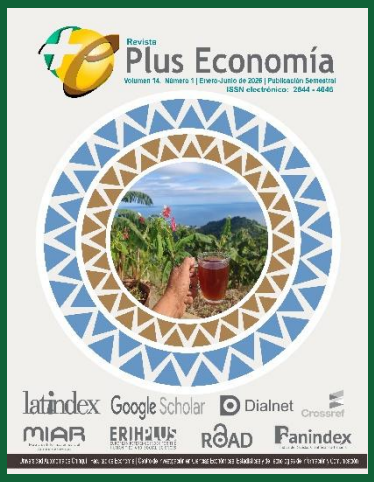
Revista
PLUS ECONOMÍA

República de Panamá
Universidad Autónoma de Chiriquí (UNACHI)
Facultad de Economía
Centro de Investigación en Ciencias Económicas, Estadísticas y de Tecnologías de Información y Comunicación (CICEETIC)
pluseconomia@unachi.ac.pa



ISSN electrónico: 2644-4046

EL IMPACTO DEL RANSOMWARE EN PANAMÁ (2021-2025)

The Impact of Ransomware in Panama (2021–2025)

Vol. 14, Núm. 1 | Enero-Junio de 2026 |

pp. 36-43

Cristina Núñez
Argelia García
Mixela Amaya
Frank Rivera

Centro Regional Universitario de Los Santos, Universidad de Panamá (UP)

Licencia CC BY-NC-SA 4.0 (https://creativecommons.org/licenses/by-nc-sa/4.0/)

EL IMPACTO DEL RANSOMWARE EN PANAMÁ (2021-2025)

DOI: https://doi.org/10.59722/pluseconomia.v14i1.1139

Fecha de recepción: 27/02/2025 **Fecha de aprobación:** 26/06/2025

Autor

CRISTINA NUÑEZ

https://orcid.org/0009-0003-5493-9814
criss062222@gmail.com

ARGELIA GARCÍA

https://orcid.org/0009-0008-6060-462X
argelialis44@gmail.com

MIXELA AMAYA

https://orcid.org/0009-0002-5835-8091
mixelade@gmail.com

FRANK RIVERA

https://orcid.org/0009-0002-9894-3455
frivmendiet@hotmail.com

Afiliación

CRU - Los Santos, Universidad de Panamá.

Resumen

Ransomware es un tipo de software malicioso (malware) que restringe el acceso a un sistema o a los datos de un usuario, exigiendo el pago de un rescate para restablecer el acceso.

En pleno siglo XXI, muchos somos aficionados a la tecnología, pero el ransomware se ha convertido en un tipo de malware que cifra los archivos o bloquea el acceso a un sistema. Este exige un rescate a la víctima para restaurar el acceso. Generalmente, los ataques piden el pago en criptomonedas para dificultar el rastreo. Si una empresa o persona es víctima de ransomware, se recomienda no pagar el rescate, ya que no garantiza la recuperación de los archivos. En este caso, se debe contactar a expertos en ciberseguridad**.**

Palabras clave

Ransomware, rescate ciberseguridad, malware, rastreo, rehén digital, ciberataque

The Impact of Ransomware in Panama (2021–2025)

Abstract: Ransomware is a type of malicious software (malware) that restricts access to a system or a user's data, demanding a ransom payment to restore access.

In the 21st century, many of us are technology fans, but ransomware has become a type of malware that encrypts files or blocks access to a system. This demands a ransom from the victim to restore access. Generally, attacks ask for payment in cryptocurrencies to make tracing difficult. If a company or person is a victim of ransomware, it is recommended not to pay the ransom, as it does not guarantee the recovery of the files. In this case, cybersecurity experts should be contacted.

Keywords: Rasomware, cybersecurity rescue, malware, tracking, digital hostage, cyberattack

Introducción

El ransomware ha cobrado numerosas víctimas en todo el mundo. Si una persona sospecha ser víctima de ransomware, el paso recomendable sería intentar recuperar los datos mediante métodos de descifrado, en lugar de ceder al chantaje de los criminales.

La creciente frecuencia de ataques de ransomware ha motivado un análisis profundo sobre el tema: "Impacto del ransomware en Panamá (2021-2025)". Para ello, es crucial confirmar la naturaleza del ataque, ya que estos suelen ocurrir al visitar sitios web inseguros o fraudulentos, o al descargar archivos y programas infectados.

En la actualidad, es imperativo adoptar medidas preventivas para proteger nuestra información del ransomware. Según el artículo de Kaspersky, "Protección contra el ransomware: cómo mantener a salvo tus archivos en 2025", se destaca que: "...el ransomware atrapa a la víctima, la convierte en un 'rehén digital' y exige un rescate para liberar lo secuestrado. Si no quieres que tu computadora o archivos sean bloqueados, la prevención es fundamental".

Para comprender mejor el ransomware, podemos definirlo como una de las amenazas más peligrosas en el mundo digital. Panamá ha sido blanco de múltiples ataques en los últimos años, afectando principalmente a empresas. El objetivo de estos ataques es secuestrar los archivos del usuario y exigir un rescate para su liberación. La prevención es clave para proteger la información (González, 2021).

Panamá ha avanzado en la regulación de la ciberseguridad mediante leyes y normativas que buscan proteger a empresas y ciudadanos. La Ley 81 de 2019, sobre Protección de Datos Personales, establece responsabilidades para el resguardo de información sensible.

Cada año, los ataques son más frecuentes y sofisticados. En 2024, Panamá experimentó un aumento significativo en los ataques de ransomware.

Materiales y métodos

Este estudio descriptivo se basó en un análisis documental exhaustivo de artículos, noticias y reportes publicados en más de 30 sitios web especializados. Se recopiló información sobre incidentes de ransomware en Panamá durante el período 2021-2025.

La recolección de datos incluyó el análisis de informes de seguridad emitidos por CSIRT-Panamá, CERT-Panamá y firmas de ciberseguridad. Se realizaron entrevistas a expertos en ciberseguridad para complementar el análisis cuantitativo y cualitativo, con el objetivo de obtener hallazgos significativos sobre el impacto actual del ransomware en Panamá. Los resultados obtenidos evidencian un aumento considerable en los ataques de ransomware en Panamá, lo que ha generado pérdidas significativas para diversas organizaciones.

Discusión

Según los resultados encontrados (en los sitios Web descritos anteriormente) nos indican que Panamá no se escapa de la realidad de los ataques cibernéticos, durante varios años hemos sido afectados por este tipo de ataque, logrando así causar daños irreversibles a entidades gubernamentales panameñas sufriendo

ataques de ransomware y afectando el acceso a servicios críticos.

Durante los años 2021 al 2025, Panamá registró un incremento en los ataques de ransomware, entre los más sobresaliente tenemos:

Año 2021:

- **Ministerio de Salud (MINSA):** En marzo de 2021, el Ministerio de Salud de Panamá sufrió un ataque de ransomware que afectó sus sistemas de información, comprometiendo datos sensibles de pacientes y operaciones internas (CERT-Panamá, 2021).

Año 2022

- **Ministerio de Economía y Finanzas (MEF):** En mayo de 2022, un ataque de ransomware afectó los servidores del MEF, generando retrasos en la facturación y afectando a contribuyentes (CERT-Panamá, 2022).
- **Empresa privada de telecomunicaciones**: En septiembre de 2022, ciberdelincuentes cifraron bases de datos de clientes, exigiendo un rescate en Bitcoin (CSIRT-Panamá, 2022).
- **Banco Nacional de Panamá:** En diciembre de 2022, un intento de ransomware logró cifrar servidores, pero fue mitigado a tiempo sin pérdidas financieras significativas (CSIRT-Panamá, 2022).

Año 2023

- **Supermercado de cadena nacional:** En junio de 2023, sus sistemas de pago fueron secuestrados por ransomware, interrumpiendo sus operaciones por días y causando millonarias pérdidas (Kaspersky, 2023).
- **Universidad Tecnológica de Panamá (UTP):** En marzo de 2023, los sistemas internos fueron atacados con ransomware, afectando la base de datos de estudiantes e investigadores (Kaspersky, 2023).
- **Bern Hotels & Resorts**: En diciembre de 2023, uno de los grupos hoteleros más grandes de Panamá fue atacado, comprometiendo información personal y operativa (CSIRT-Panamá, 2023).

Año 2024

- **Eastern Shipbuilding:** En febrero de 2024, la empresa de construcción naval fue atacada por el grupo Lockbit3, afectando sus operaciones (Panamcham, 2024).
- **Distribuidora David:** En agosto de 2024, esta empresa de servicios al consumidor fue atacada por el grupo Dispossessor (Panamcham, 2024).
- Firma Fábrega Molino: En marzo de 2024, esta firma de abogados fue atacada por el grupo Alphv, comprometiendo datos legales y de clientes (Panamcham, 2024).

Año 2025

- **BlackLock:** En 2025, el grupo BlackLock se ha convertido en uno de los más prolíficos, utilizando tácticas de doble extorsión y atacando infraestructuras críticas (Check Point, 2025).

Se espera un aumento en los ataques sofisticados, con actores de amenazas aprovechando tecnologías emergentes como la inteligencia artificial (Check Point, 2025).

Podemos analizar que, los sectores de banca y finanzas fueron los más afectados, seguidos del sector gubernamental. Los principales países de origen de estas amenazas fueron Estados Unidos (61%), Panamá (12%), Países Bajos (6%) y Singapur (3%). (La Estrella de Panamá, 2024)

En los libros y el web se encuentran estrategias que se deben tomar para proteger los datos y dentro de ellas podemos reafirmar:

- **Mantener el software actualizado** (Smith, 2020). Actualizar regularmente el sistema operativo y los programas reduce vulnerabilidades que pueden ser explotadas por ciberdelincuente. Se recomienda habilitar actualizaciones automáticas y utilizar parches de seguridad oficiales.
- **No abrir correos o enlaces sospechosos** (Kaspersky, 2022). Es importante verificar siempre la autenticidad del remitente y evitar abrir archivos adjuntos o enlaces sospechosos. Un ejemplo común en Panamá es la suplantación de identidad de bancos para obtener credenciales.

- **Realizar copias de seguridad** (NIST, 2021). Se recomienda realizar copias periódicas y almacenarlas en lugares seguros desconectados de la red.
- **Usar software de seguridad** (McAfee, 2021). Antivirus y herramientas anti-ransomware pueden detectar y bloquear amenazas antes de que afecten el sistema.
- **Deshabilitar macros en archivos sospechosos** (Microsoft, 2022). Algunos ataques utilizan macros en documentos de Word o Excel para ejecutar código malicioso.
- **Implementar autenticación de doble factor** (Google Security, 2021). El uso de doble autenticación en cuentas y accesos a sistemas dificulta el acceso de los atacantes en caso de robo de credenciales.
- **Educar y Sensibilizar sobre Ciberseguridad**. Capacitar a empleados y usuarios sobre buenas prácticas de ciberseguridad puede prevenir ataques exitosos.

Conclusiones

El ransomware ha experimentado un aumento considerable en Panamá durante los últimos años, impactando tanto al sector público como al privado. Este incremento ha resultado en pérdidas económicas sustanciales, riesgos significativos para la seguridad de datos críticos y una disminución en la confianza hacia los sistemas digitales.

La implementación de estrategias de protección y la inversión en ciberseguridad son cruciales para mitigar estas amenazas. Es esencial que las organizaciones adopten medidas preventivas, como la actualización constante de software, la realización de copias de seguridad y la capacitación continua del personal en prácticas de ciberseguridad. La colaboración público-privada es fundamental para prevenir futuros ataques de ransomware. Iniciativas como la creación de equipos de respuesta a incidentes y la realización de simulacros de ciberseguridad mejoran la preparación y la resiliencia organizacional.

El gobierno panameño debe continuar desarrollando y actualizando

regulaciones y políticas de ciberseguridad. La cooperación internacional es igualmente vital, dado que el ransomware es una amenaza global que demanda una respuesta coordinada a nivel mundial.

En síntesis, el aumento de los ataques de ransomware en Panamá resalta la urgencia de fortalecer las defensas cibernéticas nacionales. La inversión en tecnología de seguridad avanzada, la educación continua y la colaboración intersectorial son elementos clave para construir un entorno digital seguro y confiable. Solo un esfuerzo conjunto y sostenido permitirá mitigar el impacto de estas amenazas y salvaguardar el futuro digital de Panamá.

Referencias

ANPanamá. (s.f.). Empresas en Panamá, las más afectadas por ciberataques en la región. ANPanamá. https://www.anpanama.com/Empresas-en-Panama-las-mas-afectadas-por-ciberataques-en-la-region-15660.note.aspx

CERT-Panamá. (2021). Informe obre ciberataques en Panamá. Recuperado de https://cert.pa/?page_id=4094

CERT-Panamá. (2022). Reporte anual de incidentes de seguridad en Panamá. Recuperado de https://cert.pa/?page_id=4094

CSIRT-Panamá. (2022). Amenazas de ransomware en Panamá. Recuperado de https://csirt.pa/informes/ransomware2022.pdf

CSIRT-Panamá. (2023). Reporte sobre ataques de ransomware en Panamá. Recuperado de https://csirt.pa/informes/ransomware2023.pdf

Google Security. (2021). Protección de cuentas mediante autenticación de doble factor. Recuperado de https://security.google.com/protection/2fa

Kaspersky. (2023). Ransomware en Latinoamérica: tendencias y casos recientes. Recuperado de https://www.kaspersky.com/blog/ransomware-latam-2023

La Estrella de Panamá. (2024, 15 de enero). Ciberataques en Panamá se incrementaron en 74%: La banca es el sector más vulnerable. La Estrella de Panamá. https://www.laestrella.com.pa/economia/ciberataques-en-panama-se-incrementaron-en-74-la-banca-es-el-sector-mas-vulnerable-XK9480660?utm_source=chatgpt.com

NIST. (2021). Estrategias de respaldo y recuperación de datos. Recuperado de https://www.nist.gov/publications/data-backup-and-recovery-strategies-2021