Ransomware en Costa Rica: Lecciones aprendidas en instituciones públicas desde la ingeniería de sistemas

Ransomware in Costa Rica: Lessons Learned in Public Institutions from a Systems Engineering Perspective

Andy Alberto Carrillo-Espinoza[1]

Fecha de recepción: 2 de agosto, 2025
Fecha de aprobación: 18 de noviembre, 2025

Carrillo-Espinoza, A.A. Ransomware en costa rica: lecciones aprendidas en instituciones públicas desde la ingeniería de sistemas. *Tecnología en Marcha*. Vol. 39 Nº 2. Abril-Junio, 2026. Pág. 140-146.

https://doi.org/10.18845/tm.v39i2.8130

1 Consultor especialista en ciberseguridad. Co-fundador LAND4. Costa Rica.
andy.carrillo@land4.cr
https://orcid.org/0009-0001-6772-4420

Palabras clave

Ransomware; ciberseguridad; instituciones públicas; ingeniería de sistemas; Costa Rica; Zero Trust; MITRE ATT&CK.

Resumen

El ransomware es un software malicioso que cifra los archivos del sistema afectado y exige un pago por su liberación [1]. Su evolución ha pasado de familias aisladas como CryptoLocker a complejos modelos Ransomware-as-a-Service (RaaS), que extienden el delito mediante la venta o alquiler de kits listos para atacar [2], [3]. Costa Rica ha sido uno de los países latinoamericanos más golpeados: entre 2019 y 2024 varias instituciones públicas —incluida la Caja Costarricense de Seguro Social— sufrieron brechas críticas que derivaron en la declaración de emergencia nacional por ciberataques [4], mientras los registros del CSIRT-CR muestran una tendencia ascendente de incidentes en el mismo periodo [5]. Las pérdidas económicas asociadas a la campaña del grupo Conti en 2022 superaron los USD 125 millones e impactaron directamente en la continuidad de servicios esenciales [6]. Este artículo analiza las tácticas, técnicas y procedimientos observados en los principales incidentes costarricenses, mapeándolos al marco MITRE ATT&CK; identifica vulnerabilidades comunes en infraestructura, gobierno de TI y resiliencia organizacional; y propone un marco de defensa integral que combina controles de ISO/IEC 27001, el NIST Cybersecurity Framework y principios Zero Trust. Las lecciones aprendidas evidencian la necesidad de segmentación de red, autenticación multifactor, planes de respuesta y copias de seguridad inmutables como pilares para fortalecer la ciberresiliencia institucional.

Keywords

Ransomware; cybersecurity; public institutions; systems engineering; Costa Rica; Zero Trust; MITRE ATT&CK.

Abstract

Ransomware is malicious software that encrypts system files and demands payment for the decryption key [1]. Its trajectory has shifted from isolated strains such as CryptoLocker to a fully fledged Ransomware-as-a-Service (RaaS) economy on the darknet, where attack kits are rented to affiliates [2], [3]. Costa Rica stands out as one of the most affected Latin-American countries: successive campaigns between 2019 and 2024 forced the government to declare a national emergency, disrupting public health, finance and customs services [4]. National incident data published by CSIRT-CR confirm a steady rise in reported ransomware events over the same period [5], while losses attributed to the 2022 Conti campaign alone exceeded USD 125 million [6]. This study analyses the tactics, techniques and procedures employed in these attacks, mapping them to the MITRE ATT&CK knowledge base and correlating them with known vulnerability profiles. On this basis, it proposes an integrated defence framework that blends ISO/IEC 27001 controls, the NIST Cybersecurity Framework and Zero-Trust principles, emphasising network segmentation, multifactor authentication, immutable backups and rehearsed incident-response playbooks. The lessons extracted aim to guide public institutions in Latin America toward enhanced cyber-resilience and faster recovery when confronted with modern ransomware threats.

Introducción

El ransomware es un tipo de software malicioso que cifra los archivos del sistema comprometido y exige un pago a cambio de la clave de descifrado, afectando la disponibilidad y la confidencialidad de la información [1].

En la última década, la amenaza ha evolucionado de campañas aisladas —por ejemplo CryptoLocker en 2013— a un modelo de negocio industrializado conocido como Ransomware-as-a-Service (RaaS), donde los desarrolladores alquilan su có-digo y soporte a afiliados que ejecutan los ataques [2]. Este ecosistema ilícito reproduce la lógica de los servicios legí-timos en la nube, con paneles de control, reparto de beneficios y actualizaciones continuas que facilitan la escalabili-dad del delito [3].

Costa Rica experimentó el impacto más severo de esta tendencia en 2022, cuando la campaña del grupo Conti interrumpió servicios públicos esenciales y las pérdidas económicas directas superaron los USD 125 millones, según estimaciones independientes [6]. Este episodio visibilizó la vulnerabilidad de la infraestructura esta-tal y la necesidad de fortalecer la ciberresiliencia institucional.

De acuerdo con la Unión Internacional de Telecomuni-caciones, la ciberseguridad comprende el conjunto de herramientas, políticas y prácticas destinadas a proteger el en-torno digital y los activos de información ante amenazas, vulnerabilidades e incidentes maliciosos [7]. Bajo esta premisa, las instituciones públicas deben adoptar marcos de referencia y controles que permitan prevenir, detectar y responder oportunamente a los ataques de ransomware.

En este marco, el presente artículo analiza los principales incidentes de ransomware que afectaron al sector público costarricense entre 2019 y 2024, mapea las tácticas, téc-nicas y procedimientos (TTP) observados al marco MITRE ATT&CK y propone un marco de defensa integral basado en los controles de ISO/IEC 27001, el NIST Cybersecurity Framework y principios de Zero Trust. Las lecciones aprendidas pretenden orientar a las entidades públicas de América Latina hacia una mejor prevención, detección y respuesta frente a esta amenaza creciente.

Materiales y métodos

Diseño de investigación

El presente estudio se desarrolló bajo un enfoque cualitativo de alcance descriptivo-analítico, fundamentado en el análisis documental y forense de fuentes abiertas (OSINT). La metodología se estructuró para identificar, categorizar y correlacionar los vectores de ataque con los fallos de control en la infraestructura crítica nacional.

Selección de la muestra

Se aplicó un muestreo no probabilístico intencional para seleccionar los casos de estudio. Los incidentes analiza-dos corresponden a la Caja Costarricense de Seguro Social (CCSS), el Ministerio de Obras Públicas y Transportes (MOPT) y la Refinadora Costarricense de Petróleo (RECOPE). La selección se basó en tres criterios de inclusión: (1) incidentes ocurridos en el periodo 2019-2024, (2) afectación confirmada a la continuidad de servicios esenciales, y (3) disponibilidad de información técnica suficiente para la reconstrucción de la cadena de ataque.

Fuentes de información

La recolección de datos se realizó mediante la triangulación de fuentes primarias y secundarias:

- Fuentes oficiales: Se examinaron los portales del CSIRT-CR [8], el Reporte anual de incidentes 2023 del CSIRT-CR [5], así como la normativa nacional vigente sobre ciberataques [9] y los lineamientos de la Estrategia Nacional de Ciberseguridad 2023-2027.
- Estándares y reportes globales: El marco de referencia incluyó la norma ISO/IEC 27032:2023 [10] para la gestión de ciberseguridad, la base de datos de vulnerabilidades CVE Details [12] y el Crypto-Crime Report 2024 de Chainalysis [13] para contextualizar el entorno de amenazas global.

Procedimiento de análisis

El procesamiento de la información se sistematizó en dos fases:

1. Mapeo de Tácticas y Técnicas: Para cada caso, se reconstruyó el flujo del incidente identificando los puntos de entrada, movimiento lateral e impacto. Estos hallazgos se normalizaron utilizando la matriz de conocimiento MITRE ATT&CK [11], permitiendo una comparación estandarizada de los vectores de ataque. Se incorporaron estudios recientes sobre la aplicación de ATT&CK en entornos corporativos [14] para validar la clasificación.
2. Evaluación de Madurez y Contexto: Se contrastó la respuesta institucional contra los niveles de madurez digital del sector público [15]. Finalmente, para enriquecer la discusión más allá de los aspectos técnicos, se integró una perspectiva sobre la cultura de ciberseguridad académica [16] y el rol emergente de la inteligencia artificial en la formación de talento en TI [17], elementos clave para proponer soluciones sostenibles.

Resultados

El análisis forense comparativo de los incidentes en la CCSS, el MOPT y RECOPE permitió identificar patrones técnicos recurrentes en la cadena de ataque (Cyber Kill Chain). A continuación, se detallan los hallazgos categorizados por vector de compromiso y estado de los controles.

Vectores de acceso y movimiento lateral

Los datos evidencian que el compromiso inicial no dependió de vulnerabilidades de día cero (zero-day), sino de fallos en la higiene de seguridad básica. En el 100% de los casos analizados donde hubo divulgación técnica, el acceso inicial se logró mediante la explotación de servicios de escritorio remoto (RDP) expuestos a internet sin restricciones geográficas o a través de campañas de phishing dirigidas a credenciales administrativas.

Una vez dentro de la red, la ausencia de segmentación (arquitectura plana) y la falta de Autenticación Multifactor (MFA) fueron los factores determinantes que facilitaron la escalada de privilegios y el movimiento lateral sin detección, reproduciendo el escenario crítico que motivó la declaración de emergencia nacional en 2022 [4].

Impacto operativo y económico

A nivel de resiliencia, se constató que ninguna de las entidades contaba con respaldos inmutables o desconectados (air-gapped) en el momento del ataque. Esta carencia operativa provocó el cifrado de los sistemas de recuperación, prolongando la interrupción de servicios y elevando los costos de remediación. Específicamente, se estima que las pérdidas directas asociadas a la campaña del grupo Conti superaron los USD 125 millones, afectando a más de 30 000 estaciones de trabajo del sector público [6].

Esta tendencia de vulnerabilidad se ve corroborada por los registros del CSIRT-CR, que reportan un incremento sostenido del 38% en los incidentes de ransomware atendidos entre los años 2019 y 2024 [5].

Cuadro 1. Vulnerabilidades comunes identificadas en los ataques analizados.

Institución	Acceso inicial	Segmentación de red	MFA	Backups	Plan de respuesta
CCSS	RDP/ Hive	No	No	No	No
MOPT	Phishing	No	Parcial	Parcial	Parcial
RECOPE	No divulgado	No	Parcial	Parcial	Parcial

El Cuadro 1 sintetiza la postura de seguridad de las instituciones afectadas, evidenciando una ausencia sistémica de defensa en profundidad. Los hallazgos confirman que, independientemente de la institución, la falta de controles de identidad (MFA) y de contención (segmentación) constituyó el denominador común que maximizó el impacto de los ataques.

Discusión

Los hallazgos sugieren que la crisis de ciberseguridad en Costa Rica no fue consecuencia de una sofisticación tecnológica inédita por parte de los atacantes, sino de una deuda técnica acumulada en la gobernanza de TI. Al correlacionar los incidentes con el marco MITRE ATT&CK, se observa que técnicas estándar —como el abuso de credenciales válidas y servicios remotos externos— siguen siendo altamente efectivas debido a la falta de higiene digital básica en el sector público.

Contextualización regional

Este patrón de vulnerabilidad trasciende las fronteras nacionales. Al contrastar el caso costarricense con eventos recientes en la región, se identifican paralelismos claros. Por ejemplo, el ataque de ransomware a IFX Networks en Colombia paralizó más de dos millones de procesos judiciales en 2023 [18], y el compromiso al Ministerio de Salud de Argentina expuso debilidades críticas en el control interno de datos sensibles [19].

La similitud entre estos eventos confirma que las instituciones públicas latinoamericanas comparten una superficie de ataque frágil ante el modelo de Ransomware-as-a-Service (RaaS). Esto valida la hipótesis de que la inversión tecnológica aislada es insuficiente; se requiere adoptar marcos de arquitectura Zero Trust adaptados a la realidad presupuestaria y operativa de la región, tal como sugiere la normativa técnica nacional [9].

Limitaciones del estudio

Es necesario reconocer las limitaciones en el alcance de este análisis. Principalmente, la dependencia de fuentes de información pública restringe la profundidad técnica en ciertos casos. Específicamente, la falta de divulgación de un informe forense detallado sobre el incidente en RECOPE impide confirmar con certeza las técnicas de movimiento lateral empleadas. Asimismo, las cifras de impacto económico se basan en estimaciones de terceros [6], dado que no todas las instituciones han transparentado los costos totales de recuperación.

Conclusiones y recomendaciones

El análisis de los incidentes en la CCSS, el MOPT y RECOPE permite concluir que la severidad del impacto no respondió a la sofisticación de los vectores de ataque, sino a la ausencia de controles fundamentales de ciberhigiene. La evidencia forense confirmó que la explotación de servicios remotos (RDP) y el uso de arquitecturas de red plana facilitaron el despliegue del ransomware, demostrando la ineficacia de la seguridad perimetral tradicional frente a amenazas modernas.

A partir de estos hallazgos, se determinan las siguientes prioridades técnicas:

1. Gestión de Identidad: La implementación de Autenticación Multifactor (MFA) resulta imperativa para mitigar el compromiso de credenciales, identificado como el principal vector de acceso inicial.
2. Segmentación: La transición hacia modelos Zero Trust se establece como el único mecanismo validado para contener el movimiento lateral de los adversarios dentro de la red administrativa.
3. Resiliencia: La adopción de respaldos inmutables y desconectados (estrategia 3-2-1) constituye un requisito indispensable para garantizar la recuperación operativa ante el cifrado de activos críticos.

Referencias

[1] Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing & Analysis Center (MS-ISAC), #StopRansomware Guide: Ransomware and Data Extortion Prevention and Response, Washington, DC, USA, Jan. 2023. [Online]. Disponible en: https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (accesado Jul. 14, 2025).

[2] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A survey on ransomware: Evolution, taxonomy, and defense solutions,” Computers & Security, vol. 125, Art. no. 102913, 2023. [Online]. Disponible en: https://doi.org/10.1016/j.cose.2023.102913

[3] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, “The ransomware-as-a-service economy within the darknet,” Computers & Security, vol. 92, Art. no. 101762, 2020. [Online]. Disponible en: https://doi.org/10.1016/j.cose.2020.101762

[4] P. M. Datta and T. Acton, “Ransomware and Costa Rica’s national emergency: A defense framework and teaching case,” Journal of Information Technology Teaching Cases, vol. 13, no. 1, pp. 1–12, 2023. [Online]. Disponible en: https://doi.org/10.1177/20438869221149042

[5] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) – CSIRT-CR, Reporte anual de incidentes de seguridad informática 2023, San José, Costa Rica, 2023.

[6] C. Rosch, “Un ciberataque masivo en Costa Rica aflige a la ciudadanía,” Rest of World, Jun. 2, 2022. [Online]. Disponible en: https://restofworld.org/2022/ciberataque-costa-rica-ciudadania (accesado Jul. 14, 2025).

[7] International Telecommunication Union (ITU), Recommendation X.1205: Overview of Cybersecurity, Geneva, Switzerland, 2008. [Online]. Disponible en: https://www.itu.int/rec/T-REC-X.1205-200804-I/en (accesado Jul. 14, 2025).

[8] Centro Criptológico Nacional (CCN-CERT), “Creación del CSIRT-CR de Costa Rica,” 2023. [Online]. Disponible en: https://www.ccn-cert.cni.es/es/component/content/article/1002-creacion-del-csirt-cr-de-costa-rica.html?catid=23&Itemid=11827 (accesado Jul. 14, 2025).

[9] República de Costa Rica, Decreto Ejecutivo N.° 43542-MP-MICITT: Declaratoria de emergencia nacional por ciberataques, Imprenta Nacional, San José, Costa Rica, May 2022. [Online]. Disponible en: https://www.imprentanacional.go.cr (accesado Jul. 14, 2025).

[10] International Organization for Standardization (ISO), ISO/IEC 27032:2023 –Cybersecurity – Guidelines for Internet Security, 2nd ed., Geneva, Switzerland, 2023.

[11] MITRE Corporation, “ATT&CK® knowledge base,” 2025. [Online]. Disponible en: https://attack.mitre.org (accesado May 19, 2025).

[12] CVE Details, “CVE vulnerability database,” 2025. [Online]. Disponible en: https://www.cvedetails.com (accesado May 19, 2025).

[13] Chainalysis Inc., Crypto-Crime Report 2024, New York, NY, USA, 2024. [Online]. Disponible en: https://www.chainalysis.com/resources/reports/2024-crypto-crime-report/ (accesado Jul. 14, 2025).

[14] Y. Jiang, W. Zhou, C. Qian, and L. Li, “MITRE ATT&CK applications in cybersecurity and the way forward,” arXiv preprint arXiv:2502.10825, 2025. [Online]. Disponible en: https://arxiv.org/abs/2502.10825 (accesado Jul. 14, 2025).

[15] Programa Sociedad de la Información y el Conocimiento (PROSIC), Informe de labores 2022, Universidad de Costa Rica, San José, Costa Rica, Feb. 2025. [Online]. Disponible en: https://prosic.ucr.ac.cr/sites/default/files/2025-02/informe_2022_completo.pdf (accesado Jul. 14, 2025).

[16] M. P. Castro-López, “Conocimiento de la percepción de la ciberseguridad en los estudiantes de la Universidad de Costa Rica,” Tecnología en Marcha, vol. 37, no. esp. 6, pp. 5–11, 2024. [Online]. Disponible en: https://doi.org/10.18845/tm.v37i6.7261

[17] J. F. Useda-Medrano, A. A. Ortiz-García, and F. Chávez-Baltodano, “Visión estudiantil: IA en la transformación de la enseñanza de ingeniería en TI,” Tecnología en Marcha, vol. 38, no. esp. 5, pp. 37–46, 2025. [Online]. Disponible en: https://doi.org/10.18845/tm.v38i5.7897

[18] O. Griffin, “More than 50 Colombian state, private entities hit by cyber-attack– Petro,” Reuters, Sep. 18, 2023. [Online]. Disponible en: https://www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/ (accesado Jul. 14, 2025).

[19] Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), “La UFECI abrió una investigación preliminar por un supuesto ataque informático al Ministerio de Salud de la Nación,” Ministerio Público Fiscal de la Nación, Argentina, Oct. 24, 2022. [Online]. Disponible en: https://www.fiscales.gob.ar/cibercrimen/la-ufeci-abrio-una-investigacion-preliminar-por-un-supuesto-ataque-informatico-al-ministerio-de-salud-de-la-nacion/ (accesado Jul. 14, 2025).

Declaración sobre uso de Inteligencia Artificial (IA)

El autor declara el uso de las herramientas de inteligencia artificial *ChatGPT* y *Gemini* para traducir partes de este artículo del español al inglés. La herramienta nos ayudó a agilizar el proceso de traducción, pero realizamos una revisión exhaustiva para asegurar la calidad y precisión de las traducciones. Además, como apoyo para darle formato a las referencias bibliográficas.