AMENAZAS EN LA SOMBRA: EL IMPACTO DE LOS ATAQUES DE CIBERDELINCUENTES EN LA REPÚBLICA DE PANAMÁ

SHADOW THREATS: THE IMPACT OF CYBERCRIMINAL ATTACKS IN THE REPUBLIC OF PANAMA

Cristel Edith Santamaria De Gracia[1]

Resumen

El presente trabajo aborda el Impacto de los ataques de ciberdelincuentes en la República de Panamá, en el cual se destacan varios aspectos claves como, los conceptos que engloban la ciberdelincuencia, también se mencionan el Convenio de Ciberdelincuencia y leyes que rigen estos actos delictivos en Panamá, se detallan los ataques más frecuentes de ciberdelincuentes en Panamá y se concluye proporcionando recomendaciones para contrarrestar la ciberdelincuencia y se destaca la importancia de la educación y la conciencia pública sobre la ciberseguridad, así como la necesidad de implementar medidas de seguridad sólidas en sistemas y redes.

Palabras claves: Amenazas, Ataques, Ciberdelincuentes, Impacto, Panamá.

Abstract

This work addresses the Impact of cybercriminal attacks in the Republic of Panama, in which several key aspects are highlighted, such as the concepts that encompass cybercrime, the Cybercrime Convention and laws that govern these criminal acts in Panama are also mentioned. , details the most frequent attacks by cybercriminals in Panama and concludes by providing recommendations to counter cybercrime and highlights the importance of education and public awareness about cybersecurity, as well as the need to implement solid security measures in systems and networks.

Keywords: Threat, Attacks, Cybercriminals, Impact, Panama.

Introducción

En la actualidad, las Tecnologías de la Información y la Comunicación (TIC) han experimentado un progreso notable, lo que ha traído consigo una serie de ventajas y oportunidades para el crecimiento de las naciones (Ruiz, García, Martínez y Vidal, 2020) y, por ende, de la República de Panamá.

Los ataques cibernéticos se han convertido en una amenaza constante que afecta a gobiernos, empresas y ciudadanos en todo el mundo (Bastidas, Martelo y Fontalvo, 2019; Romero de la Ossa y Buelvas, 2021), y en el país de Panamá no es inmune a la creciente ola de ciberdelincuencia y al impacto de los ataques de ciberdelincuentes que desafían la integridad y seguridad de los sistemas informáticos.

Recepción: 10 de marzo de 2024 / Evaluación: 10 de abril de 2024 / Aprobado: 16 de mayo de 2024

[1] Magister en Tecnología y Sistema de la información Empresarial. Docente en la Universidad Internacional Nueva Luz – Panamá. Email: cristelsantamaria1991@gmail.com

Estos delitos van desde phishing, fraude, la vulneración de la seguridad de la información, suplantación de identidad, intrusiones en redes, estafas, hasta el robo de datos sensibles de personas y empresas y la nación istmeña enfrenta desafíos significativos en el ámbito de la ciberseguridad.

Este artículo reflexivo brinda un aporte académico, ya que se adentra en el fascinante mundo de los ataques de ciberdelincuentes, en el cual conoceremos conceptos que engloban a la ciberdelincuencia, y los ciberdelitos, identificaremos los tipos de actores que son identificados como agentes de amenazas cibernéticas o individuos con intenciones maliciosa, que deliberadamente ocasionan daños a dispositivos o sistemas digitales, explotando vulnerabilidades en sistemas informáticos y comprometiendo la seguridad, además, conoceremos sobre los ataques más frecuentes de ciberdelincuentes en Panamá, también veremos algunas leyes que rigen a la República de Panamá en temas de ciberdelincuencia, a su vez y por último se detallan algunas recomendaciones para evitar los ataques de ciberdelincuentes.

La finalidad de artículo de reflexión es dar a conocer el impacto de los ataques cibernéticos en la República de Panamá y que a medida que el país avanza, continúa su transformación digital y el riesgo de que existan más ataques a la seguridad cibernética.

Este artículo proporcionará una visión en profundidad de un problema que no conoce fronteras y subraya la necesidad de una ciberseguridad sólida y una mayor concienciación sobre las amenazas cibernéticas en el país.

Marco teórico

En este capítulo se desarrollará una caracterización de los ataques de los ciberdelincuentes y el impacto de los mismos en la República de Panamá.

Fundamentos teóricos de los ataques de los ciberdelincuentes

En la actualidad se ha escuchado mucho sobre los ataques de ciberdelincuentes, y que cada año que avanza actores se las ingenian para cometer delitos informáticos.

La palabra ciberdelincuencia viene de ciber- y delincuencia, que significa actividad delictiva que se lleva a cabo a través de internet Real Academia Española [RAE] (sf). Por otro lado, Mateos (2013), define la ciberdelincuencia "como el conjunto de aquellas acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito". Otro concepto ligado a este tema es el delito informático, que para Cordero (2021), es "aquella acción antijurídica realizada mediante dispositivos electrónicos con la finalidad de dañar otros equipos o provocando un daño en sí mismo".

Ante estas conceptualizaciones, se puede inferir que la ciberdelincuencia son los delitos que se cometen por el internet y tecnologías digitales, que vulneran los datos e informaciones de usuarios y empresas aprovechándose de las debilidades de las redes, infraestructuras y sistemas informáticos.

Otros autores hablan de un término reciente en el ámbito de los delitos cibernéticos, que es la cibercriminología. Para (Jaishankar 2007, 2010, 2011 y Jahankhani 2018) como lo menciona Cámara (2020) definen la cibercriminología como:

> El estudio de la causa de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico. En esencia, la cibercriminología implica el examen del comportamiento criminal y la victimización en el ciberespacio desde una perspectiva teórica y criminológica.

En cuanto a Peña (2023), menciona que el termino original de cibercriminalidad se atribuye a:

> Jaishankar, "padre fundador" de la cibercriminología, quien lo considera, con carácter general, un nuevo campo académico; una subdisciplina de la criminología, como una materia multidisciplinar que abarca diversos campos, tales como la criminología, la victimología, la sociología, la ciencia de internet y las ciencias de la computación.

En pocas palabras, la cibercriminología se enfoca en el estudio científico del crimen, la conducta delictiva, los factores que contribuyen a la criminalidad y las respuestas sociales al delito y a pesar de que el término es relativamente nuevo su objetivo principal es comprender por qué las personas cometen delitos y desarrollar estrategias eficaces para prevenir y controlar la delincuencia.

Otro termino muy común es Ciberamenaza, que para Ureña (2015), la define "como aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización y manipulación, control o sustracción." En otras palabras, se refiere a los peligros o riesgos que pueden sufrir los sistemas informáticos, datos digitales redes y redes.

Acuñado a este tema se relacionan otros términos similares como el cyborgcriminology o criminología ciborg, término acuñado por Pérez Suarez (2015), que es un término que combina los campos de la criminología (el estudio del comportamiento delictivo) y la tecnología, específicamente la tecnología de los "cyborgs" o seres cibernéticos.

Leyes que rigen a la República de Panamá en temas de ciberdelincuencia

Señala (Rojas 2016 como citó Godoy, 2020, p. 124).

> El Código Penal de la República de Panamá, aprobado mediante Ley 14 del 18 de mayo de 2007, en su Título VIII, sobre los "delitos contra la Seguridad Jurídica de los Medios Electrónicos" regula los delitos contra la seguridad informática. Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas: a) ingresar o utilizar de bases de datos, red o sistemas informáticos; y, b) apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión. Además, determina ciertas conductas como circunstancias agravantes que aumentan la pena de prisión.

Estos delitos están relacionados con la ciberseguridad y abordan actividades ilegales que afectan la integridad y la seguridad de los sistemas y datos electrónicos.

La Asamblea Nacional de la República de Panamá (2008), contiene la Ley 51 de 22 de julio de 2008, titulada "Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico", establece el marco regulador para la creación, utilización y almacenamiento de documentos electrónicos y firmas electrónicas, así como el proceso de registro y la fiscalización de los prestadores de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas en el territorio de la República de Panamá. Por lo tanto, esta ley panameña también establece penas para aquellos que cometan delitos informáticos, que pueden incluir multas y/o prisión.

Además, la Asamblea Nacional de Panamá (2013), aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013. Y fue publicada en la Gaceta Oficial No. 27403-A del 25 de octubre del mismo año. Cabe decir que, es el convenido

Budapest, que trata de hacerle frente a los delitos informáticos y del internet, este es un convenio internacional que se basa en la armonización de leyes entre naciones.

El convenio sobre la Ciberdelincuencia fue elaborado por el consejo de Europa, sin embargo, se fueron añadiendo otros países como China, Japón, Canadá, además se han previsto adhesiones de otros países no europeos, como México y Costa Rica, incluyendo países latinoamericanos como Panamá.

El Convenio sobre la Ciberdelincuencia de Budapest establece en su preámbulo la importancia de la cooperación internacional en la lucha contra la ciberdelincuencia.

> Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable; (Consejo de Europa, 2001).

Por otro lado, está la Ley 81 de 26 de marzo de 2019, que fue publicada en la Gaceta Oficial No. 28743-A, y entró en vigencia el 29 de marzo de 2021. Es conocida como la Ley de Protección de Datos Personales en Panamá y busca garantizar la privacidad y seguridad de la información personal. Asamblea Nacional de Panamá (2019).

A pesar de que existen leyes en Panamá que penan y multan delitos informáticos, "algunas conductas delictivas que se cometen a través de medios digitales no estén tipificadas como delito, hacen difícil perseguirlas" (Ávila, 2022a). A su vez, en los últimos años los ciberdelitos han aumentado en Panamá y los ciberdelincuentes se están adaptando a nuevas tácticas de delincuencia para cometer sus ilegalidades.

Para Zambrano y Hernández (2020) en el Informe Global de Ciberseguridad califica a la República de Panamá como:

> […] la nación más comprometida de la zona central de América, quedando en el puesto #13 de América y #97 a nivel global. Seguido de Panamá, Guatemala fue calificado con el puesto #16 de la región y #112 global. Costa Rica es el estado #18 de América y el #115 global. Los demás estados centroamericanos quedaron últimos en la lista. (p. 5).

Los ataques más frecuentes de ciberdelincuentes en Panamá

Los delitos informáticos que se cometen a través de medios informáticos son particularidades delictivas, y esta incluye una amplia variedad de categorías de crímenes.

Ciberdelitos en Panamá

Tigo Bussiness (sf), expresa que tal como sucede en el mundo físico, las personas cuidan sus bienes y propiedades porque existen riesgos. Y nadie quiere ser víctima de un robo o de un delito. En Panamá se reportan entre los delitos más frecuentes en la red los siguientes: Estafas, Extorsión, Hurto, Robos, Delitos contra la seguridad informática.

Ministerio Público (2021) En Panamá de enero-abril de 2021, se han registrado 794 denuncias bajo la modalidad del "Ciberdelito", de las cuales 655 corresponden a casos de estafa, representando una incidencia del 68% del total de estafas comunes registradas solo en el área Metropolitana.

Ávila (2022b), menciona que dentro de los ataques de ciberdelincuentes más comunes que se cometen a través de los medios informáticos y que en nuestro país no están tipificados o

regulados dentro del Código Penal, se encuentra el secuestro informático o "ramsomware", suplantación de identidad o "phishing", engaño a menores o "grooming" y hostigamiento o "stalking".

En cuanto a Rodríguez (2022), menciona que “los delitos cibernéticos que más afectan a la población panameña son: la vulneración de la seguridad de la información, el robo de datos, fraude, suplantación de identidad, entre otros”. Esto trae a colación, que los delitos informáticos son un desafío en constante evolución, y las autoridades en Panamá deben adaptarse a las nuevas amenazas cibernéticas a medida que surgen. La educación y la conciencia pública sobre la ciberseguridad son esenciales para protegerse contra los delitos informáticos.

> Panamá no escapa del aumento de los ciberataques (2022), expresa que según estadísticas de la Procuraduría General de la Nación, los casos de delitos informáticos hasta el mes de julio del 2022 han tenido un repunte de 421%, mientras que, en los últimos seis años, la mayor incidencia de ciberdelitos la tuvo el 2021 con 794 denuncias, de esas el 68% fueron estafas, mientras el 2020 cerró con 423 casos de extorsión.

Según el análisis Global de Fraude 2022 de Appgate, realizado por García (2023), explica las cifras significativas nunca antes vistas en delitos cibernéticos y casos de fraude en Panamá. El porcentaje de Phishing mantiene encabezando la lista con un 66%, continua el Trademark 20%, seguido con las aplicaciones móviles maliciosas 6%, luego está la Redirección de Phishing 4% y como último punto está Información Disclosure 4%.

Según la encuesta Global de Seguridad de la Información 2023 de EY (2023), evidencia que las empresas tienen que implementar y reforzar su seguridad. La mayoría de los ataques fue ‘ransomware’ o secuestro de datos en Centroamérica, Panamá y República Dominicana, el riesgo de ataques de ransomware o secuestro de datos en las empresas registró un aumento significativo, con un 60% de las amenazas en 2023.

En el año 2023, la ciberdelincuencia ha estado muy activa en América Latina, a tal modo que el phishing se sextuplicó en la región con el reinicio de la actividad económica y el apoyo de la Inteligencia Artificial. Además, el panorama de amenazas para 2023 de Kaspersky reveló un aumento del 50% en los ataques de troyanos bancarios en la región, lo que equivale a 5 ataques por minuto. En la lista destaca Panamá con un aumento de más de 128% de ataque. Staff Vida Digital (2023).

Ciudad de Panamá-ANPanamá (2024), expresa que la República de Panamá contabilizó 1.7 millones intentos de ataques de phishing en 2023, de los más de 286 millones de intentos en Latinoamérica que sigue siendo una de las regiones más atacadas con mensajes falsos enviados principalmente a través de SMS y WhatsApp.

Protegiendo el Futuro Digital (2024), expone que según el último reporte de amenazas cibernéticas de Check Point, en nuestro país una organización ha sido atacada 1164 veces por semana, en los últimos seis meses. Siendo los sectores de banca y finanzas y el sector gubernamental los blancos principales de los ataques en el país. Por su parte, Estados Unidos, Panamá, Alemania y Canadá son los principales países de origen de dichas amenazas. En los últimos seis meses se dieron 2012 ataques al sector de la banca – finanzas y 737 al gobierno, el cual, se debe reconocen la urgencia de abordar de manera preventiva y oportuna las amenazas de ciberdelincuencia.

En los aportes mencionados destacan la creciente amenaza de los ciberdelitos en Panamá, con una variedad de ataques cibernéticos y un aumento en los casos denunciados y que las autoridades panameñas deben hacer frente a esta problemática.

Recomendaciones para contrarrestar a ciberdelincuencia

Panamá con repunte de delitos contra la ciberseguridad (2022), menciona una manera de combatir los ataques ciberdelincuentes:

> Para contrarrestar los ataques en la red es necesario aplicar la Ciberdefensa, el famoso término utilizado en la actualidad a escala mundial, que busca proteger a las compañías contra el robo de datos, para lo que el profesional en ciberseguridad necesita conocer y explorar las ventajas y debilidades de la empresa para crear un buen plan de defensa. El experto puede defenderse utilizando el sistema "Security Information and Event Management" por sus siglas "SIEM", para analizar en tiempo real alertas y registros, donde su función principal es detectar y neutralizar las amenazas informáticas, evitando posibles ciberataques en la infraestructura tecnológica de la organización.

Desde luego, es evidente que no basta con la regulación; es necesario también proporcionar formación a profesionales y personas que se interesan por la responsabilidad social empresarial, por lo ético y la seguridad informática (Pertuz y Castro, 2021; Pérez, 2020). Es por esta razón que las instituciones académicas, como la Universidad Tecnológica de Panamá (2023) ofrece en un:

> Programa de Licenciatura en Ciberseguridad con título intermedio de Técnico en Ingeniería con especialización en Ciberseguridad, la cual prepara a profesionales para ser líderes en la seguridad, privacidad y protección de datos, análisis de posibles amenazas en los sistemas informáticos y las redes.

Esta licenciatura se centra en garantizar la seguridad, confidencialidad, integridad y la disponibilidad de los datos, así como en prevenir el robo, la duplicación no autorizada y el acceso indebido a la información. En cambio, para Gordon (2021):

> […] la materia Informática, en cualquiera de sus presentaciones en la UP, incluye un apartado de prevención de los ciberdelitos. Aunque sigue siendo sorprendente que no se oferte como materia especializada, o práctica forense, en las carreras relacionadas de la facultad de Derecho y Ciencias Políticas.

Siguiendo en la misma línea de la formación académica sobre el tema de la ciberseguridad, el gobierno nacional de la República de Panamá creo el Equipo Nacional de Seguridad de la Información del Estado Panameño, el CSIRT Panamá. Tal como lo indica la Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (BID-OEA, 2020) el CSIRT "ofrece formación continua en seguridad cibernética para profesionales en los departamentos de tecnología de las instituciones gubernamentales"

Otros puntos importantes para contrarrestar la ciberdelincuencia, según la entrevista con el teniente de SENAFRONT Ricardo Alfonso Sánchez Barreto realizada por López. Roberto (2023), menciona que las personas consideran que para proteger su sistema de ataques de cibernéticos se necesita instalar un antivirus y comprar firewall o cortafuego y que eso va a proteger nuestro sistema por siempre, sin embargo, el teniente expresa que esto es falso, ya que cada día aparecen nuevas amenazas. Otro punto que mencionó el teniente Sánchez, es que se debe crear conciencia a la población, ya que es esencial emplear contraseñas fuertes como medida fundamental para proteger la seguridad de nuestros dispositivos. En ocasiones, recurrimos a contraseñas basadas en datos personales como nuestro nombre y el año de creación. En su lugar, se recomienda el uso de combinaciones de letras mayúsculas y minúsculas, caracteres especiales y números para reforzar la seguridad. También recomienda que se debe actualiza regularmente los dispositivos, debido que las actualizaciones contienen mejoras de seguridad que refuerzan la protección de tus dispositivos. Igualmente, es fundamental instalar un

software de seguridad de confianza para resguardar los dispositivos contra virus, malware y otros programas dañinos, y, por último, se deben realizar respaldos periódicos de los datos importantes y sensibles. De este modo, en caso de infección por un virus o robo de algún dispositivo, se podrá recuperar la información de manera rápida.

Conclusiones

En conclusión, el panorama actual de las Tecnologías de la Información y la Comunicación (TIC) en la República de Panamá es un reflejo de la dualidad inherente en este campo. Mientras que las TIC han brindado numerosas ventajas y oportunidades para el crecimiento nacional, también han expuesto al país a riesgos y amenazas cibernéticas que afectan a múltiples niveles, desde individuos hasta sectores económicos y gubernamentales. Este artículo ha abordado de manera integral el impacto de los ataques de ciberdelincuentes en Panamá, explorando conceptos fundamentales de ciberdelincuencia, la regulación legal en el país, los actores involucrados y los tipos de ataques más frecuentes.

Para enfrentar esta creciente amenaza, es esencial que Panamá se enfoque en la educación y la concienciación pública en torno a la ciberseguridad. Además, se deben implementar medidas de seguridad robustas en sistemas y redes para proteger la integridad de la información y garantizar la continuidad de las operaciones críticas. En un entorno digital en constante evolución, la adaptación y la preparación son esenciales para salvaguardar los intereses del país y sus ciudadanos frente a las amenazas cibernéticas emergentes.

Referencias bibliográficas

ANPanamá. (2022, octubre 26). *Panamá no escapa del aumento de los ciberataques (2022). Agencias de noticias.* 4-11-2023. https://www.anpanama.com/Panama-no-escapa-del-aumento-de-los-ciberataques--13042.note.aspx

ANPanamá. (2024, abril 11). *Ciberdelincuentes intentaron 1.7 millones de ataques en Panamá durante el 2023*. https://www.anpanama.com/Ciberdelincuentes-intentaron-17-millones-de-ataques-en-Panama-durante-el-2023-16355.note.aspx#:~:text=(Ciudad%20de%20Panam%C3%A1%2DANPanam%C3%A1),trav%C3%A9s%20de%20SMS%20y%20WhatsApp

Agredo Satizábal, F. (2019). Impacto de las TIC en la competitividad empresarial soportada por un modelo de educación digital. *Enfoque Disciplinario*, *4*(1), 37-50. Recuperado a partir de http://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/20

Ávila, L. (febrero 13, 2022 a). Ciberdelitos no son bien perseguidos en Panamá. *Panamá América.* 3/11/2023 https://www.panamaamerica.com.pa/judicial/ciberdelitos-no-son-bien-perseguidos-en-panama-1202128

Ávila, L. (febrero 13, 2022 b). Ciberdelitos no son bien perseguidos en Panamá. *Panamá América.* 3/11/2023 https://www.panamaamerica.com.pa/judicial/ciberdelitos-no-son-bien-perseguidos-en-panama-1202128

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. 5/11/2023, https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bastidas Gómez, M., Martelo Gómez, R., & Fontalvo Herrera, T. (2019). Caracterización de smart cities para el fortalecimiento del turismo en la ciudad de Cartagena. *Aglala*, *10*(1), 241–268. https://doi.org/10.22519/22157360.1346 (Original work published 1 de agosto de 2019)

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social, Núm. 60, abril-junio 2020.11-10-2023. https://dialnet.unirioja.es/descarga/articulo/7524987.pdf

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia de Budapest. Preámbulo. 1/11/2023. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

García, L. (2022). Un año de cifras nunca antes vistas en delitos cibernéticos y casos de fraude. La Estrella de Panamá. 8/11/2023. https://www.laestrella.com.pa/cafe-estrella/tecnologia/230518/2022-ano-cifras-vistas

Gordon, G. (2022). Prevención de Delitos Informáticos en los Sistemas Virtuales Educativos en Panamá. Revista Saberes APUDEP, Vol. 5, Núm. 1, enero-junio, 2022, pp. 518-534. Universidad de Panamá. 2/11/2023. https://revistas.up.ac.pa/index.php/saberes_apudep/article/view/2652/2400

Godoy, J. (2020). Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Información Contables Administrativos (SICA). Revista Científica Orbis Cognitiva, Año 4, Vol. 4, Núm. 1 pp. 113-134, enero - junio, 2020. Universidad de Panamá. 3/11/2023. https://revistas.up.ac.pa/index.php/orbis_cognita/article/view/1109/925

La Estrella de Panamá. (2023). *Los ciberataques en la región han crecido más de un 60% en 2023*. 10/7/2024. https://www.laestrella.com.pa/economia/los-ciberataques-en-la-region-han-crecido-mas-de-un-60-en-2023-KA7534158

Ley 51, julio 22, 2008. Asamblea Nacional. Gaceta Oficial de la República de Panamá. 31/10/2023. https://www.gacetaoficial.gob.pa/pdfTemp/26291_A/17859.pdf

Ley 79, octubre 22, 2013. Asamblea Nacional. Gaceta Oficial de la República de Panamá. 31/10/2023. https://www.gacetaoficial.gob.pa/pdfTemp/27403_A/44172.pdf

Ley 81, marzo 26, 2019. Asamblea Nacional. Gaceta Oficial de la República de Panamá. 2/11/2023.https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

López, R. (2023). Los buenos 'ciberhábitos' cierran las puertas a los ataques digitales. La estrella de Panamá. 6/11/2023. https://www.laestrella.com.pa/nacional/230418/buenos-ciberhabitos-cierran-puertas-ataques

Mateos, I. (2013). Ciberdelincuencia Desarrollo y persecución tecnológica. Universidad Politécnica de Madrid. 9/11/2023. https://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

Ministerio Público. (2021, mayo 18). "EL CIBERDELITO ES REAL" MINISTERIO PÚBLICO Y POLICÍA NACIONAL LANZAN CAMPAÑA DE PREVENCIÓN DEL DELITO. 10/7/2024 https://ministeriopublico.gob.pa/notas-de-prensa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/#:~:text=En%20Panam%C3%A1%20de%20enero%2Dabril,solo%20en%20el%20%C3%A1rea%20Metropolitana

Panamá 24 Horas. (2024, enero 18). *Protegiendo el Futuro Digital: Soluciones Seguras aborda las amenazas Cibernéticas del 2024*. 10/7/2024. https://www.panama24horas.com.pa/tecnologia/protegiendo-el-futuro-digital-soluciones-seguras-aborda-las-amenazas-ciberneticas-del-2024/

Panamá con repunte de delitos contra la ciberseguridad (2022). ECO TV. 5/11/2025. https://www.ecotvpanama.com/nacionales/panama-repunte-delitos-contra-la-ciberseguridad-n5728785

Peña, D. (2023). Ciberdelitos y Criminalidad Informática: Rol de la prevención en la expansión de la ciberdelincuencia. Revista Iberoamericana De Derecho Informático (Segunda Época), Núm 13, 2023, pp. 57-72. 11/10/2023. https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/download/3998/3473

Pertuz Leones, L., & Castro Alfaro, A. (2021). La ética empresarial como pilar fundamental de la responsabilidad social. *Enfoque Disciplinario*, *6*(1), 1-9. Recuperado a partir de http://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/23

PÉREZ SUÁREZ, J.R. (2015). We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet. Doctoral thesis, University of Huddersfield.11/4/2024

Real Academia Española. (s.f.). Ciberdelincuencia. En Diccionario de la lengua española. 31/10/2023. https://dle.rae.es/ciberdelincuencia?m=form

Rodríguez, M. (2022). Urgen política pública para una mejor regulación y defensa contra los ciberataques. La Estrella de Panamá. 5/11/2023 https://www.laestrella.com.pa/economia/220624/urgen-politica-publica-mejor-regulacion-defensa-ciberataques

Romero Alvarez, Y., de la Ossa Guerra, S., & Buelvas Parra, J. (2021). Las nuevas competencias del administrador de Empresas en Colombia: Revisión de tema. *Conocimiento Global*, *6*(S1), 165-179. Recuperado a partir de https://conocimientoglobal.org/revista/index.php/cglobal/article/view/138

Ruiz Cabezas, M., García Moreno, A., Martínez Zabaleta, M., & Vidal Tovar, C. (2020). La gestión del conocimiento en las empresas cooperativas. *Conocimiento Global*, *5*(2), 53-69. Recuperado a partir de https://conocimientoglobal.org/revista/index.php/cglobal/article/view/103

Staff Vida Digital. (2023, diciembre 7). *2023: Empresas de Centroamérica de las más afectadas en la región por el Ransomware*.10/7/2024. https://vidadigital.com.pa/2023-empresas-de-centroamerica-de-las-mas-afectadas-en-la-region-por-el-ransomware/

Tigo Business. (s.f.). *Ciberdelitos en Panamá*. 10/7/2024. https://www.tigo.com.pa/empresas/blog/ciberdelitos-en-panama

Universidad Tecnológica de Panamá. (2023.). Oferta académica: Licenciatura en Ciberseguridad. 5/11/2023. https://fisc.utp.ac.pa/licenciatura-en-ciberseguridad

Ureña, F. (2015). "Ciberataques, la mayor amenaza actual". 8-11/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Zambrano, A., & Hernández, L. (2020). Centroamérica cibersegura. Instituto Panamericano de Derecho y Tecnología. 4/11/2023. https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf