593 Digital Publisher
CEIT
ISSN 2588-0705

¿Están los institutos universitarios en Ecuador preparados para los ciberataques?

Are Ecuadorian universities prepared for cyberattacks?

Feddor Gabriel Derenzin-Martinez [1]
Tecnológico Universitario Euroamericano - Ecuador
fderenzin@euroamericano.edu.ec

doi.org/10.33386/593dp.2024.6.2864

V9-N6 (nov-dic) 2024, pp 1220-1232 | Recibido: 21 de agosto del 2024 - Aceptado: 30 de septiembre del 2024 (2 ronda rev.)

1 ORCID: http://orcid.org/0009-0002-0357-7764

Cómo citar este artículo en norma APA:A

Derenzin-Martinez, F., (2024). ¿Están los institutos universitarios en Ecuador preparados para los ciberataques?. 593 Digital Publisher CEIT, 9(6), 1220-1232, https://doi.org/10.33386/593dp.2024.6.2864

Descargar para Mendeley y Zotero

RESUMEN

En el último año, las instituciones educativas se han convertido en uno de los sectores más atacados a nivel mundial, según el Check Point Security Report (2024a). Esto pone en peligro la seguridad de los datos y la continuidad de las operaciones académicas. En Ecuador, datos de ESET (2023) revelan que el país ocupa el primer lugar en ataques de phishing en Latinoamérica, lo que evidencia su vulnerabilidad ante múltiples amenazas, incluyendo malware, ransomware y ataques de ingeniería social. A pesar de la creciente preocupación, la falta de datos específicos sobre el impacto en las universidades ecuatorianas limita la comprensión plena de la magnitud del problema.

Las herramientas de código abierto han emergido como una solución viable para mejorar la ciberseguridad, siempre que se cuente con personal capacitado para su implementación. No obstante, la automatización sin supervisión puede generar riesgos adicionales, lo que resalta la importancia de combinar la tecnología con la intervención humana. La colaboración internacional es fundamental para fortalecer la seguridad cibernética en las universidades, permitiendo el intercambio de conocimientos y recursos. La creación de Centros de Operaciones de Seguridad (SOC) basados en tecnologías abiertas ha demostrado ser una estrategia eficaz para el monitoreo y la respuesta a incidentes en tiempo real, ofreciendo también oportunidades de formación práctica. En Ecuador, la colaboración con el Equipo de Respuesta a Emergencias Informáticas (EcuCERT) podría fortalecer aún más la seguridad en el ámbito universitario.

Palabras claves: ciberataques, ciberseguridad, colaboración, educación, SOC (centro de operaciones de seguridad).

ABSTRACT

In the last year, educational institutions have become one of the most attacked sectors worldwide, according to the Check Point Security Report (2024a). This puts data security and the continuity of academic operations at risk. In Ecuador, data from ESET (2023) reveals that the country ranks first in phishing attacks in Latin America, which shows its vulnerability to multiple threats, including malware, ransomware, and social engineering attacks. Despite growing concern, the lack of specific data on the impact on Ecuadorian universities limits a full understanding of the magnitude of the problem.

Open source tools have emerged as a viable solution to improve cybersecurity, provided that trained personnel are available for their implementation. However, unsupervised automation can generate additional risks, highlighting the importance of combining technology with human intervention. International collaboration is essential to strengthen cybersecurity in universities, allowing the exchange of knowledge and resources. The creation of Security Operations Centers (SOC) based on open technologies has proven to be an effective strategy for monitoring and responding to incidents in real time, while also offering practical training opportunities. In Ecuador, collaboration with the Computer Emergency Response Team (EcuCERT) could further strengthen security in the university environment.

Keywords: cyberattacks, cybersecurity, collaboration, education, SOC (security operations center).

Introducción

El avance acelerado de la digitalización y el uso intensivo de la tecnología en los institutos universitarios de Ecuador han expuesto a estas instituciones a una creciente ola de ciberamenazas cada vez más sofisticadas. Los ataques como el ransomware, el malware y el phishing se han vuelto comunes, afectando tanto a empresas privadas como a instituciones educativas, las cuales ahora son objetivos prioritarios para los ciberdelincuentes. Según informes recientes de EcuCERT (2021) y el Check Point Security Report (2024a), el número de direcciones IP comprometidas ha aumentado críticamente, destacando una evolución en las técnicas empleadas por los atacantes, quienes se dirigen específicamente al sector educativo. Esta situación subraya la necesidad urgente de implementar estrategias robustas y adaptativas para enfrentar estas amenazas (CHECK POINT, 2024a).

En Ecuador, se ha observado un incremento alarmante en los ataques de ingeniería social, los cuales explotan la confianza humana para obtener acceso a información sensible. Un estudio reciente muestra que la mayoría de los incidentes cibernéticos reportados están relacionados con el phishing, y Ecuador es uno de los países más afectados en Latinoamérica (ESET, 2023). Además, el país ha experimentado un aumento en los ciberdelitos en general, como lo evidencian los numerosos ataques informáticos a empresas y entidades públicas, lo que demanda una mejora en la seguridad digital y la concienciación sobre los riesgos asociados (Juca-Maldonado & Medina-Peña, 2023).

A medida que las instituciones educativas dependen cada vez más de la infraestructura digital para sus operaciones diarias, la seguridad cibernética se convierte en un desafío crucial. Un estudio reciente sugiere que los costos asociados a los incidentes de ciberseguridad son un factor determinante en las decisiones de inversión en seguridad, indicando que las instituciones deben aprender de sus experiencias para justificar y aumentar sus inversiones en ciberseguridad. Esto refleja la importancia de implementar un aprendizaje organizacional efectivo, que derive de la evaluación de incidentes previos para mejorar las capacidades de respuesta (Shaikh & Siponen, 2024).

El objetivo de este estudio es analizar las ciberamenazas que afectan a las instituciones universitarias en Ecuador, identificar los principales tipos de ataques y proponer soluciones basadas en prácticas de ciberseguridad adaptadas a este sector. Se plantea la siguiente pregunta de investigación: ¿Qué medidas de seguridad cibernética pueden implementar las universidades ecuatorianas para mitigar el impacto de ciberamenazas crecientes?

Para profundizar en este análisis, a continuación, se presentan los principales desafíos, oportunidades y estrategias que las universidades ecuatorianas deben enfrentar y adoptar para mejorar su ciberseguridad. Estos puntos se abordan en las siguientes secciones, comenzando por los retos actuales y avanzando hacia soluciones concretas que incluyen la adopción de herramientas de código abierto y la colaboración internacional.

Retos actuales de ciberseguridad en universidades

A pesar de la creciente amenaza, muchas universidades en Ecuador carecen de los recursos necesarios para implementar estrategias efectivas de ciberseguridad, como los Centros de Operaciones de Seguridad (SOC). Según 11 Strategies of a World-Class Cybersecurity Operations Center, "la defensa contra adversarios cibernéticos sofisticados requiere estrategia, información oportuna y vigilancia las 24 horas" (Knerler et al., 2022). Sin embargo, la falta de personal técnico y los recursos limitados en estas instituciones educativas limitan gravemente su capacidad para gestionar y responder de manera eficiente ante incidentes de seguridad (Vielberth et al., 2020). Además, la capacitación en ciberseguridad es deficiente, lo que exacerba la vulnerabilidad ante ataques de ingeniería social como el phishing, una táctica comúnmente utilizada para explotar las debilidades humanas (Garzón Ibarra et al., 2024).

593 Digital Publisher CEIT ISSN 2588-0705

La legislación y su impacto en la ciberseguridad universitaria

En el ámbito legislativo, Ecuador enfrenta desafíos adicionales que complican aún más la implementación de medidas efectivas de ciberseguridad. La falta de una legislación robusta es un problema que deja a las universidades en una situación de vulnerabilidad. Según Delitos Informáticos: Caso Ecuador, "Ecuador no cuenta con una legislación robusta para enfrentar las ciberamenazas" (Ponce Tubay, 2024). Este vacío legal no solo retrasa la adopción de políticas de prevención, sino que también limita las capacidades institucionales para implementar soluciones avanzadas como los SOC.

El potencial de las herramientas de código abierto

Frente a la escasez de recursos financieros y humanos, las herramientas de código abierto han surgido como una solución viable para mejorar la ciberseguridad en las universidades ecuatorianas. Según Herramientas de Ciberseguridad de Código Abierto y su Implementación en PYMES, "estas herramientas ofrecen una alternativa económica y eficiente, siempre y cuando se cuente con personal capacitado" (Pineda et al., 2023). Soluciones como Suricata, una herramienta eficaz para la detección de intrusos y la gestión de tráfico, se han convertido en opciones atractivas para las instituciones con limitaciones presupuestarias (Mario Jesus, 2023).

No obstante, es crucial señalar que la dependencia excesiva en la automatización de estas herramientas puede conllevar riesgos. Automation Bias and Complacency in Security Operation Centers advierte que "la complacencia generada por el uso excesivo de la automatización puede llevar a errores críticos" (Tilbury & Flowerday, 2024). Por lo tanto, se requiere una supervisión adecuada para equilibrar la automatización con la intervención humana, asegurando una protección efectiva.

Colaboraciones internacionales como estrategia de fortalecimiento

En este contexto, las colaboraciones internacionales han demostrado ser una herramienta clave para el fortalecimiento de la ciberseguridad en las universidades. Según Electric Power Systems Research: Best Practices in International Collaborations for Cybersecurity, "las alianzas internacionales permiten compartir conocimientos y mejorar significativamente las defensas cibernéticas" (Ghiasi et al., 2023). La participación de las universidades ecuatorianas en redes globales de ciberseguridad podría facilitar el acceso a mejores prácticas y recursos tecnológicos que de otra manera serían inaccesibles.

Amenazas Emergentes: Ransomware y su Impacto en la Educación Superior

Uno de los riesgos más graves que enfrentan las universidades es el ransomware. Según el ESET Security Report 2024, "el 23% de las organizaciones en América Latina han sido víctimas de ataques de ransomware" (ESET, 2024). Estos ataques, que pueden paralizar sistemas institucionales durante días o semanas, son una clara manifestación de las vulnerabilidades en las redes universitarias.

La gestión eficiente de datos es otro componente clave en la ciberseguridad universitaria. Soluciones como Elasticsearch permiten una administración eficaz de grandes volúmenes de datos, lo que facilita la detección temprana de incidentes de seguridad (Polytseris, 2024). Esto podría ayudar a las universidades a mejorar su capacidad de respuesta ante incidentes cibernéticos.

SOC: Una Solución Integral para Universidades

La implementación de Centros de Operaciones de Seguridad basados en tecnologías de código abierto ha demostrado ser una de las soluciones más eficaces para mitigar los riesgos cibernéticos en instituciones con recursos limitados. Según el estudio Implementación de

un Centro de Operaciones de Seguridad y Redes (NSOC) usando herramientas Open Source para la Infraestructura Industrial de la Empresa Eléctrica Quito, "la adopción de un SOC mejora significativamente la capacidad de respuesta ante incidentes" (Herrera Lara, 2022).

Además, la creación de SOC en los campus universitarios no solo fortalece la seguridad institucional, sino que también brinda a los estudiantes la oportunidad de adquirir experiencia práctica en ciberseguridad. Según SOC It to 'Em: Bringing a Security Operations Center onto a University Campus, "la implementación de un SOC en el campus ofrece una oportunidad para que los estudiantes adquieran habilidades en ciberseguridad mientras refuerzan la infraestructura de la universidad" (Marquardson, 2022).

La Situación en Ecuador y el Rol de EcuCERT

En Ecuador, la creación del Equipo de Respuesta a Emergencias Informáticas (EcuCERT) ha sido un paso crucial para mejorar la ciberseguridad en el país. Según Ecucert. docx, "EcuCERT desempeña un papel clave en la gestión de incidentes y la implementación de estrategias de mitigación ante ciberataques en infraestructuras críticas del país" (Leonardo Rafael, 2020). Durante 2023, el informe de EcuCERT documentó "70,608 direcciones IP comprometidas y 201,627 eventos relacionados con ciberataques" (ECUCERT, 2021). Esto refleja la urgente necesidad de que las universidades refuercen sus defensas cibernéticas.

Método

Este estudio adopta un enfoque mixto, combinando técnicas de investigación cuantitativa y cualitativa para abordar de manera integral la preparación de los institutos universitarios en Ecuador frente a los ciberataques. Esta combinación metodológica permite una visión más completa del problema, integrando la medición objetiva de los datos con un análisis contextual profundo que abarca los desafíos específicos que enfrentan estas instituciones.

Justificación del Enfoque Mixto

El enfoque mixto se justifica en la necesidad de obtener una comprensión más detallada y aplicable del panorama de ciberseguridad en las universidades ecuatorianas. Mientras que el análisis cuantitativo permite medir y evaluar la frecuencia, tipo e impacto de los ciberataques mediante el uso de datos estadísticos provenientes de fuentes como EcuCERT, ESET y Check Point (ECUCERT, 2021)(CHECK POINT, 2024a), el enfoque cualitativo profundiza en las experiencias y desafíos operativos que enfrentan las universidades al implementar medidas de ciberseguridad. Esta integración asegura que no solo se identifiquen patrones estadísticos, sino que también se comprendan las barreras prácticas y las oportunidades de mejora en la implementación de estas medidas (Garzón Ibarra et al., 2024).

El enfoque mixto es esencial, ya que los datos cuantitativos por sí solos no capturarían las complejidades operativas ni los recursos limitados que enfrentan las universidades. Del mismo modo, los hallazgos cualitativos se ven fortalecidos al correlacionarse con datos concretos sobre la frecuencia e impacto de los ciberataques. Esta integración permite formular recomendaciones prácticas y basadas en evidencias.

Enfoque Cuantitativo

El análisis cuantitativo de este estudio se centrará en los datos obtenidos de informes locales y globales de ciberseguridad, como los de EcuCERT, ESET y Check Point, que documentan la frecuencia y el impacto de ciberataques en las instituciones educativas de Ecuador, con un enfoque particular en ataques como ransomware, phishing y malware (ECUCERT, 2021)(CHECK POINT, 2024a). Estos datos serán comparados con las tendencias globales para identificar similitudes y diferencias en la exposición y respuesta ante ciberamenazas entre las universidades ecuatorianas y otras instituciones a nivel internacional (Garzón Ibarra et al., 2024).

593 Digital Publisher CEIT ISSN 2588-0705

Además, se correlacionarán estos datos con los recursos tecnológicos y financieros de las universidades, utilizando análisis estadísticos como la correlación para identificar patrones de vulnerabilidad en instituciones con limitaciones de recursos. Esto permitirá comprender mejor cómo la falta de personal especializado y la infraestructura insuficiente afectan la frecuencia y gravedad de los incidentes cibernéticos. Los resultados cuantitativos proporcionarán una base sólida para las recomendaciones sobre mejores prácticas en la implementación de medidas de ciberseguridad, con un énfasis particular en soluciones económicas y efectivas, como los Centros de Operaciones de Seguridad (SOC) basados en tecnologías de código abierto (Pineda et al., 2023).

Enfoque Cualitativo

El enfoque cualitativo se basa en una revisión exhaustiva de literatura existente y estudios de caso relevantes, priorizando aquellos que exploran la implementación de SOCs en universidades con recursos limitados. Se utilizarán bases de datos académicas como IEEE Xplore, ACM Digital Library y Scopus para seleccionar estudios que aborden las mejores prácticas en ciberseguridad universitaria, como el de Marquardson (2022), que demuestra cómo los SOC mejoran la capacidad de respuesta ante incidentes en instituciones educativas, promoviendo la resiliencia cibernética. Asimismo, el estudio de López-Anchala & Ordóñez-Parra (2024) explora la importancia de las auditorías regulares y su relación con la capacidad de respuesta ante ciberataques.

El análisis cualitativo se llevará a cabo mediante análisis temático, lo que permitirá identificar patrones comunes entre las experiencias de las universidades, como la falta de personal capacitado, la resistencia al cambio tecnológico y la dependencia de soluciones automatizadas sin la supervisión adecuada. La inclusión de estas experiencias complementará los datos cuantitativos, ofreciendo un marco más detallado para la formulación de recomendaciones adaptadas al contexto ecuatoriano.

Integración de Resultados

La integración de los enfoques cuantitativo y cualitativo permitirá generar una visión completa del estado de la ciberseguridad en las universidades ecuatorianas. Los hallazgos cuantitativos proporcionarán una base empírica sólida, mientras que el análisis cualitativo profundizará en las barreras prácticas que enfrentan las instituciones. Esta combinación garantizará que las recomendaciones propuestas sean tanto realistas como basadas en evidencias, con un enfoque particular en soluciones de bajo costo como los SOC de código abierto, que han demostrado ser eficaces en entornos con limitaciones de recursos.

Objetivos del Enfoque

Los objetivos específicos de este enfoque son:

Determinar el nivel de vulnerabilidad de los institutos tecnológicos universitarios frente a ciberataques.

Identificar las principales amenazas y vulnerabilidades que afectan a estas instituciones.

Proponer la implementación de un SOC basado en tecnologías de código abierto.

Desarrollo

Las principales fuentes de datos para este estudio incluyen:

Informes de EcuCERT (2021-2023)

Los datos fundamentales para este estudio fueron obtenidos de las infografías publicadas anualmente por EcuCERT para los años 2021, 2022 y 2023 (ECUCERT, 2021).. Estas infografías están disponibles al público en el sitio web oficial de EcuCERT y ofrecen estadísticas mensuales que detallan los incidentes cibernéticos, el número de direcciones IP afectadas por vulnerabilidades e incidentes, y otros indicadores críticos de ciberseguridad.

Proceso de Extracción de Datos

Se accedió a cada infografía mensual de EcuCERT a través de su portal oficial. Los documentos fueron revisados manualmente para extraer datos clave, incluyendo:

Número de IPs reportadas por vulnerabilidad e incidente.

Principales tipos de incidentes y vulnerabilidades reportados.

Alertas generadas y fraudes detectados.

Los datos recopilados se organizaron meticulosamente en hojas de cálculo de Microsoft Excel por mes y tipo de incidente o vulnerabilidad correspondientes a cada año.

Análisis de Datos

Se utilizó Microsoft Excel para analizar los datos y discernir tendencias y patrones. Se generaron gráficos y tablas para visualizar la evolución de las vulnerabilidades e incidentes a lo largo de los años, basándose en las visualizaciones encontradas en las infografías originales de EcuCERT.

Resultados

Los datos recopilados a través de los informes de EcuCERT, ESET, y Check Point proporcionan un panorama claro sobre la situación de ciberseguridad en las universidades ecuatorianas. Estos resultados revelan una vulnerabilidad significativa frente a diversas amenazas cibernéticas, incluyendo phishing, ransomware, malware, y otras formas de ataques cibernéticos, lo que pone de relieve la necesidad urgente de mejorar la infraestructura y las medidas de seguridad en las instituciones educativas.

Vulnerabilidades en direcciones IP

Las tablas a continuación muestran el número de direcciones IP reportadas con vulnerabilidades y con incidentes cibernéticos durante el período de 2021 a 2023, basado en los datos de EcuCERT.

Tabla 1

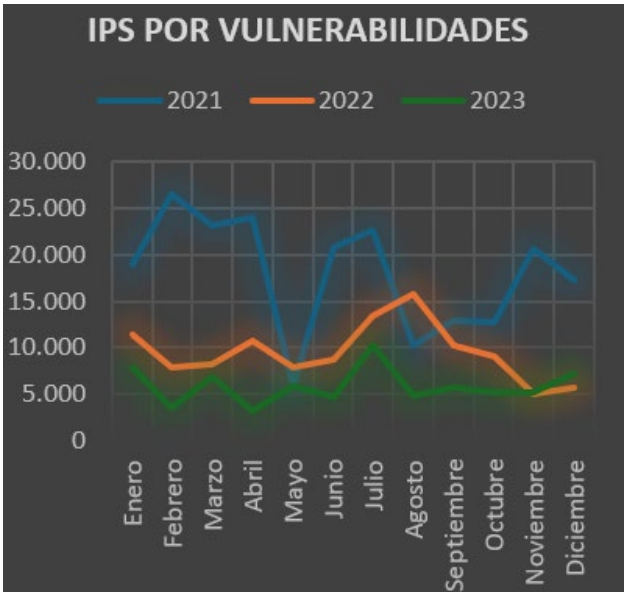
Cantidad de IP reportadas con vulnerabilidades (2021-2023)

IPS POR VULNERABILIDADES			
Mes	2021	2022	2023
Enero	18.897	11.336	7.899
Febrero	26.474	7.844	3.485
Marzo	23.224	8.269	6.853
Abril	23.953	10.796	3.182
Mayo	5.942	7.977	5.886
Junio	20.875	8.731	4.793
Julio	22.721	13.463	10.316
Agosto	10.209	15.781	4.819
Septiembre	12.908	10.188	5.703
Octubre	12.682	9.091	5.146
Noviembre	20.559	4.996	5.217
Diciembre	17.292	5.740	7.309

Nota: Los datos fueron obtenidos de la página oficial de EcuCert (ECUCERT, 2021), accedido 20/09/2024

Figura 1

Cantidad de IP reportadas con vulnerabilidades



Nota: Este gráfico muestra la cantidad mensual de IPs reportadas por vulnerabilidades desde el año 2021 hasta el 2023. Las líneas representan cada año, facilitando la comparación directa de las tendencias a lo largo del tiempo. Los datos fueron tomados de la página oficial de EcuCert (ECUCERT, 2021).

I

593 Digital Publisher
CEIT
ISSN 2588-0705

ncidentes cibernéticos reportados

La siguiente tabla muestra la cantidad de direcciones IP reportadas con incidentes durante el mismo periodo.

Tabla 2

Cantidad de IP reportadas con incidentes

IPS POR INCIDENTES			
Mes	2021	2022	2023
Enero	3.208	19.493	14.810
Febrero	3.001	14.892	7.555
Marzo	2.306	15.847	16.898
Abril	1.754	17.275	11.106
Mayo	316	15.352	12.844
Junio	617	28.917	37.765
Julio	2.618	16.485	26.367
Agosto	1.188	23.663	19.086
Septiembre	1.214	19.785	16.677
Octubre	7.497	15.623	12.489
Noviembre	13.407	11.415	13.972
Diciembre	9.114	9.048	12.058

Nota: Los datos fueron obtenidos de la página oficial de EcuCert (ECUCERT, 2021), accedido 20/09/2024

Figura 2

Cantidad de IP reportadas con incidentes

Nota: Este gráfico muestra la cantidad mensual de IPs reportadas por incidente desde el año 2021 hasta el 2023. Las líneas representan cada año, facilitando la comparación directa de las tendencias a lo largo del tiempo. Los datos fueron tomados de la página oficial de EcuCert (ECUCERT, 2021).

Tipos de incidentes cibernéticos

La siguiente tabla muestra la cantidad de incidentes por tipo registrados en las instituciones ecuatorianas.

Tabla 3

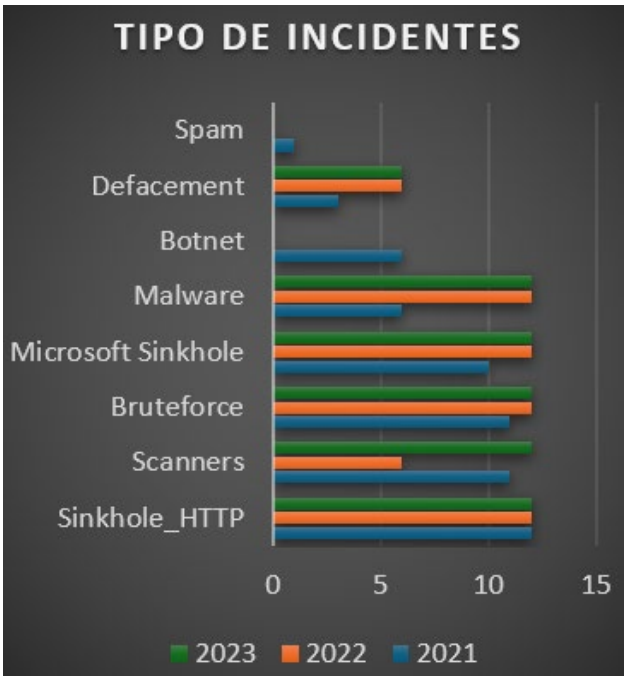
Cantidad de incidentes reportados por tipo

Tipo de Incidente	2021	2022	2023
Sinkhole_HTTP	12	12	12
Scanners	11	6	12
Bruteforce	11	12	12
Microsoft Sinkhole	10	12	12
Malware	6	12	12
Botnet	6	-	-
Defacement	3	6	6
Spam	1	-	-

Nota: Los datos fueron obtenidos de la página oficial de EcuCert (ECUCERT, 2021), accedido 20/09/2024

Figura 3

Cantidad de incidentes reportados por tipo.



Nota: Distribución de la cantidad de incidentes reportados por tipo. Los datos reflejan la frecuencia anual de los tipos de incidentes más

comunes detectados y reportados por EcuCERT durante los años 2021, 2022 y 2023. Cada barra representa el número de incidentes reportados por año para cada categoría de incidente. Los datos fueron extraídos de los informes anuales de (ECUCERT, 2021).

Vulnerabilidades reportadas

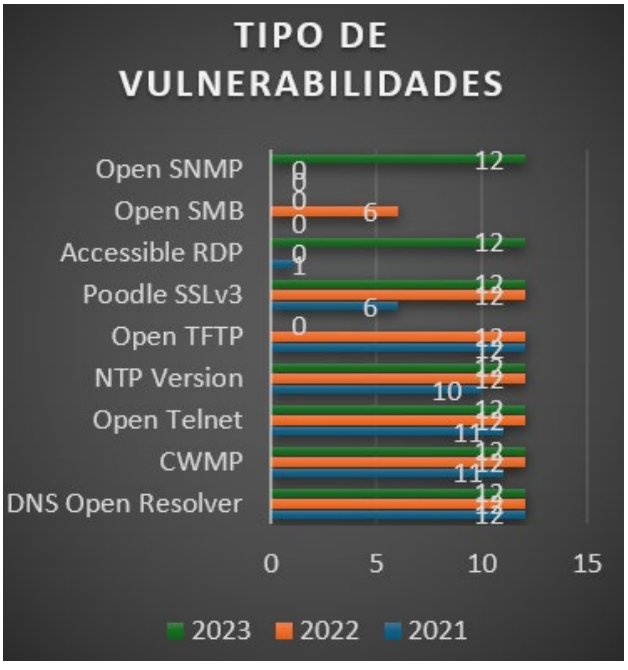
La siguiente tabla muestra los tipos de vulnerabilidades más reportadas en las redes educativas ecuatorianas.

Tabla 4
Cantidad de vulnerabilidades reportados por tipo

Tipo de Vulnerabilidad	2021	2022	2023
DNS Open Resolver	12	12	12
CWMP	11	12	12
Open Telnet	11	12	12
NTP Version	10	12	12
Open TFTP	12	12	-
Poodle SSLv3	6	12	12
Accessible RDP	1	-	12
Open SMB	-	6	-
Open SNMP	-	-	12

Nota: Los datos fueron obtenidos de la página oficial de EcuCert (ECUCERT, 2021), accedido 20/09/2024

Figura 4
Cantidad de incidentes reportados por tipo.



Nota: Distribución de la cantidad de vulnerabilidades reportados por tipo. Los datos reflejan la frecuencia anual de los tipos de incidentes más comunes detectados y reportados por EcuCERT durante los años 2021, 2022 y 2023. Cada barra representa el número de incidentes reportados por año para cada categoría de incidente. Los datos fueron extraídos de los informes anuales de (ECUCERT, 2021).

Análisis de amenazas: Phishing, Ransomware, y Malware

Phishing

Según el informe de ESET, el phishing es la amenaza más prevalente en Ecuador, representando el 35% de todos los incidentes en el país en 2023. Este tipo de ataque afecta gravemente a las instituciones educativas debido a la creciente dependencia de plataformas digitales. Ecuador ocupa la primera posición en América Latina en términos de ataques de phishing. (ESET, 2023).

Figura 5
Tasas de Phishing por País en 2023

Nota: La gráfica ilustra las tasas de detección de phishing en diferentes países de América Latina. Ecuador y Brasil muestran las tasas más altas, lo que indica áreas donde las campañas de concientización y las medidas de seguridad

593 Digital Publisher CEIT ISSN 2588-0705

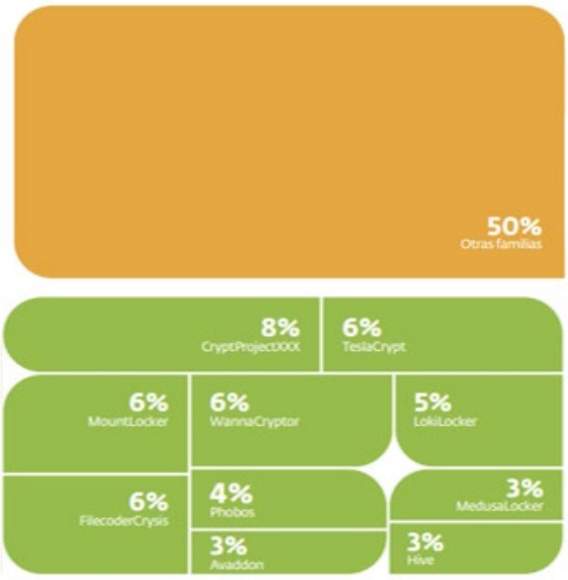
podrían ser particularmente necesarias (ESET, 2023).

Ransomware

El ransomware sigue siendo una de las amenazas más destructivas para las universidades ecuatorianas. Representa el 25% de los ataques reportados y ha visto un aumento del 15% en 2023 en comparación con el año anterior. Las instituciones carecen de medidas adecuadas para mitigar este tipo de ataque, lo que paraliza sus operaciones. (CHECK POINT, 2024a).

Figura 6

Familias ransomware más detectadas | 2023 | LATAM



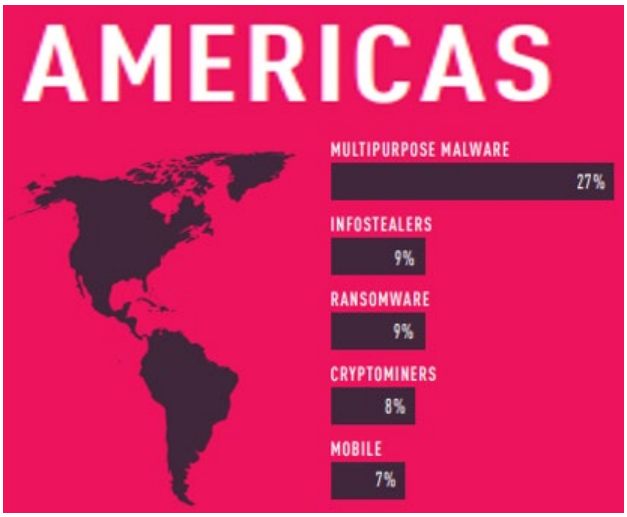
Nota: Esta figura ilustra la proporción de las diferentes familias de ransomware más frecuentemente identificadas en América Latina durante el año 2023 (ESET, 2024).

Malware

El malware representa el 20% de los ataques en las universidades ecuatorianas. Las redes que no cuentan con actualizaciones de seguridad son las más vulnerables. (*Fuente: ESET, 2024*).

Figura 7

Porcentaje de organizaciones afectadas por tipo de malware en las Américas en 2023



Nota: Esta gráfica muestra el porcentaje de organizaciones en las Américas afectadas por diversos tipos de malware en 2023. El malware multipropósito lidera con un 27% de incidencia, seguido por los infostealers con un 9%, igualando los porcentajes de ransomware y criptominers (CHECK POINT, 2024b)

Comparación con Tendencias Globales

Los datos muestran que Ecuador tiene un nivel de exposición superior al promedio global en ataques de phishing y ransomware. Las universidades ecuatorianas enfrentan con mayor frecuencia ataques comunes como el phishing en comparación con otras regiones del mundo, lo que subraya la necesidad de infraestructura de ciberseguridad más robusta.

Interpretación de los Resultados

Los datos muestran una alta vulnerabilidad en las universidades ecuatorianas frente a ciberamenazas. El phishing y el ransomware son los ataques más comunes, lo que indica que se deben implementar medidas inmediatas como la creación de Centros de Operaciones de Seguridad (SOC) y la capacitación en seguridad digital para mitigar estos riesgos.

Conclusiones

El presente estudio ha permitido identificar las principales vulnerabilidades y amenazas que enfrentan las universidades ecuatorianas en el contexto de la ciberseguridad. A partir del análisis cuantitativo de los datos proporcionados por EcuCERT, ESET, y Check Point, se concluye que las instituciones educativas en Ecuador son especialmente vulnerables a ataques de phishing y ransomware, con una incidencia superior al promedio de América Latina.

1. Vulnerabilidad ante el phishing

Los datos revelan que Ecuador ocupa la primera posición en América Latina en cuanto a ataques de phishing dirigidos a universidades. Este tipo de ciberamenazas, que representa el 35% de los incidentes reportados, pone de manifiesto la falta de concienciación y formación en ciberseguridad dentro del entorno educativo. Se hace evidente que la adopción de medidas de concienciación y capacitación sobre los riesgos del phishing debe ser una prioridad para las universidades ecuatorianas.

2. Aumento de los ataques de ransomware

El ransomware representa el 25% de los incidentes cibernéticos en las instituciones educativas del país, lo que subraya la necesidad urgente de implementar mecanismos de defensa más avanzados. Los ataques de ransomware no solo comprometen la integridad de los sistemas, sino que tienen un impacto significativo en la operatividad de las universidades, interrumpiendo sus actividades diarias y poniendo en riesgo la información crítica. La falta de recursos económicos y de personal capacitado ha sido uno de los factores que agravan esta situación, por lo que se recomienda la adopción de SOC basados en tecnologías de código abierto como una alternativa económica y efectiva.

3. Persistencia del malware

El malware, que constituye el 20% de los ataques registrados, sigue siendo una amenaza común en las redes educativas, particularmente en aquellas que no cuentan con actualizaciones de seguridad periódicas. Las universidades ecuatorianas deben fortalecer sus sistemas de seguridad mediante la implementación de políticas de gestión de vulnerabilidades y actualizaciones regulares, así como el uso de herramientas de detección de malware más sofisticadas.

4. Comparación con tendencias globales

El análisis comparativo con datos globales muestra que, aunque las universidades ecuatorianas enfrentan amenazas similares a las de otras regiones del mundo, su frecuencia de ataques comunes como el phishing y ransomware es mucho mayor. Este hecho refleja una infraestructura de ciberseguridad deficiente que requiere mejoras inmediatas. A diferencia de otros países que enfrentan ataques más sofisticados, Ecuador sigue luchando contra amenazas que, con la implementación de medidas básicas de seguridad, podrían mitigarse de manera efectiva.

5. Propuestas de mejora

Dada la alta vulnerabilidad detectada, se recomienda a las universidades ecuatorianas implementar las siguientes acciones:

Creación de SOC basados en código abierto: Este tipo de soluciones permitirían a las universidades monitorizar de manera continua sus redes y responder rápidamente a los incidentes de seguridad. Además, representan una opción económicamente viable para instituciones con recursos limitados.

Capacitación en ciberseguridad: Las universidades deben implementar programas de formación continua para estudiantes y personal académico, con el fin de aumentar la concienciación sobre los riesgos del phishing y otras formas de ataques de ingeniería social.

Mejoras en la infraestructura de seguridad: Es necesario invertir en herramientas y tecnologías de detección y mitigación de amenazas como el malware y el ransomware, así como asegurar la actualización constante de los sistemas.

593 Digital Publisher CEIT ISSN 2588-0705

Colaboración con organismos globales: Las universidades deberían buscar alianzas estratégicas con organismos internacionales de ciberseguridad para compartir conocimientos y acceder a recursos que fortalezcan sus capacidades de defensa.

6. Hacia una ciberseguridad sostenible

En conclusión, la implementación de soluciones adaptadas a las necesidades y limitaciones de las universidades ecuatorianas, junto con una mayor inversión en infraestructura y formación, permitirá a estas instituciones enfrentar de manera más efectiva las crecientes ciberamenazas. La creación de un entorno educativo seguro es crucial no solo para proteger los datos sensibles, sino también para asegurar la continuidad de las operaciones académicas en un mundo cada vez más digitalizado.

Referencias bibliográficas

CHECK POINT. (2024a). *CYBER SECURIT Y REPORT 2024*. https://pages.checkpoint.com/2024-cyber-security-repo

CHECK POINT. (2024b). *Cyber Security Report 2024*. https://pages.checkpoint.com/2024-cyber-security-report

ECUCERT. (2021). *Estadísticas de Seguridad de Redes de Telecomunicaciones*. https://www.ecucert.gob.ec/estadisticas/

ESET. (2023). *Eset Security Report Latinoamerica 2023*. https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

ESET. (2024). *Eset Security Report Latinoamerica 2024*. 31. https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-2024-es.pdf

Garzón Ibarra, C. S., Navas Tapia, C. A., Illicachi Tene, A. M., Espinoza Toapanta, R. J., & Estrella Ormaza, G. S. (2024). Análisis de los Ataques de Ingeniería Social en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(1), 4354–4367. https://doi.org/10.37811/cl_rcm.v8i1.9777

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975. https://doi.org/10.1016/j.epsr.2022.108975

Herrera Lara, L. A. (2022). *IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD Y REDES (NSOC) USANDO HERRAMIENTAS OPEN SOURCE PARA LA INFRAESTRUCTURA INDUSTRIAL DE LA EMPRESA ELÉCTRICA QUITO.* https://bibdigital.epn.edu.ec/handle/15000/22864

Juca-Maldonado, F., & Medina-Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Portal de La Ciencia*, *4*(3), 325–337. https://doi.org/10.51247/pdlc.v4i3.394

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center*. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Leonardo Rafael, C. V. (2020). *Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado*. https://repositorio.uisek.edu.ec/bitstream/123456789/3959/3/Leonardo%20Rafael%20Chuquiguanca%20Vicente.pdf#page=49&zoom=100,92,537

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales. *Revista Multidisciplinaria Perspectivas Investigativas*, *4*(especial), 14–27. https://doi.org/10.62574/rmpi.v4iespecial.154

Mario Jesus, F. C. (2023). *Implementación de una plataforma server utilizando la arquitectura Suricata Open Source para la detección y prevención de intrusos en la red*. https://orcid.org/0000-0001-6377-8328

Marquardson, J. (2022). SOC It to 'Em: Bringing a Security Operations Center onto a University Campus. *Journal of Information Systems Education*, *33*(3), 300–305.

Pineda, M. V., Mauricio, A., & Quiceno, Á. (2023). *Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia*. http://revista.escolme.edu.co/index.php/cies/article/viewFile/479/520

Polytseris, Z. (2024). *Migrating the Linked Data into Elasticsearch*. https://pergamos.lib.uoa.gr/uoa/dl/object/3397216/file.pdf

Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, *1*(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

Shaikh, F. A., & Siponen, M. (2024). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*, *26*(3), 1109–1120. https://doi.org/10.1007/S10796-023-10404-7/TABLES/2

Tilbury, J., & Flowerday, S. (2024). Automation Bias and Complacency in Security Operation Centers. *Computers*, *13*(7), 165. https://doi.org/10.3390/computers13070165

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514