Polo del Conocimiento

Pol. Con. (Edición núm. 96) Vol. 9, No 8
Agosto 2024, pp. 2710-2723
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v9i8.7850

Prevención de ataques ransomware en entidades públicas y privadas en el Ecuador

Prevention of ransomware attacks on public and private entities in Ecuador

Prevenção de ataques de ransomware a entidades públicas e privadas no Equador

Christhopher Wladimir Freire-Altamirano [I]
christhopher.freire.55@est.ucacue.edu.ec
https://orcid.org/0009-0000-7441-7691

Marco Yamba-Yugsi [II]
marco.yamba@ucacue.edu.ec
https://orcid.org/0000-0003-4095-1444

Laura Alexandra Ureta-Arreaga [III]
laura.ureta@ucacue.edu.ec
https://orcid.org/0000-0001-5328-8085

Correspondencia: christhopher.freire.55@est.ucacue.edu.ec

Ciencias de la Computación
Artículo de Investigación

*** Recibido:** 11 de junio de 2024 ***Aceptado:** 25 de julio de 2024 *** Publicado:** 19 de agosto de 2024

I. Universidad Católica de Cuenca, Azogues, Ecuador.
II. Universidad Católica de Cuenca, Cuenca, Ecuador.
III. Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El *ransomware* es un programa dañino que entra en las computadoras y encripta los archivos, impidiendo su acceso hasta que se abone un rescate. Esta forma de ataque informático aprovecha fallos en la seguridad cibernética para tomar información importante y pedir dinero, usualmente en forma de criptomonedas, a cambio de la clave para desencriptarla. El *ransomware* suele expandirse mediante emails de *phishing*, páginas web dañinas y debilidades en programas de computadora. La frecuencia y sofisticación creciente de estos ataques los convierten en una de las mayores amenazas en el campo de la ciberseguridad debido a su naturaleza destructiva y lucrativa. Cabe recalcar que el objetivo de esta investigación es analizar porque se da estos tipos de ataques de *ransomware* en entidades públicas y privadas de Ecuador. Dado el aumento significativo de estos ataques en los últimos años, se hace imperativo implementar medidas de ciberseguridad robustas para proteger datos sensibles y garantizar la continuidad operativa. Tambien se utilizó una metodología descriptiva que incluyó una revisión exhaustiva de la literatura existente y estudios de casos reales para identificar las mejores prácticas y su efectividad. Los resultados indican que la capacitación continua de empleados, la realización de copias de seguridad regulares, la actualización constante del software y el monitoreo continuo de las redes son fundamentales para la prevención de ataques de *ransomware*. Además, se destaca la importancia de establecer políticas de control de acceso y autenticación estrictas, así como de utilizar herramientas avanzadas de detección de amenazas. La conclusión enfatiza que una aproximación multidimensional, que combine educación, tecnología y políticas de seguridad, es esencial para una protección eficaz contra el *ransomware*. Este enfoque no solo reduce la vulnerabilidad de las entidades ecuatorianas frente a estos ataques, sino que también contribuye a una cultura organizacional de ciberseguridad sólida.

Palabras clave: *ransomware*; ciberseguridad; prevención; entidades públicas; Ecuador.

Abstract

Ransomware is a harmful program that enters computers and encrypts files, preventing access until a ransom is paid. This form of computer attack takes advantage of flaws in cybersecurity to take important information and ask for money, usually in the form of cryptocurrencies, in exchange for the key to decrypt it. Ransomware typically spreads through phishing emails, harmful web pages, and weaknesses in computer programs. The increasing frequency and sophistication of these attacks make them one of the biggest threats in the field of cybersecurity due to their destructive

and lucrative nature. It should be noted that the objective of this investigation is to analyze why these types of ransomware attacks occur in public and private entities in Ecuador. Given the significant increase in these attacks in recent years, it is imperative to implement robust cybersecurity measures to protect sensitive data and ensure operational continuity. A descriptive methodology was also used that included an exhaustive review of existing literature and real case studies to identify best practices and their effectiveness. The results indicate that continuous employee training, performing regular backups, constantly updating software, and continuous monitoring of networks are critical to preventing ransomware attacks. Additionally, the importance of establishing strict access control and authentication policies, as well as using advanced threat detection tools, is highlighted. The conclusion emphasizes that a multidimensional approach, combining education, technology and security policies, is essential for effective protection against ransomware. This approach not only reduces the vulnerability of Ecuadorian entities to these attacks, but also contributes to a strong organizational cybersecurity culture.

Keywords: ransomware; cybersecurity; prevention; public entities; Ecuador.

Resumo

Ransomware é um programa prejudicial que entra em computadores e criptografa arquivos, impedindo o acesso até que um resgate seja pago. Essa forma de ataque informático aproveita falhas de segurança cibernética para roubar informações importantes e pedir dinheiro, geralmente na forma de criptomoedas, em troca da chave para descriptografá-las. O ransomware normalmente se espalha por meio de e-mails de phishing, páginas da web prejudiciais e pontos fracos em programas de computador. A crescente frequência e sofisticação destes ataques fazem deles uma das maiores ameaças no domínio da cibersegurança devido à sua natureza destrutiva e lucrativa. Deve-se notar que o objetivo desta investigação é analisar por que esses tipos de ataques de ransomware ocorrem em entidades públicas e privadas no Equador. Dado o aumento significativo destes ataques nos últimos anos, é imperativo implementar medidas robustas de cibersegurança para proteger dados sensíveis e garantir a continuidade operacional. Foi também utilizada uma metodologia descritiva que incluiu uma revisão exaustiva da literatura existente e estudos de casos reais para identificar as melhores práticas e a sua eficácia. Os resultados indicam que o treinamento contínuo dos funcionários, a realização de backups regulares, a atualização constante de software e o monitoramento contínuo das redes são essenciais para prevenir ataques de ransomware. Além

disso, destaca-se a importância de estabelecer políticas rígidas de controle de acesso e autenticação, bem como de utilizar ferramentas avançadas de detecção de ameaças. A conclusão sublinha que uma abordagem multidimensional, que combine políticas educativas, tecnológicas e de segurança, é essencial para uma proteção eficaz contra o ransomware. Esta abordagem não só reduz a vulnerabilidade das entidades equatorianas a estes ataques, mas também contribui para uma forte cultura organizacional de cibersegurança.

Palavras-chave: ransomware; segurança cibernética; prevenção; entidades públicas; Equador.

Introducción

El *ransomware* es una forma de software malicioso que puede causar serios problemas. Básicamente, bloquea el acceso a los sistemas informáticos o encripta los datos importantes, y luego los atacantes exigen un pago para liberar esa información. Esto suele suceder cuando los ciberdelincuentes encuentran debilidades en la seguridad, a menudo a través de correos electrónicos engañosos, sitios web maliciosos o programas que no están actualizados (Malwarebytes, 2019).

El incremento de ataques de *ransomware* ha puesto en jaque a las entidades públicas y privadas de Ecuador (Alvarado J. , 2020), subrayando la vulnerabilidad de las infraestructuras digitales frente a estas amenazas. En los últimos años, se han registrado numerosos incidentes que han afectado significativamente la operación de diversas organizaciones (El Comercio, 2019).

Por ejemplo, en abril de 2022, el Municipio de Quito fue víctima de un ataque que afectó entre el 15% y el 20% de su información, dejando fuera de servicio su plataforma de trámites digitales temporalmente (Primicias, 2024). Este ataque tenía como objetivo inhabilitar todo el archivo digital de la administración municipal, dejando la información encriptada (Enriquez, 2022). Asimismo, el Banco Pichincha sufrió varios ciberataques en 2021, los cuales interrumpieron sus operaciones, afectaron los cajeros automáticos y el portal de banca *online* (Primicias, 2024).

Estos incidentes destacaron la necesidad de fortalecer la seguridad cibernética en el sector financiero. De hecho, Ecuador se encuentra entre los países de Latinoamérica más golpeados por los delitos informáticos, ocupando el puesto 119 de 182 países en vulnerabilidad por ataques cibernéticos según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (Alvarado J. , 2020).

El problema específico que este estudio aborda es la vulnerabilidad de las entidades públicas y privadas de Ecuador frente a los ataques de *ransomware*. Estos ataques representan una amenaza significativa para la seguridad de los datos y la continuidad operativa de las organizaciones. Mitigar este problema es crucial para proteger la información sensible y asegurar la estabilidad de los servicios esenciales en el país.

La problemática de los ciberataques en Ecuador no es aislada, sino que forma parte de una tendencia creciente en toda América Latina, el uso de la virtualidad aumentó exponencialmente, incrementando el flujo de información digital y, con ello, las oportunidades para los cibercriminales (Enriquez, 2022). En 2022, los ataques de *ransomware* en la región aumentaron un 25% respecto al año anterior (Primicias, 2024). Países como Costa Rica han declarado emergencias nacionales debido a ciberataques, subrayando la gravedad de la situación (Onofe, 2022).

Además, un informe de Kaspersky señaló que el Ecuador en los últimos 12 meses ha recibido 212000 ataques de los cuales 139000 fueron del *ransomware WannaCry*, destacando la magnitud de la amenaza en la región (Karspersky, 2023). Numerosos estudios han explorado la naturaleza y el impacto de los ataques de *ransomware* a nivel global. Investigaciones previas han identificado las principales técnicas utilizadas por los cibercriminales y han destacado la necesidad de implementar medidas preventivas efectivas (Enriquez, 2022).

Sin embargo, existe una brecha en el conocimiento sobre la efectividad de estas medidas en el contexto específico de Ecuador y América Latina. Este estudio busca llenar esa brecha, proporcionando una evaluación de las estrategias de prevención más efectivas en este entorno. El objetivo de este estudio es desarrollar estrategias efectivas para prevenir ataques de *ransomware* en entidades públicas y privadas de Ecuador.

El objetivo de esta investigación es evaluar y mejorar la efectividad de las medidas de ciberseguridad en empresas públicas y privadas en Ecuador mediante la implementación, capacitación en ciberseguridad para empleados y la adopción de sistemas automatizados. Este objetivo busca reducir el riesgo de ciberataques y minimizar las pérdidas financieras, abordando la necesidad crítica de concientización en ciberseguridad y la falta de preparación detectada en análisis previos. La capacitación en seguridad y las actualizaciones de sistemas han demostrado ser efectivas en la defensa contra amenazas como *LockBit 3.0* y *Quick Assist*, destacando la importancia de una preparación adecuada y la relación directa entre las medidas de seguridad implementadas y la eficacia en la respuesta a incidentes. La pregunta de investigación específica

que se abordarán incluye: ¿Cuáles son las medidas de ciberseguridad más efectivas para prevenir ataques de *ransomware* en Ecuador?

Este estudio es importante porque proporciona una comprensión detallada de las amenazas de *ransomware* en Ecuador y ofrece recomendaciones prácticas para mejorar la ciberseguridad en el país. Las implicaciones prácticas incluyen la implementación de programas de capacitación, la adopción de tecnologías avanzadas de monitoreo y la cooperación interinstitucional. Estos resultados no solo contribuirán al fortalecimiento de la ciberseguridad en Ecuador, sino que también ofrecerán una base sólida para futuras investigaciones y desarrollos en el campo de la ciberseguridad.

Metodología

El estudio realizado fue de carácter descriptivo, con un enfoque mixto, enfocado en examinar y explicar los ataques de *ransomware* y las estrategias de prevención y respuesta aplicadas en organizaciones tanto públicas como privadas en Ecuador. Fue llevada a cabo una completa recolección de datos secundarios de fuentes como publicaciones académicas, informes técnicos y estudios de casos relevantes, lo que permitió establecer una base sólida y actualizada sobre la ciberseguridad en el país.

La combinación de datos cualitativos y cuantitativos se utilizó para lograr una comprensión completa de la situación. La información cualitativa examinó vivencias, tácticas y obstáculos enfrentados por las organizaciones afectadas, evaluando narraciones de profesionales en ciberseguridad e informes sobre incidentes concretos. Los datos numéricos y las medidas tomadas, posibilitaron un análisis total de la situación.

Se explicó la frecuencia de ataques, variedades de *ransomware*, protocolos de protección, repercusiones y eficacia de las respuestas utilizando la información disponible. La obtención de datos se llevó a cabo en un solo periodo de tiempo, desde 2019 hasta 2023, combinando información de varias fuentes para ofrecer una perspectiva completa de los incidentes pasados y presentes.

Los casos individuales de entidades afectadas por *ransomware* fueron incluidos en la unidad de análisis. La investigación se enfocó en describir y correlacionar patrones y tendencias observados. La validez interna se aseguró al utilizar fuentes verificadas y actualizadas, junto con un análisis riguroso con verificaciones cruzadas para evitar sesgos y garantizar la precisión. Se recopilaron

datos a través de la revisión de literatura académica y técnica, y se llevó a cabo el análisis utilizando tanto metodologías cualitativas como cuantitativas.

El estudio utilizó información secundaria y no requirió consentimiento informado al no incluir la participación directa de individuos humanos. Se aseguró la protección de las consideraciones éticas relacionadas con la confidencialidad y anonimato de la información utilizada. Toda la información se obtuvo de fuentes públicas y disponibles, siguiendo las normas éticas de investigación.

Resultados

Los planes de contingencia son fundamentales, ya que los servicios o negocios no pueden detenerse sin incurrir en pérdidas económicas. La Secretaría Nacional de Administración Pública (SNAP), encargada del estado, ha establecido directrices para la Seguridad de la Información. La perspectiva, mediante la cual se direccionan los datos de manera segura, considera alternativas de cooperación a los procesos internos.

Sin embargo, tanto el sector público como el privado carecen de una planificación de continuidad del negocio que incluya un plan de Respuesta a Incidentes Cibernéticos (CIRP, por sus siglas en inglés). Hasta ahora, solo se ha implementado un conjunto de sitios alternativos para casos de desastres (naturales o artificiales). Evaluar las amenazas permitirá determinar las mejores medidas de prevención que deben adoptarse para proteger a la organización o empresa. Se identificaron patrones y tendencias en los ataques de *ransomware*. Los datos cualitativos fueron analizados a través de la codificación temática con el fin de comprender las experiencias y estrategias de las entidades afectadas.

Caso de ciberataque en el Ecuador: En el 2019, se observaron ciberataques dirigidos a los sitios web de organizaciones gubernamentales y privadas en Ecuador. Entre las instituciones públicas afectadas se encontraban la embajada, el banco central, la presidencia y el SRI, entre otras, debido a conflictos diplomáticos relacionados con Julian Assange. Este incidente puso en evidencia la insuficiente preparación y la baja percepción de la importancia de la ciberseguridad en el país (El Comercio, 2019). Aunque los ataques no tuvieron un impacto significativo, la falta de interés en invertir en ciberseguridad por parte de las empresas resultó en sitios web y bases de datos comprometidos, entre otros incidentes, como podemos observar en la *tabla 1* las tendencias a partir del 2019 hasta el 2024.

Tabla 1.

Tabla de tendencia de ataques Ransomware entre 2019 y 2023.

Año	Número de Ataques Documentados
2019	682
2020	1852
2021	1340
2022	393
2023	1750
2024	2500 hasta mayo del 2024

Nota: Estos datos fueron adaptados de (Karspersky, 2023)

Tipos de *ransomware* utilizados: En la *Tabla 2* se identificaron diversas cepas de *ransomware* utilizadas en los ataques, incluyendo *LockBit 3.0* y otras variantes documentadas en informes técnicos (Agencia de Regulación y Control de las Telecomunicaciones, 2024).

Tabla 2.

Frecuencia de Ransomware utilizados.

Tipo de *Ransomware*	Frecuencia de Uso
LockBit 3.0	Alta
Quick Assist	Media
Otras variantes	Variable

Nota. Los datos fueron extraídos de (Agencia de Regulación y Control de las Telecomunicaciones, 2024). Se considera alta cuando el más del 50% de los ataques de ransomware fueron documentados en un año. Puede ser considerado de media frecuencia si ha sido responsable de aproximadamente el 20% al 40% de los ataques de ransomware documentados en un año. Se clasifica Variable si aparecen en menos del 20% de los ataques documentados y no muestran un patrón claro o consistente en su uso.

Medidas de seguridad implementadas: Como podemos observar en la *Tabla 3* las entidades afectadas han implementado una variedad de medidas de seguridad, tales como la actualización de sistemas, implementación de protocolos de respuesta rápida y capacitación en ciberseguridad para el personal.

Tabla 3.

Implementación de medidas de seguridad a las entidades afectadas.

Medida de Seguridad	Implementación (%)
Actualización de sistemas	80%
Protocolos de respuesta	75%
Capacitación en ciberseguridad	65%

Nota. Datos adaptados de (Primicias, 2024) y (Swissinfo.ch, 2022)

Impacto de los ataques: Los ataques de *ransomware* han tenido un impacto significativo en las operaciones de las entidades afectadas, causando desde interrupciones temporales hasta pérdidas financieras considerables. La Agencia de Regulación y Control de las Telecomunicaciones reportó que el ataque al Municipio de Quito afectó aproximadamente el 15% de sus datos como podemos observar en la *Tabla 4.*

Tabla 4.

Efectos de los ataques recibidos en las entidades.

Entidad Afectada	Impacto del Ataque
Municipio de Quito	15% de los datos afectados
Banco Pichincha	Interrupciones temporales
Otras entidades	Pérdidas financieras

Nota. Estos datos fueron obtenidos de (Onofe, 2022) y (Swissinfo.ch, 2022)

Efectividad de las respuestas: La efectividad de las respuestas varió según la entidad y la preparación previa como lo podemos visualizar en la *Tabla 5*. Las entidades con protocolos de respuesta establecidos y personal capacitado lograron mitigar mejor los efectos de los ataques.

Tabla 5.

Nivel de respuesta ante los efectos de los ataques Ransomware.

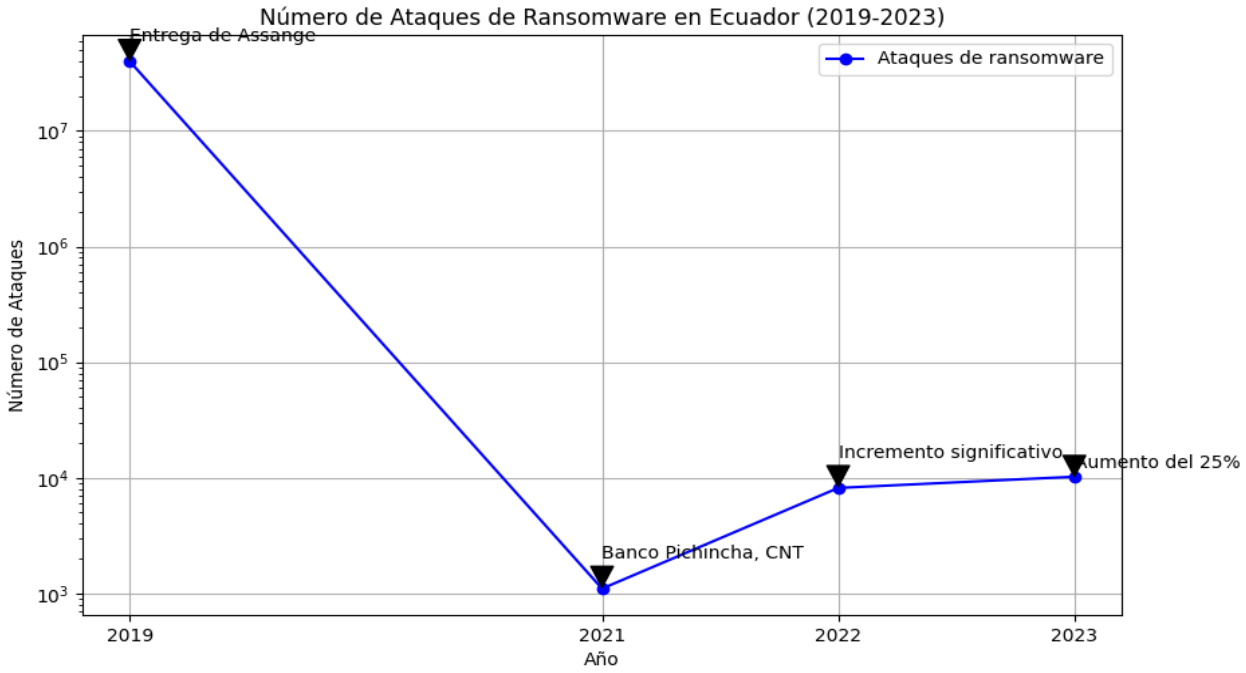
Entidad	Efectividad de la Respuesta
Municipio de Quito	Alta
Banco Pichincha	Media
Otras entidades	Variable

Nota. Datos extraídos de (Swissinfo.ch, 2022). La efectividad de la respuesta se considera alta cuando la entidad mitiga rápidamente el ataque y restaura operaciones con mínimas interrupciones. Es media si la recuperación es razonable pero aún conlleva algunas pérdidas y demoras. Es variable si la entidad muestra inconsistencias significativas en su capacidad de respuesta y recuperación.

Identificación de patrones y tendencias: Se identificaron patrones y tendencias en los ataques de *ransomware*, como el incremento en la frecuencia de los ataques durante los años analizados y la prevalencia de ciertas cepas de *ransomware*, como *LockBit 3.0* y *Quick Assist*.

Figura 1

Entre el año 2019 y 2023 el número de ataques Ransomware fue aumentando.



Fuente: A partir de Tecnociencias (Primicias, 2024)

Pol. Con. (Edición núm. 96) Vol. 9, No 8, Agosto 2024, pp. 2710-2723, ISSN: 2550 - 682X

Tabla 6.

Ataques documentados entre el 2019 y 2023.

Año	Número de Ataques Documentados	Descripción de Incidentes	Fuente
2019	682	Ataque masivo tras la entrega de Julián Assange	**Primicias**
2021	1852	Banco Pichincha, CNT, Ministerio de Finanzas	**Welivesecurity**
2022	1340	Incremento significativo de ataques, afectando diversas entidades	**Sextas Jornadas de Seguridad Bancaria**
2022	393	Ataques a bancos, retail y organismos públicos	**Fluid Attacks**
2023	1750	Incremento de ataques de *ransomware* en general	**Forbes**

Nota. Elaboración de un conjunto de artículos (Primicias, 2024), (Onofe, 2022), (Alvarado J. , 2020)*, etc.*

Discusión

En este artículo se examinó la situación de los ataques de *ransomware* en Ecuador durante el período de 2019 a 2024, encontrando un aumento significativo en los últimos años. Estos hallazgos están en línea con estudios previos a nivel global. Según Interpol (2020) y Unit 42 de Palo Alto Networks (2024) reportan que estos ataques también van en aumento. Es decir, no es una tendencia única de Ecuador, sino a nivel mundial. Estos datos subrayan la necesidad de implementar medidas de ciberseguridad más robustas para proteger tanto a las entidades públicas como privadas. También se puede adaptar, las medidas de seguridad que las organizaciones de más prestigio están utilizando para mitigar los ataques y adaptarlas a nuestro entorno.

Ecuador ha implementado varias estrategias para enfrentar los ciberataques, como, por ejemplo: la actualización de sistemas, la implementación de protocolos de respuesta rápida y la capacitación al personal Toapanta et al. (2020) Por otro lado, en el estudio realizado por SMT Toapanta y otros (2020), destaca que en Latinoamérica se han desarrollado algoritmos para prevenir y minimizar los ciberataques. Mientras Ecuador han optado por mejorar la infraestructura y la capacitación interna, en Latinoamérica ha sido más amplio, buscando soluciones tecnológicas avanzadas y modelos

generales de protección. Ecuador debe considerar soluciones más amplias como las implementadas en el resto de países latinoamericanos.

Para mejorar la preparación para la ciberseguridad en Ecuador, es esencial considerar no solo los aspectos técnicos sino también los factores socioeconómicos y políticos que influyen en las prácticas de ciberseguridad en el país. Las investigaciones futuras sobre ciberseguridad en Ecuador deberían centrarse en explorar las amenazas, tendencias y tecnologías emergentes para anticiparse a los riesgos y vulnerabilidades cibernéticos. Los responsables políticos y las organizaciones de Ecuador deben priorizar las inversiones e iniciativas en ciberseguridad para fortalecer la postura del país en materia de ciberseguridad y proteger la infraestructura crítica y los datos confidenciales de los ciberataques.

Conclusiones

En conclusión, la capacitación en seguridad a los empleados es fundamental para reducir el riesgo de ciberataques en Ecuador. Los programas de concientización minimizan la vulnerabilidad y generan beneficios económicos. La implementación de sistemas automatizados como CyRIS mejorará la formación en ciberseguridad. Además, los planes de contingencia son esenciales para evitar pérdidas financieras. Aunque SNAP ha establecido políticas, carece de un Plan de respuesta a incidentes cibernéticos (CIRP). El análisis de amenazas ayuda a determinar las mejores medidas preventivas.

El análisis de enfoque mixto reveló patrones y estrategias para combatir los ataques de *ransomware*, destacando amenazas como *LockBit 3.0* y *Quick Assist*. Las empresas han introducido medidas de seguridad como actualizaciones de sistemas y formación en ciberseguridad que han demostrado su eficacia en empresas con protocolos y personal capacitado. La identificación de patrones y la relación entre las medidas de seguridad y la eficacia de la respuesta resalta la importancia de una preparación adecuada. Los ciberataques de 2019 demostraron la falta de preparación en materia de ciberseguridad en Ecuador. Las empresas que invirtieron en actualizaciones de sistemas y capacitación pudieron defenderse mejor de los ataques.

Referencias

1. Alvarado, J. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. ITSJBA. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf
2. Arevalo, D., & Afp, A. (s. f.). Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange. El Comercio. https://www.elcomercio.com/actualidad/seguridad/ecuador-denuncia-millones-ciberataques-assange.html
3. Ecucert. (2024). Uso de Quick Assist en ataques de ingeniería social que conducen a ransomware. 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
4. Efe. (2024, 31 enero). El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos. SWI swissinfo.ch. https://www.swissinfo.ch/spa/el-municipio-de-quito-v%C3%ADctima-de-ciberataque-que-afect%C3%B3-el-15-de-sus-datos/47525602
5. El 69% de las organizaciones de Latinoamérica sufrió algún incidente de seguridad durante el último año. (s. f.). ESET. 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/
6. Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky. (2023, 30 agosto). Kaspersky. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky
7. Enriquez, L. (2024, 6 marzo). Hacia una cultura de «Valor al riesgo» en la ciberseguridad del Ecuador. Observatorio Ciberderechos y Tecnosociedad.
8. https://www.uasb.edu.ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/
9. Galiette, A., & Santos, D. (2024, 11 enero). Medusa Ransomware Turning Your Files into Stone. Unit 42. https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
10. LockBit 3.0 Ransomware. (2023). Centro De Respuesta A Incidentes Informáticos Del Ecuador. https://www.ecucert.gob.ec/wp-content/uploads/2024/05/AL-2024-007-LockBit-3.0-Ransomware.pdf

11. Morales-Paredes, P. I., & Medina-Chicaiza, P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. 3C TIC, 10(2), 49-75. https://doi.org/10.17993/3ctic.2021.102.49-75
12. Pesantes, K. (2023, 13 octubre). Ransomware: pagos a cibercriminales llegan a USD 7,8 millones en 2022. Primicias. https://www.primicias.ec/noticias/tecnologia/ransomware-pagos-cibercriminales-millonarios/
13. Primicias, E. /. R. (2023, 18 octubre). El «ransomware» acecha a Ecuador y a otros países de la región. Primicias. https://www.primicias.ec/noticias/tecnologia/ransomware-acecha-ecuador-paises-region/
14. Solano, E. (2022, 30 junio). Ataques cibernéticos amenazan seguridad en Ecuador - Diálogo Américas. Diálogo Américas. https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/
15. Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. (s. f.). https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19
16. Malwarebytes. (2019, 25 noviembre). Ransomware: qué es y cómo eliminarlo. Malwarebytes. https://es.malwarebytes.com/ransomware/