Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

pp. 72 - 88

Un estudio de las afectaciones en las empresas panameñas a causa de los ciberdelincuentes y el uso de ransomware para el robo de información

A study of the effects on Panamanian companies as a result of cybercriminals and the use of ransomware for information theft

Luis Francisco González Jaén[1], Miguel Vargas-Lombardo[2]

[1] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá. luis.gonzales19@utp.ac.pa. https://orcid.org/0009-0008-8915-3308
[2] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, GISES, Panamá. miguel.vargas@utp.ac.pa. https://orcid.org/0000-0002-2074-2939

Recibido: 28 de junio de 2024 Aceptado: 16 de diciembre de 2024

DOI https://doi.org/10.48204/j.colonciencias.v12n1.a6827

Resumen

La investigación tiene como propósito de determinar la realidad con respecto a la tasa de incidencia de los ciberataques en la Panamá en específicamente los ataques de *ransomware* representando un problema creciente dentro del país. Se seleccionaron aleatoriamente 34 empresas para participar en el estudio, asegurando una representación adecuada de distintas regiones y el impacto en el sector comercio. El estudio tiene un enfoque cuantitativo, se aplicó una encuesta como instrumento de recolección de datos a los gerentes de tecnologías de la información y las comunicaciones dentro de las empresas en las provincias de Panamá, Colón y del interior del país. Los resultados permitirán recomendar mejoras en los servicios de seguridad informática en las empresas consultadas.

Palabras clave: Ciberdelito; ciberseguridad; incidente; regulaciones; seguridad de datos; ransomware.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Abstract

The purpose of the research is to determine the reality regarding the incidence rate of cyberattacks in Panama, specifically ransomware attacks representing a growing problem within the country. Thirty-four companies were randomly selected to participate in the study ensuring adequate representation of different regions and the impact on the commercial sector. The study has a quantitative approach, and a survey was applied as a data collection instrument to information and communications technology managers within companies in the provinces of Panama, Colon and the interior of the country. The results will allow us to recommend improvements in computer security services in the companies consulted.

Keywords: Cybercrime; cybersecurity; incident; regulations; data security; ransomware.

Introducción

El ransomware ha emergido como una de las amenazas cibernéticas más significativas y perjudiciales de los últimos años. Su evolución desde su aparición inicial hasta las variantes más avanzadas y sofisticadas de hoy en día ha transformado el panorama de la ciberseguridad, afectando a individuos, empresas y organizaciones en todo el mundo (Olabim et al., 2024).

De acuerdo con dos Santos (2024), el ransomware ha experimentado una evolución notable en términos de complejidad y sofisticación desde sus primeras manifestaciones a principios de la década de 2000. Inicialmente, el ransomware se limitaba principalmente a bloquear la pantalla de la computadora de la víctima o cifrar archivos específicos, exigiendo un rescate para restaurar el acceso. Sin embargo, con el tiempo, los ciberdelincuentes han desarrollado variantes más avanzadas que utilizan técnicas de cifrado más fuertes, tácticas de ingeniería social sofisticadas y explotación de vulnerabilidades de día (Cen, 2024).

La comercialización del ransomware ha sido un impulsor clave de su evolución. Con el surgimiento del ransomware como servicio (RaaS, por las siglas en inglés para *Ransomware as a*

Service), los grupos delictivos organizados pueden alquilar o comprar acceso a kits de ransomware completos, facilitando así la proliferación de este tipo de programa maligno o *malware*. (Moreno et al., 2020; Romero Rubiano, 2023)

El aumento en el uso de las TICs (Tecnologías de las Información y Comunicación) y el propio avance tecnológico ha llevado a un incremento de los ciberataques por ransomware en los últimos años y Panamá no ha sido la excepción. Es cada día más común encontrase con noticias sobre nuevos ataques y nuevas variantes del virus. Es importante conocer la frecuencia con la que ocurren estos ataques y su impacto en las empresas y la sociedad con el fin de implementar medidas efectivas que los contrarresten. En este sentido, se plantean dos interrogantes fundamentales:

- ¿Cuáles ataques de ramsonware afectan a las empresas en Panamá?
- ¿Qué medidas son tomadas los gerentes de tecnologías para mitigar los ciberataques en las empresas en la república de Panamá?

En los últimos años, se han observado varias tendencias preocupantes en el panorama del ramsonware. Además, se ha observado un cambio hacia tácticas de doble extorsión, donde los atacantes amenazan con filtrar datos confidenciales si no se paga el rescate, además de cifrar los archivos de la víctima. Esta táctica aumenta la presión sobre las víctimas y puede tener consecuencias devastadoras en términos de privacidad, reputación y cumplimiento normativo.

El ciberdelito se ha convertido en un problema creciente en Panamá, por ello en esta investigación se abordará el tema los ataques de ramsonware en empresas de ciudad de Colón, Ciudad de Panamá y el interior de país; a medida que la tecnología ha avanzado, también lo ha hecho la sofisticación y la cantidad de delitos cibernéticos que se cometen. Los ciberdelitos como tal no son solo ramsonware que es el punto principal de esta investigación también pueden incluir una amplia gama de actividades ilegales, como el robo de identidad, la extorsión, el fraude, el espionaje cibernético, el ciberacoso y el sabotaje (Latto, 2024).

Estos delitos no solo pueden causar un gran daño financiero a las empresas y a las personas, sino que también pueden afectar la seguridad nacional y la privacidad de los ciudadanos. Aunado a lo anterior, en los últimos años se ha visto un aumento exponencial en el área de los ciberdelitos, siendo el periodo 2020-2021 uno de los más intensos, con un conteo de más de 767 millones de intentos de ciberataque en toda la república de Panamá entre ellos ramsonware (Quirós, 2021).

En 2023, se registraron al menos 8,000 casos de ataques de ransomware e intentos de este en todo Panamá. El país lidera la región en la cantidad de ataques de este tipo sufridos (TVN Panamá, 2024). Desde el sector bancario panameño, se destaca el trabajo realizado para hacer frente a estas amenazas fraudulentas. Según gerentes de ciberseguridad en Panamá, se ha presentado un aumento significativo en los ataques de ransomware que implican el secuestro de información en varias empresas (TVN Panamá, 2024).

En enero del 2021 el Ministerio de Desarrollo Social de Panamá (MIDES) publicó un comunicado explicando que el organismo fue víctima de un ataque de ransomware en donde el mismo inhabilito los servidores y los sistemas de respaldo (*backups)* dificultando todo el proceso de recuperación y continuidad de los sistemas. El equipo de tecnología del MIDES junto a proveedores de seguridad externos procedieron a trabajar en conjunto para recuperar el funcionamiento de los sistemas.

Asimismo, se realizó la denuncia del incidente a la Fiscalía Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática. En palabras del director nacional de Inclusión del Ministerio de Desarrollo Social, Juan Carlos Córdoba, “el Estado panameño no está dispuesto a pagar a los cibercriminales” (Agencias EFE, 2024). En septiembre del 2023 ocurrió uno de los eventos de mayor impacto a nivel de Latinoamérica, que involucró el secuestro digital de información y aplicaciones el proveedor multinacional de servicios de telecomunicaciones IFX Networks, tuvo un impacto significativo en 762 empresas en toda Latinoamérica, incluyendo Panamá.

En Panamá, el Grupo Editora Panamá América, S. A. (EPASA) confirmó que también se vio afectado por este secuestro digital, con sus tres portales no disponibles (Guerrel, 2023). Grupo

TOVA y Grupo Primavera que son empresas que manejan tiendas departamentales también se vieron afectados, dejándolos inoperativos por más de una semana y con fuertes afectaciones a nivel operativo.

El escándalo de los "Panamá Papers" no fue específicamente un ataque de ransomware. Sin embargo, dada la magnitud del evento, este caso ha sido incluido en el listado de los ataques con mayor relevancias y alcance a nivel mundial en 2016, con vinculación de Gobiernos, personajes distinguidos, provocó el inicio de investigaciones judiciales y afectó fuertemente la imagen de Panamá como centro financiero internacional.

Según la Figura 1, el caso de los Panamá Papers es considerada la mayor fuga de información en la historia Se trata de una base de datos de tamaño de 2.6 TB con 11.5 millones de documentos donde, después de su análisis, aparecieron 140 políticos de más de 50 países y compañías offshore en 21 paraísos fiscales (BBC News Mundo, 2016). El sector financiero representa un 7% del producto interno bruto de Panamá por lo que se afectó la confianza hacia el propio país.

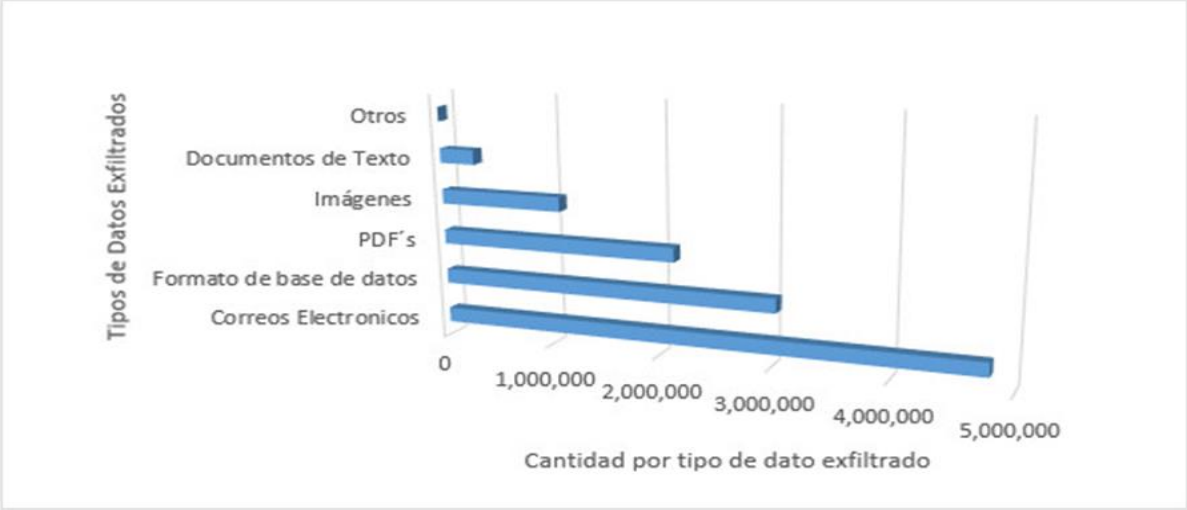
Los delincuentes cibernéticos utilizan técnicas cada vez más sofisticadas para eludir la detección y llevar a cabo sus actividades ilegales. Por otra parte, los Informes de Gestión de la Procuraduría General de la República destacan que los delitos contra la propiedad intelectual y seguridad informática más denunciados fueron los delitos contra el derecho de seguridad informática, delitos contra los derechos de propiedad intelectual (secuestro de información mediante ransomware) y delitos contra el derecho de autor. Estos delitos se encuentran tipificados dentro del Código Penal Acusatorio de la república de Panamá para poder tomar acciones legales contra los ciberdelincuentes (Procuraduría General de la Nación, 2024).

Al comparar las cifras de denuncia de ciberdelitos dadas por la Procuraduría General de la Republica y las cifras de intentos de ciberataques publicados trimestralmente por la empresa FORTINET se pueden apreciar dos realidades distintas, en las que el número de denuncias es mínimo en comparación con la cantidad de ataques que se realizan (FortiGuard Lab., 2024).

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Figura 1.

Panamá Papers: Tipos de delitos exfiltrados



Fuente: Süddeutsche Zeitung, en cooperación con The International Consortium for Investigative Journalists.

Metodología

Se utilizó una metodología de investigación cuantitativa. Se aplicó una encuesta para determinar el impacto del ransomware en diferentes áreas de Panamá cuyo instrumento permitió recopilar datos relevantes y cuantificables directamente de las empresas. El primer paso fue definir claramente el objetivo de la investigación: medir el impacto del ransomware en tres zonas donde existe un gran auge comercial como lo son la ciudad de Panamá, la ciudad de Colón y el interior del país. Seguido, se diseñó una encuesta que implicó la creación de un cuestionario estructurado con preguntas específicas que cubren varios aspectos relevantes del ransomware y la ciberseguridad. Las preguntas fueron formuladas para recopilar información sobre:

- Incidencia de ataques de ransomware
- Preparación y conciencia sobre ciberseguridad

- Medidas de seguridad implementadas
- Frecuencia de copias de seguridad
- Planes de respuesta a incidentes
- Inversión en seguros cibernéticos
- Nivel de capacitación en ciberseguridad

La muestra seleccionada incluyó empresas de diferentes áreas de Panamá, con un enfoque en la Zona Libre de Colón. Se eligieron 34 empresas para participar en la encuesta, asegurando una representación adecuada de distintas regiones y actividades. La encuesta fue distribuida a los participantes a través de medios electrónicos, lo que facilitó una amplia distribución y una rápida recolección de datos. Se utilizó una plataforma de encuestas en línea que permite una fácil administración y recopilación de respuestas. Las respuestas se recopilaron de manera anónima para garantizar la confidencialidad de los participantes y obtener respuestas más sinceras y precisas.

La plataforma de encuestas en línea permitió una recolección eficiente y organizada de los datos. Una vez recopiladas las respuestas, se procedió al análisis de los datos. Esto implicó:

- Tabulación de respuestas: Organizar las respuestas en tablas para una fácil interpretación.
- Visualización de datos: Crear gráficos circulares para representar visualmente los resultados.
- Interpretación de resultados: Analizar los gráficos y tablas para identificar tendencias, patrones y conclusiones relevantes sobre el impacto del ransomware

Resultados

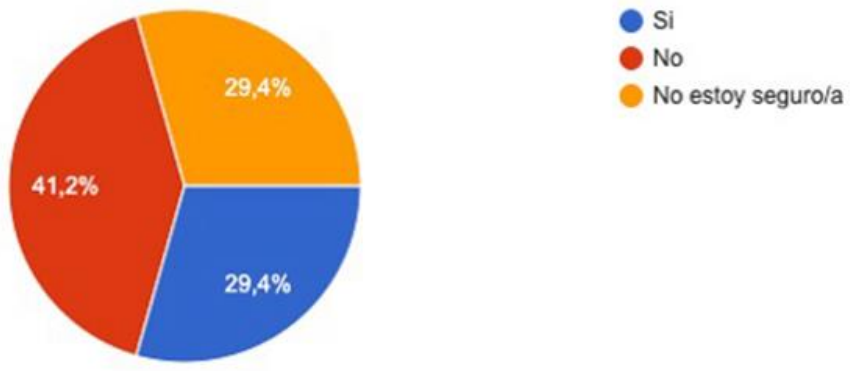
De un total de 34 Gerentes de Tecnologías de la Información y las Comunicaciones encargados de la seguridad de la información de empresas de Colón ubicadas en la Zona Libre de Colón, ciudad de Panamá y el interior de país, y que fueron encuestados, los mismos dieron

respuestas a diversas preguntas. De este total, el 50% trabajan en empresas ubicadas en la ciudad de Panamá (área Centro), 44.1% en Colón y el resto en el interior del país.

La Figura 2 muestra la distribución de empresas que han sido víctimas de un ataque de ransomware durante los últimos 12 meses. Los resultados indican que el 29.4% de las empresas encuestadas han sido víctimas de un ataque de ransomware en el último año, representando una realidad y es amenaza significativa para las organizaciones. Afortunadamente, un 41.2%, la mayor parte de las empresas no ha sido víctima de ransomware en el período mencionado. Por el otro lado, el 29.4% desconoce si han sido atacadas de manera digital. Esto puede indicar una falta de conocimiento o de monitoreo adecuado de seguridad dentro de estas empresas, lo que claramente es una brecha de vulnerabilidad.

Figura 2.

¿Ha sido su empresa víctima de un ataque de ransomware en los últimos 12 meses?



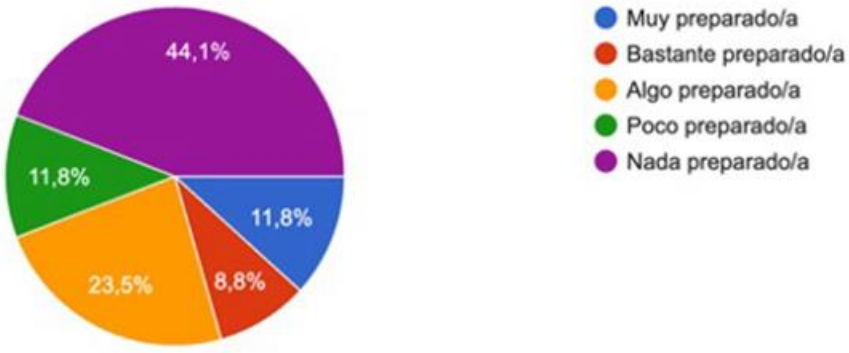
La mayoría de las empresas que reportaron haber sido víctimas de ransomware se encuentran ubicadas en la Zona Libre de Colón. Se infiere que esta zona de comercio internacional puede ser un objetivo atractivo para los atacantes de ransomware por aspectos como la alta

concentración de empresas, importancia económica para Colón y el resto de Panamá, interconexiones empresariales, entre múltiples otros factores.

Con respecto al nivel de preparación de las empresas para enfrentar un ataque de ransomware, la Figura 3 muestra que casi el 55.9% de las empresas encuestadas se encuentra poco y nada preparado, mientras que una minoría de las empresas (11.8%) se considera muy preparada para enfrentar un ataque de ransomware, lo que sugiere que estas empresas probablemente tienen medidas de seguridad robustas y planes de respuesta a incidentes bien definidos. Un porcentaje mayor (23.5%) se siente algo preparado, asumiendo que las empresas poseen buenas prácticas de seguridad, aunque pueden tener áreas que necesiten mejoras. Lo preocupante es que la mayor parte (44.1%) se considera nada preparada, lo que las pone en un alto riesgo de sufrir consecuencias graves en caso de un ataque.

Figura 3.

¿Qué tan preparado/a considera que está su empresa para enfrentar un ataque de ransomware?



En referencia a las medidas de seguridad implementadas por las empresas para prevenir ataques de ransomware, las respuestas fueron múltiples, lo que significa que una empresa podría haber seleccionado más de una opción. El 29.4% de las respuestas indicaron que las empresas utilizan software antivirus o antimalware como medida principal para prevenir ataques de

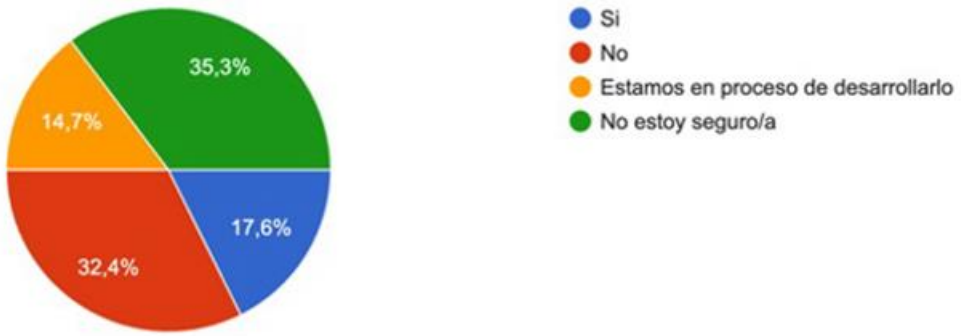
ransomware, mientras que un 5.9% confían en los firewalls como una de sus principales defensas. Un 8.8% de las empresas realizan copias de seguridad regularmente para protegerse contra la pérdida de datos en caso de un ataque, a su vez que un 8.8% señalan invertir en la capacitación de sus empleados para mejorar su conciencia y habilidades en ciberseguridad.

De estos resultados, un pequeño número de empresas (2.9%) utilizan filtros de correo electrónico y spam como medida de seguridad, frente a un 32.4% que no está segura de las medidas de seguridad implementadas en sus empresas, aspecto este delicado. En adición, un 8.8% indican implementar una combinación de todas las medidas mencionadas anteriormente.

Un aspecto fundamental y que fuera preguntado a las empresas es que, si las mismas poseen un plan de respuesta ante incidentes de ciberseguridad, específicamente para ataques de ransomware. La Figura 4 muestra que solo el 17.6% afirman tener un plan de respuesta específico para ataques de ransomware, destacando a las empresas que están proactivamente preparadas para manejar incidentes de ransomware. De manera contraria, un 32.4% no tienen un plan de respuesta ante incidentes de ransomware, lo que indica un serio nivel de desprotección ante cualquier ciber amenaza, no solamente contra ransomware.

Figura 4.

¿Tiene su empresa un plan de respuesta ante incidentes de ciberseguridad, específicamente para ataques de ransomware?



Existe un 14.7% de las empresas está en proceso de desarrollar un plan de respuesta destacando el reconocimiento de la necesidad de preparación y están tomando medidas para mejorar su seguridad, frente un alto porcentaje (35.3%) de los encuestados no está seguro si su empresa tiene un plan de respuesta ante incidentes de ransomware. Esto último sugiere una falta de comunicación interna sobre las políticas de ciberseguridad o la ausencia de un plan formalizado y conocido por los empleados.

La Figura 5 destaca las diferentes acciones que tomarían las empresas en caso de un ataque de ransomware. El instrumento estableció un listado de alternativas para identificar cuáles mecanismos son adoptados. Los resultados muestran que el 32.4% de los encuestados no está seguro sobre qué acciones tomarían sus empresas en caso de un ataque de ransomware. Este alto porcentaje es una clara falta de planificación y comunicación sobre la respuesta a incidentes de ransomware dentro de la empresa. Un 23.5% de las empresas planea restaurar los datos desde copias de seguridad en caso de un ataque. Esto es una medida proactiva y efectiva, siempre y cuando las copias de seguridad sean regulares y seguras. Un pequeño porcentaje de empresas (8.8%) contactaría a las autoridades en caso de un ataque de ransomware, contrario a un número significativo (20.6%) que realizarían consultas con un experto en ciberseguridad, siendo esto una buena práctica para asegurar que se tomen medidas adecuadas para mitigar el ataque y evitar futuros incidentes.

Dentro de las alternativa, el 5.9% de empresas consideraría pagar el rescate, lo cual no garantiza la recuperación de los datos y puede incentivar futuros ataques; por el otro lado, un 2.9% seguiría su Plan de Respuesta a Incidentes (IRP, *Incident Response Plan*) y su Plan de Continuidad del Negocio (*Business Continuity Plan*). Pocas de estas empresas indican disponer de estos planes formalizados y conocidos por los empleados. Finalmente, es preocupante que un 2.9% de los encuestados indiquen desconocer sobre el tema de ransomware, reconociendo su vulnerabilidad ante un ataque.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Figura 5.

En caso de un ataque de ransomware, ¿qué acciones tomaría su empresa?

Con respecto al nivel de capacitación en ciberseguridad que reciben los empleados de las empresas, la Figura 6 muestra que solo el 17.6% de las empresas proporcionan capacitación regular y continua en ciberseguridad a sus empleados, lo cual es una práctica ideal para mantener la concienciación y las habilidades actualizadas, en contraste con el 8.8% ofrecen capacitación en ciberseguridad de forma anual.

Por el otro lado, el 26.5% de las empresas proporcionan capacitación en ciberseguridad de forma ocasional, lo que indica una frecuencia insuficiente para mantener a los empleados preparados frente a amenazas cibernéticas actuales no solo para el ransomware. El mayor riesgo se identifica con la mayoría de las empresas (47.1%) las cuales no proporcionan ninguna capacitación en ciberseguridad a sus empleados.

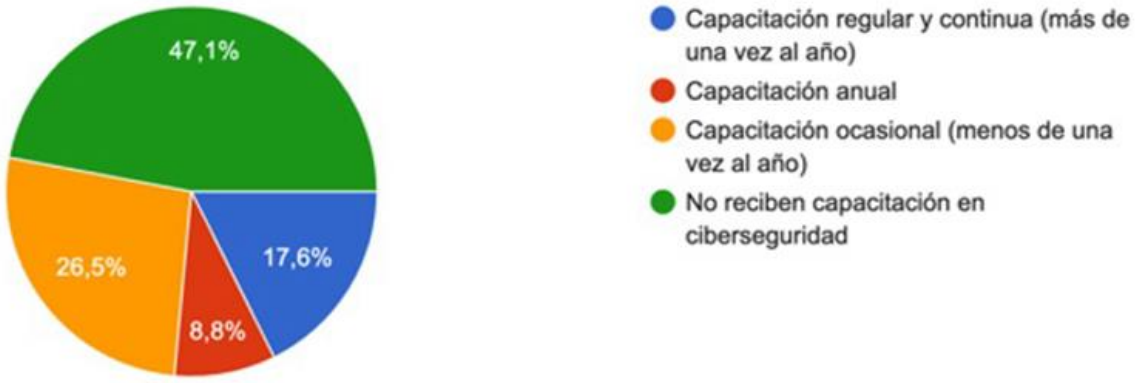
Antes las situaciones de inestabilidad en las infraestructuras tecnológicas del sector público y privado de Panamá, en el año 2011 se creó el CSIRT (*Computer Security Incident Response Team,* por sus siglas en inglés) bajo la estructura gubernamental de la Autoridad Nacional para la Innovación Gubernamental (AIG, 2011), la cual es responsable de identificar y prevenir posibles ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
revistas.up.ac.pa/index.php/revista_colon_ctn
Vol. 12, Nº 1 Enero – Junio 2025

Sin embargo, esta medida no es suficiente ante las constantes y evolucionados ransomware provenientes desde diversas redes informatizadas alrededor del mundo dispuestos a afectar cualquier tipo de empresa.

Figura 6.

¿Qué nivel de capacitación en ciberseguridad reciben los empleados de su empresa?



Los resultados obtenidos de este estudio muestran la necesaria puesta en marcha de planes de contingencia para salvaguardar la integridad de la información en las empresas y sobre todo reforzar la formación académica y profesional en el área de la ciberseguridad en el país. Queda demostrado, que se requiere entrenamiento en el área de ciberseguridad además de una mayor divulgación en el país sobre las amenazas a las cuales están expuestas las empresas panameñas.

Conclusión

El ransomware continúa evolucionando y adaptándose, siendo una amenaza cada vez más sofisticada y frecuente. Los ciberdelincuentes desarrollan nuevas técnicas para evadir las medidas

de seguridad y maximizar el impacto de sus ataques. Este crecimiento constante subraya la importancia de que las empresas no solo implementen medidas de seguridad robustas y planes de respuesta efectivos, sino que también se mantengan informadas y actualizadas sobre las últimas tendencias y tácticas de ransomware. La adaptabilidad y la preparación continua son esenciales para mitigar el impacto de esta amenaza en constante crecimiento. La Zona Libre de Colón ha emergido como una de las áreas más afectadas por el ransomware en Panamá.

Los datos muestran que una proporción significativa de empresas en esta región ha sido víctima de ataques en los últimos 12 meses. Esto destaca la necesidad urgente de abordar las vulnerabilidades específicas de esta zona para mitigar el impacto de futuros incidentes. Un hallazgo recurrente es la falta de preparación y la escasa conciencia sobre las medidas de ciberseguridad entre las empresas encuestadas.

Una gran proporción de empleados no está segura de las medidas implementadas ni de los planes de respuesta a incidentes, lo que indica una grave deficiencia en la comunicación y la capacitación interna. Aunque algunas empresas han adoptado medidas de seguridad básicas como software antivirus y copias de seguridad, muchas otras carecen de una combinación robusta de estrategias de protección. La falta de implementación de medidas avanzadas y la baja frecuencia de copias de seguridad regulares aumentan el riesgo de pérdida de datos críticos. La ausencia de planes de respuesta específicos para ataques de ransomware es una preocupación significativa.

Muchas empresas no han desarrollado ni implementado estrategias formales para manejar estos incidentes, y aquellas que lo han hecho, a menudo no comunican estos planes de manera efectiva a sus empleados. La baja adopción de seguros cibernéticos es otro punto crítico identificado. A pesar del creciente riesgo de ataques de ransomware, la mayoría de las empresas no ha invertido en pólizas de seguro que puedan mitigar las pérdidas financieras derivadas de estos incidentes.

La capacitación en ciberseguridad es inadecuada en la mayoría de las empresas encuestadas. Casi la mitad no proporciona ningún tipo de capacitación, y solo una minoría ofrece formación continua y regular. Esto deja a los empleados mal preparados para reconocer y responder a las

amenazas de ransomware. Implementar estas recomendaciones contribuirá significativamente a mejorar la postura de ciberseguridad de las empresas en Panamá, especialmente en regiones altamente afectadas como Colón. Al fortalecer las medidas preventivas, mejorar la preparación y aumentar la conciencia sobre las amenazas de ransomware, las empresas podrán reducir el riesgo de ataques exitosos y mitigar el impacto potencial en sus operaciones y finanzas.

Conflicto de interés

Los autores declaran no tener algún conflicto de interés para la redacción de este artículo.

Referencias Bibliográficas

Agencias EFE. (2024). *Hackean sistemas de ministerio que otorga ayuda a los más pobres en Panamá*. Última revisión: 31 de enero de 2024. https://www.swissinfo.ch/spa/hackean-sistemas-de-ministerio-que-otorga-ayuda-a-los-m%c3%a1s-pobres-en-panam%c3%a1/46277806

Autoridad Nacional para la Innovación Gubernamental (AIG). (2011). Decreto Ejecutivo No. 709. Proyecto CSIRT. https://aig.gob.pa/csirt/#:~:text=CSIRT%20PANAMA%20(Computer%20Security%20Incident,de%20la%20informaci%C3%B3n%20de%20Panam%C3%A1.

BBC News Mundo. (2016). *Panamá Papers: así se produjo la filtración de documentos confidenciales más grande de la historia*. BBC News. Última revisión: 5 de abril de 2016. https://www.bbc.com/mundo/noticias/2016/04/160405_economia_internacional_tecnologia_panama_papers_filtracion_mossack_fonseca_suddeutsche_informacion_encriptada_

lbhttps://www.bbc.com/mundo/noticias/2016/04/160405_economia_internacional_tecnologia_panama_papers_filtracion_mossack_fonseca_suddeutsche_informacion_encriptada_lb

Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. *Computer Networks*, 239, 110138. https://doi.org/10.1016/j.comnet.2023.110138 .

dos Santos, Z. P. (2024). *Despliegues de los Crímenes Cibernéticos: Una investigación detallada sobre las implicaciones para empresas en Brasil y Uruguay, con enfoque en ataques phishing y ransomware*. AYA Editora.

FortiGuard Labs. (2024). *Overview*. Threat Intelligence Platform | Fortinet. https://www.fortinet.com/fortiguard/labs

Guerrel, I. G. (2023). *Ciberataque masivo golpea a 762 empresas en Latinoamérica, incluyendo Panamá*. La Estrella de Panamá. Última revisión 14 de febrero de 2023. https://www.laestrella.com.pa/vida-y-cultura/tecnologia/ciberataque-masivo-golpea-762-empresas-latinoamerica-incluyendo-panama-LELE498289

Latto, N. (2024). *¿Qué es el ciberdelito y cómo puede prevenirlo? ¿Qué Es el Ciberdelito y Cómo Puede Prevenirlo?* Última revisión: 4 de mayo de 2024. https://www.avast.com/es-es/c-cybercrime#topic-1

Moreno, J., Rodríguez, C. y Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+D Tecnológico*, 16(1), 39-45. https://doi.org/10.33412/idt.v16.1.2438

Olabim, M., Greenfield, A., & Barlow, A. (2024). A Differential Privacy-Based Approach for Mitigating Data Theft in Ransomware Attacks. *Authorea, pre-print*. https://doi.org/10.22541/au.172625434.48862692/v1

Procuraduría General de la Nación. (2024, 8 mayo). *Informe de Procuraduría General de la*

Nación. Última revisión: 8 de mayo de 2024, pp.135. https://ministeriopublico.gob.pa/organizacion/publicaciones/informe-de-gestion

PurpleSec (2023). *2023 Cyber Security Statistics: The ultimate list of stats, data & trends*. Last review: February 22, 2023. https://purplesec.us/resources/cyber-security-statistics/ransomware/

Quirós, J. E. (2021). Panamá, víctima de 767 millones de intentos de ciberataques entre enero y noviembre. Tecnología, TVN Panamá. Última revisión: 1 de enero 2021. https://www.tvn-2.com/entretenimiento/tecnologia/panama-millones-intentos-ciberataques-noviembre_1_1126146.html

Romero Rubiano, J.E. (2023). *Ciberataques: análisis de Ransomware y métodos de protección.* [Trabajo de Fin de Máster – Universitat Oberta de Catalunya]. Repositorio Institucional UOC. https://openaccess.uoc.edu/handle/10609/148181

TVN Panamá. (2024). *Ciberataques: Ataques cibernéticos en Panamá ¿Cuál es su principal objetivo?* Nacionales. Última revisión: 21 de marzo de 2024. https://www.tvn-2.com/nacionales/ciberataques-ciberneticos-expertos-advierten-organizacion-promedio-sufrio_1_2123000.html