

Agencia de Regulación y Control de las Telecomunicaciones. (2024). LockBit 3.0 Ransomware. Ecuador. https://www.ecucert.gob.ec/wp-content/uploads/2024/05/AL-2024-007-LockBit-3.0-Ransomware.pdf

Agencia de Regulación y Control de las Telecomunicaciones. (2024). Uso de Quick Assist en ataques de ingeniería. Ecuador. https://www.ecucert.gob.ec/wp-content/uploads/2024/05/AL-2024-009-Uso-de-Quick-Assist-en-ataques-de-ingenieria-social-y-ransomware.pdf

Aguirre, M. (s.f.). Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática. https://dspace.ups.edu.ec/handle/123456789/20566

Alvarado, J. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Revista Científica Aristas. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

Alvarado, M. (2021). Analysis for the adoption of security standards to improve the management of securities in public organizations. https://dspace.ups.edu.ec/handle/123456789/19760

Andrade, A. (2021). Gestión Informática Educativa: Un mapeo sistemático.

Astorga, C. (s.f.). Social Nerworks Dangers: How to educate our childs in cibersecurity. https://www.revistas.una.ac.cr/index.php/EDUCARE/article/view/10041

Cloudflare. (2024). Cómo prevenir los ataques de ransomware. https://www.cloudflare.com/es-es/learning/security/ransomware/how-to-prevent-ransomware/

Enriquez, L. (2022). Hacia una cultura de "Valor al Riesgo" en la ciberseguridad del Ecuador. Quito, Quito, Ecuador. https://www.uasb.edu.ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/

ESET. (2023). El 69% de las organizaciones de Latinoamérica sufrió algún incidente de seguridad durante el último año. EEUU. https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-69-de-las-organizaciones-de-latinoamrica-sufrio-algun-incidente-de-seguridad-durante-el-ultimom-ano/

Forntinet. (2023). ¿Cómo prevenir el ransomware? https://www.fortinet.com/lat/resources/cyberglossary/how-to-prevent-ransomware

IEEE. (2019). Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory. https://ieeexplore.ieee.org/document/8667352

IEEE. (2020). Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News. https://ieeexplore.ieee.org/document/8626866

IEEE. (2021). Behavioral Malware Classification using Convolutional Recurrent Neural Networks. https://ieeexplore.ieee.org/document/8659358

Karspersky. (2023). Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky

Morales, P., & Medina, P. (2021). CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR DE LA PROVINCIA DE TUNGURAHUA - ECUADOR. Ambato, Tungurahua, Ecuador: Cuadernos de desarrollo aplicados a las TIC.

https://www.researchgate.net/publication/352872168_Ciberseguridad_en_plataformas_educativas_institucionales_de_educacion_superior_de_la_provincia_de_Tungurahua_-_Ecuador

Nissim, N. (2022). Time-interval temporal patterns can beat and explain the malware. https://www.sciencedirect.com/science/article/abs/pii/S0950705122000843?via%3Dihub

Onofe, D. (2022). Ataques cibernéticos amenazan seguridad en Ecuador. Dialogo Americas. https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

Primicias. (2024). El 'ransomware' acecha a Ecuador y a otros países de la región. Ecuador. https://www.primicias.ec/noticias/tecnologia/ransomware-acecha-ecuador-paises-region/

Primicias. (2024). Ransomware: pagos a cibercriminales llegan a USD 7,8 millones en 2022. Ecuador: Primicias. https://www.primicias.ec/noticias/tecnologia/ransomware-pagos-cibercriminales-millonarios/

Swissinfo.ch. (2022). El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos. Quito, Ecuador: Swissinfo.ch. https://www.swissinfo.ch/spa/el-municipio-de-quito-víctima-de-ciberataque-que-afectó-el-15-de-sus-datos/47525602

veam. (2023). Prevención de ransomware: Protegiendo su mundo digital. https://www.veeam.com/blog/es/ransomware-prevention-best-practices.html

Veritas. (2024). Ramsonware. https://www.veritas.com/es/es/information-center/ransomware

**Conflicto de intereses:**

Los autores declaran que no existe conflicto de interés posible.

**Financiamiento:**

No existió asistencia financiera de partes externas al presente artículo.

**Agradecimiento:**

N/A

**Nota:**

El artículo no es producto de una publicación anterior.