Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá

Cleidys Guzmán, David Palacios, Efraín Palacios, Docente: Eliana Acevedo

Facultad de Tecnología, Construcción y Medio Ambiente, Licenciatura en Sistemas de programación, Asignatura: Metodología de la Investigación

cleidysguzmangordon@gmail.com, dapspalacio55@gmail.com, jpalacioefrain0504@gmail.com

DOI: 10.37594/sc.v1i4.1296

Resumen

Esta investigación se realizó con el propósito de determinar la tasa de incidencia de los ciberdelitos en Panamá ya que es un problema creciente dentro del país. Como objetivo general se buscó calcular la incidencia de los ciberdelitos y sus regulaciones en panamá entre 2019-2022. El estudio fue de enfoque cuantitativo, con un diseño no experimental transversal de campo, se aplicó la entrevista como instrumento de recolección de datos al personal docente y especialistas relacionados al área de la ciberseguridad dentro de la provincia de Panamá. La investigación llevó a la conclusión de que, si bien, Panamá es un país que se encuentra en pleno desarrollo y posee regulaciones en cuanto a ciberseguridad, sus políticas para la regulación de los ciberdelitos aún no son del todo efectivas y se requiere seguir trabajando en ellas para lograr disminuir la frecuencia en la que se cometen los mismos cada año.

Palabras clave: ciberdelitos, ciberseguridad, incidentes, regulaciones, seguridad de datos.

Incidences of cybercrime and its regulation in Panama City

Abstract

This investigation was carried out with the purpose of determining the incidence rate of cybercrimes in Panama since it is a growing problem within the country. As a general objective, we sought to calculate the incidence of cybercrime and its regulations in Panama between 2019-2022. The study had a quantitative approach, with a non-experimental cross-sectional field design, the interview was applied as a data collection instrument to the teaching staff and specialists related to the area of cybersecurity within the province of Panama. The investigation led to the conclusion that, although Panama is a country that is in full development and has regulations in terms of ybersecurity, its policies for the regulation of cybercrime are still not fully effective and further work is required on them to reduce the frequency in which they are committed each year.

Keywords: cybercrimes, cybersecurity, incidents, regulations, data security.

1. INTRODUCCIÓN

- **Justificación**

En la actualidad, los avances tecnológicos han transformado la forma en que vivimos, trabajamos e interactuamos. Sin embargo, junto con estos avances también han surgido nuevas formas de delitos conocidos como ciberdelitos, los cuales involucran la manipulación, robo o daño de información en línea.

En Panamá, la creciente amenaza de los ciberdelitos ha llevado a la implementación de medidas y regulaciones por parte de los entes reguladores para proteger a los ciudadanos y las empresas del país dado que la frecuencia con la que ocurren los ciberdelitos parece ser más grande cada día y no existe una entidad que se encargue de medir y hacer publica esta información, es por ello que la investigación tiene como objetivo principal lograr calcular el índice de incidencia de los ciberdelitos en la provincia de Panamá tomando como periodo de tiempo los años 2019-2022 para así determinar cuál es la posibilidad de que ocurra un ciberdelito, sumado a lo anterior, también se pretende clasificar cuáles son los ciberdelitos más comunes en Panamá, como funcionan los distintos entes encargados de estos y cuáles son las políticas existentes relacionadas al tema.

Todo esto permitirá ampliar el conocimiento existente en cuanto a los ciberdelitos en panamá y permitirá así conocer tanto las medidas públicas conocidas como la percepción del usuario que puede llegar a ser víctima.

En esta investigación, se examinará la incidencia de los ciberdelitos en Panamá entre los años 2019-2022, así como las medidas tomadas por las autoridades para combatirlos, incluyendo las regulaciones implementadas por la Autoridad Nacional para la Innovación Gubernamental (AIG) y la Dirección de investigación Judicial (DIJ), además de los artículos del código penal y las distintas Leyes relacionadas.

En las siguientes páginas se abordará con detalle la problemática de los ciberdelitos en Panamá y las regulaciones que existen para combatirlos, planteando el problema existente, las dimensiones relacionadas, las investigaciones previas, y terminando con la aplicación de la metodología, la recolección y análisis de los datos y gráficas para pasar a las conclusiones.

- **Descripción de la temática o problema de investigación**

El ciberdelito se ha convertido en un problema creciente en Panamá, ya que a medida que la tecnología ha avanzado, también lo ha hecho la sofisticación y la cantidad de delitos cibernéticos que se cometen. Los ciberdelitos 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 [1]. 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 Panamá [2], y es que los delincuentes cibernéticos utilizan técnicas cada vez más sofisticadas para eludir la detección y llevar a cabo sus actividades ilegales; por otra parte, según los informes de gestión de la Procuraduría General de la República (PGR), publicados el 1ro de junio de cada año [3], 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 industrial y delitos contra el derecho de autor; todos estos delitos se encuentran tipificados dentro del código penal acusatorio de la República de Panamá, para poder tomar acciones legales contra los ciberdelincuentes, ahora, al comparar las cifras de denuncia de ciberdelitos dadas por la Procuraduría General de la Republica y las cifras de intentos de ciberataques publicadas por la empresa FORTINET cada trimestre [4], 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.

Justamente esto lleva a formular ciertas interrogantes como ¿Cuáles son los entes reguladores en Panamá encargados de los ciberdelitos? o ¿Cuál es el índice de incidencia de los ciberdelitos en Panamá? Preguntas a las que es necesario darles respuesta, sí se quiere tener una visión más clara de Panamá como país que enfrenta este problema creciente.

- **Antecedentes investigativos**

En la actualidad, la era digital ha permitido una gran cantidad de beneficios en cuanto a la comunicación y el intercambio de información en todo el mundo, sin embargo, este avance tecnológico también ha dado lugar a nuevas formas de delincuencia, conocidas como ciberdelitos. Estos delitos incluyen actividades como la piratería informática, el robo de identidad, el acoso cibernético y el fraude en línea, entre otros.

Un primer antecedente corresponde a un artículo titulado *"Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad"* [10], donde se aborda el avance de las ciberamenazas dentro de América Latina, y se establece que las principales amenazas son ataques dirigidos por malware para robar información sensible o confidencial, utilizando técnicas como *"spear-phishing" o "watering hole"* y además el autor nos habla de

cómo los troyanos dirigidos al fraude bancario aumentaron considerablemente, donde el 97% de las entidades financieras recibieron al menos un ataque y de estos, el 37% resultaron exitosos [11]. Por otra parte, hacen un análisis sobre la capacidad de comprensión de los entes reguladores sobre el tema, la debilidad de las regulaciones existentes y la necesidad de modificarlas, así como su grado de impacto en la esfera de la seguridad pública y nacional.

La investigación previamente mencionada demuestra como en América Latina en general existe un gran atraso en cuanto al establecimiento de los ciberdelitos a nivel legal, y aporta una visión del grado de importancia que tiene este dentro de un país; apoya nuestra investigación mostrando cuán necesario es conocer quiénes son las personas encargadas de manejar esta nueva forma de delinquir usando el ciberespacio como herramienta y medio, unido a eso, también muestran cuan es necesario comprender y analizar los procesos tomados por estas mismas para conocer la efectividad de sus acciones, mejorar y prever las situaciones que pueden poner en riesgo al público.

Por otro lado el articulo *"Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad"* [12], es una investigación centrada en las acciones delictivas en el ciberespacio, esta analiza los puntos de vista de diversos autores acerca de la aparición del ciberdelito en temas de terrorismo, generando así el llamado *"ciberterrorismo"*, además intenta explicar el cómo las naciones han reaccionado ante estas situaciones, y realiza toda esta explicación haciendo un recorrido que va desde la conceptualización y análisis del concepto de *"ciberespacio"* y sus amenazas, hasta las consecuencias que este ha provocado en distintas naciones y organizaciones, para terminar mostrando la visión estratégica de defensa de los estados y las líneas de actuación que se utilizan en España y Europa para contrarrestar su efecto destructivo en la sociedad actual.

La investigación citada se vincula con la planteada ya que explica el impacto que puede tener la ciberdelincuencia dentro de un país y como esta es cada vez más común y cambiante, además, plantea uno de los modelos más comunes de prevención de incidentes de seguridad y hace especial énfasis en cómo los estados de gobierno deben mantenerse en constante revisión para lograr prevenir dichos incidentes y, por otro lado, también tener la capacidad de tomar decisiones de seguridad conociendo el estado actual de su ciberespacio.

Por último, en el artículo *"Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios"* [13], sus autores abordan toda el área de los ciberdelitos, conceptualizando cada uno de estos, estableciendo sus riesgos y tipología para así pasar al tema de la impunidad en la administración de justicia sobre los delitos informáticos. Este trabajo de investigación está centrado en delitos que afectan a las empresas, ya sea en su reputación o ingresos y concluye en que cada día

los delitos informáticos van aumentando tanto en tipo como en tamaño y es necesario instaurar un sistema de seguridad tal que permita resguardar la información sensible de las personas sin ningún tipo de riesgo de vulneración.

En este marco teórico, se evidencia la importancia de estudiar la incidencia de los ciberdelitos y la eficacia de las regulaciones implementadas en Panamá, para determinar si estas medidas están siendo efectivas en la prevención y control de los ciberdelitos dentro del país.

- **Formulación de la interrogante**

El aumento en el uso de las tecnologías ha llevado a un incremento de los ciberataques y delitos informáticos en los últimos años y Panamá no ha sido la excepción. Es cada día más común encontrase con noticias sobre distintos delitos cometido usando medios informáticos, Por esta razón, es importante conocer la frecuencia con la que ocurren estos delitos y su impacto en la sociedad, para poder implementar medidas efectivas que los contrarresten. En este sentido, se plantean dos interrogantes fundamentales:

¿Cómo se puede calcular el índice de incidencia de los ciberdelitos en Panamá, ocurridos entre los años 2019 – 2023?

¿Cuáles han sido las medidas tomadas por los entes reguladores para contrarrestar los ciberdelitos en Panamá?

Objetivos

Objetivo General

Calcular la incidencia de los ciberdelitos y sus regulaciones en panamá entre 2019-2022.

Objetivos Específicos

1. Indicar el número de Incidentes de ciberdelitos en panamá entre 2019-2022.
2. Clasificar los tipos de ciberdelitos en panamá entre 2019-2022.
3. Establecer cuáles son los entes reguladores de los ciberdelitos en panamá.

- **Breve desarrollo teórico y conceptual**

El avance tecnológico ha transformado la forma en que interactuamos con el mundo, permitiéndonos realizar diversas actividades de manera más eficiente. Sin embargo, también ha dado lugar a una serie de riesgos asociados con la seguridad informática y los ciberdelitos. En Panamá, estos incidentes no son ajenos a la realidad del país, y es importante comprender el papel de los entes reguladores de ciberdelitos para prevenir, investigar y sancionar estos delitos.

En este capítulo se examinarán los incidentes de seguridad informática y los ciberdelitos en Panamá, así como los entes reguladores encargados de la lucha contra estos delitos. Se explorará la legislación panameña en materia de ciberseguridad y los mecanismos implementados para garantizar la seguridad en línea.

Incidentes de Seguridad

Los incidentes de seguridad se pueden definir como un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información [5].

Es decir, son el conjunto de sucesos posibles que pueden comprometer la integridad de la información que se encuentra resguardada en algún tipo de base de datos y que afectaría tanto al usuario dueño de la información como a la empresa encargada de protegerla.

Ciclo de vida de la gestión de incidentes. La mayoría de los estándares de referencia para la gestión de incidentes describen una serie de etapas a seguir para un manejo adecuado de los mismos, que se resume en una etapa de preparación (pre-incidente), una etapa de detección del incidente, otra etapa en la que se toman las decisiones correspondientes a la contención, erradicación y recuperación ante el incidente, y por último una etapa de actividad post-incidente. [5], a continuación, se describe un poco cada etapa mencionada:

Planificación y preparación: se centra en llevar a cabo todas las acciones necesarias para la preparación ante un incidente de seguridad, esta etapa engloba: plan de gestión de incidentes, procedimientos de actuación, política de seguridad de la información, establecimiento del equipo de respuesta a incidentes de seguridad, concienciación y formación sobre la gestión de incidentes, implantación y mantenimiento de los elementos de monitorización de eventos de seguridad, simulacros del plan de gestión de incidentes, definición de la taxonomía de incidentes de seguridad, plan de intercambio de información y comunicación con terceros y formación permanente del equipo humano.

Detección y reporte: esta fase consta de: recopilación de información, tanto interna como externa a través de los mecanismos establecidos en la etapa anterior, identificar actividad anómala, registrar y notificar el incidente en caso de confirmarse.

Respuesta: se continúa con la investigación del incidente siendo necesario en ocasiones llevar a cabo una recopilación y análisis de evidencias para ampliar la información de la que se dispone,

de forma que las decisiones que se tomen en esta etapa sean las más adecuadas, proporcionadas y ágiles. Esta fase pasa por las siguientes subetapas: contención del incidente, erradicación del incidente y recuperación tras el incidente.

Lecciones aprendidas: esta etapa ayuda a identificar tanto las carencias como los puntos fuertes de las etapas llevadas a cabo, así como pone de manifiesto posibles mejoras en protección y ciberdefensa de la organización; sus objetivos son: identificación de mejoras ante los planes, políticas, procedimientos, etc. Evaluación de la efectividad, agilidad y desempeño del equipo de respuesta ante incidentes, identificación de mejoras ante los sistemas de monitorización y obtención de información.

Cierre del incidente: Actividad post-incidente. El incidente de seguridad no se dará por finalizado hasta haber identificado las lecciones aprendidas y haya un plan para llevarlas a cabo.

Procedimiento de respuestas. Las organizaciones deben disponer de un procedimiento global de gestión de incidentes de seguridad de la información cuyo objetivo sea establecer las directrices generales para la gestión de incidentes de seguridad, con el fin de prevenir y mitigar el impacto de estos, Este procedimiento deberá cubrir al menos los siguientes elementos clave [6]:

- Declaración de compromiso de la gestión.
- Propósito y objetivos del procedimiento. Alcance del procedimiento; a quién y a qué se aplica y bajo qué circunstancias.
- Definir qué se considera incidente de seguridad y sus consecuencias dentro del contexto de la organización.
- Criterios de clasificación para un incidente de seguridad.
- Criterios para evaluar la criticidad de un incidente de seguridad.
- Estructura organizativa y delimitación de roles, responsabilidades y niveles de autoridad.
- En este punto se debería incluir de forma clara la autoridad del equipo de respuesta ante incidentes (por ejemplo, para confiscar equipos, inspeccionar tráfico, descifrarlo o no, etc.).
- Contactos. Deberán estar siempre actualizados y probados (que los números de teléfono sean los correctos, los correos electrónicos adecuados, etc.).

Por consiguiente, se puede apreciar que la gestión general de los incidentes de seguridad es bastante estructurada, y que para poder intentar prever un ataque a nivel mayor y estar realmente preparados para ello, se tienen que realizar una serie de procedimientos y un trabajo en conjunto entre distintas entidades que permita la elaboración de un plan estratégico donde se establezcan todas las posibles medidas a tomar considerando los recursos disponibles.

Los Ciberdelitos

Son delitos convencionales que toman nueva vida con el uso de las tecnologías de la información y la Comunicación y se caracterizan por el uso de redes de transmisión de datos y por su relación con los sistemas informáticos, que pueden afectar a bienes jurídicos diversos de naturaleza individual o supraindividual [7]. Por lo expuesto se puede entender que los ciberdelitos son nuevas formas de cometer crímenes ya existentes, los cuales en una gran cantidad de casos se encuentran ya tipificados dentro del código penal acusatorio o alguna ley equivalente, pero que, dada la evidencia dentro de esta investigación, aún queda mucho camino por recorrer en cuanto al correcto abordaje de los delitos que se realizan con herramientas tecnológicas, ya que se siguen considerando como *"nuevos delitos"*.

Por otro lado, el cibercrimen o los ciberdelitos pueden ser definidos como aquellos delitos que solo pueden ser cometidos usando ordenadores, redes u otras formas de tecnologías de la información y la comunicación (TIC), y por lo tanto exigen una conexión obligatoria a internet; el cibercrimen incluye tales actividades como la creación y propagación de malware, piratería informática usada para robar datos personales o industriales sensibles y ataques de denegación de servicio para causar daño financiero y/o reputacional.

Teniendo claro el concepto de lo que es un ciberdelito, a continuación se explicará cuáles son los delitos que se encuentran relacionados a las nuevas tecnologías y cuáles son los distintos tipos de ciberdelitos.

Delitos Especialmente Relacionados a las nuevas tecnologías. Con la creciente dependencia actual en la vida diaria de las TIC, surgen innumerables vulnerabilidades que abren camino a la ciberdelincuencia, representativa de una amenaza global, técnica, transfronteriza y anónima, y comprensiva de cualquier tipo de actividad ilegal [7]. Gracias al avance tecnológico constante que existe se crean también nuevas vulnerabilidades que ponen en riesgo al usuario que confía en el uso de distintos productos o servicios, y dado que estamos interconectados en una red sin fronteras o limites, donde toda la información viaja de un punto a otro en cuestión de segundos, resulta muy complicado pensar que estamos realmente seguros y que existe una forma sencilla de detener un fenómeno que no para de crecer. Por lo tanto, gracias al crecimiento constante de la inseguridad en la red, muchos usuarios o personas maliciosas hallaron nuevas maneras de cometer diversos actos delictivos, consiguieron nuevos espacios, y ahora estos crímenes pasaron de ser solo físicos a poder llevarse de forma digital.

Descubrimiento de secretos o vulneración de la intimidad por particular. El delito de descubrimiento de secretos o vulneración de la intimidad es un delito de pura actividad, en el que el bien jurídico protegido es la intimidad en sus vertientes negativa como derecho de defensa [7], existen varias formas, estas son:

1. Apoderamiento de papeles, cartas, mensajes de correo electrónico e interceptación de las telecomunicaciones o utilización de artículos técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación
2. Apoderamiento, utilización o modificación sin autorización de datos reservados de carácter personal o familiar que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.
3. Difusión, revelación o cesión a terceros sin autorización de imágenes o grabaciones audiovisuales datos o hechos descubiertos o imágenes captadas obtenidas con anuencia de la persona afectada y en lugar fuera del alcance de terceros.

El intrusismo informático

Consiste en acceder a datos o programas informáticos contenidos en un sistema informático o en parte de este o en mantenerse dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, por cualquier medio o procedimiento[7]. Por tanto, es una práctica ilegal que consiste en realizar actividades relacionadas con la informática o tecnología de la información sin estar debidamente capacitado o tener la autorización necesaria, esto puede poner en riesgo la seguridad de la información y sistemas informáticos, además de afectar la calidad de los servicios que se brindan y puede manifestarse en distintas formas, como: la realización de trabajos de programación, análisis de sistemas, administración de redes y bases de datos, sin tener la formación necesaria o la certificación correspondiente. También puede darse en situaciones en las que se intenta acceder de manera ilegal a sistemas o redes informáticas.

Estafa informática: En el ciberfraude convergen el ciberespacio y el fraude, en el que se hace uso de las tecnologías de la información y la comunicación para lograr un beneficio patrimonial ilícito derivado de un perjuicio patrimonial [5]. Cuando se refiere a la estafa informática o ciberestafa se habla de una forma de fraude que se realiza a través de medios tecnológicos para obtener algún beneficio perjudicando a otros, la ciberestafa hace uso la mayor parte del tiempo de técnicas de ingeniería social como, phishing, bating, pretexting, spamming de contactos, etc.

Entes Reguladores en Panamá

En Panamá, existen varios entes reguladores encargados de combatir los ciberdelitos y proteger la seguridad en línea. Uno de los principales es la Dirección de Investigación Judicial (DIJ), que

forma parte de la Policía Nacional y se encarga de investigar y prevenir delitos informáticos, también está la Autoridad Nacional para la Innovación Gubernamental (AIG), que tiene como objetivo promover la innovación y el uso de tecnologías de la información y comunicación en el sector público, y a su vez, prevenir y combatir los ciberdelitos, otro de los entes creados para atender estos conflictos es el CSIRT Panamá, el cual se encarga de dar respuesta a incidentes de seguridad en Panamá y *"entre sus objetivos están la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá"*.

Estos entes reguladores trabajan de manera coordinada y apoyándose en lo establecido dentro del código penal para garantizar un entorno seguro y confiable en línea para los ciudadanos panameños. A continuación, se podrán observar a detalle las regulaciones antes mencionadas.

Código Penal: Delitos contra la Seguridad Informática. Dentro del código penal en el título VIII, capítulo I de la ley sobre delitos contra la seguridad informática, hace referencia a los artículos 285 donde se establece que *"Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión"* [8]. Art. 286 *"Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión"* [8] y Art. 287 *"Las conductas descritas en los artículos 285 y 286 se agravarán de un tercio a una sexta parte de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de: Oficinas públicas o bajo su tutela, Instituciones públicas, privadas o mixtas que prestan un servicio público, Bancos, aseguradoras y demás instituciones financieras y bursátiles"* [8].

División de Ciberdelito de la Dirección de Investigación Judicial (DIJ). Es una unidad especializada encargada de investigar los delitos informáticos y de alta tecnología. Esta división es responsable de llevar a cabo investigaciones sobre delitos cometidos a través de redes informáticas, como el robo de datos, el acceso no autorizado a sistemas informáticos, el phishing, la suplantación de identidad, el grooming, entre otros.

El aumento en el uso de la tecnología y la interconexión global ha creado nuevas formas de delitos que requieren de una respuesta especializada. La División de Ciberdelitos de la DIJ fue creada en 2010, en respuesta a la creciente necesidad de combatir este tipo de delitos, desde entonces, la unidad se ha especializado en la investigación y persecución de los delitos informáticos y ha

desarrollado técnicas y metodologías específicas para este propósito.

ANTAI: Ley 81 de Protección de Datos Personales. El 29 de marzo de 2021 entró en vigencia la Ley de Protección de Datos Personales en la República de Panamá. Esta Ley tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten datos personales en los términos previstos en esta ley. [9]. Esta ley posee 46 artículos en donde se aborda el nuevo manejo de la información, mostrando, entre algunos que se pueden mencionar:

- Los principios rectores del tratamiento de datos personales, como transparencia, legalidad, finalidad, calidad, proporcionalidad y responsabilidad.
- Los derechos de los titulares de los datos personales, como el derecho de acceso, rectificación, cancelación y oposición, así como el derecho a ser informados sobre el tratamiento de sus datos.
- Las excepciones al consentimiento para el tratamiento de datos personales.
- Las obligaciones de los responsables del tratamiento de datos personales, incluyendo la implementación de medidas de seguridad adecuadas para proteger los datos personales y la obligación de informar a los titulares de los datos sobre el tratamiento de sus datos y sus derechos.
- Las transferencias internacionales de datos personales y su protección.
- La creación de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) y sus competencias en la protección de datos personales.
- Las sanciones por el incumplimiento de la Ley 81, incluyendo multas, cierre temporal o definitivo de la empresa y otras medidas que considere pertinentes la autoridad competente.

La proclamación de esta ley se puede considerar un pequeño avance dentro de todo el camino que queda por recorrer en Panamá para lograr ser un país fuerte y bien estructurado dentro del área de la seguridad informática, la aparición de una ley especial que proteja, establezca protocolos y sancione conductas inapropiadas o directamente delictivas relacionadas con la vulneración de datos personales es de gran aporte a la legislación panameña, ya que, el robo de datos o de información sensible para atacar o extorsionar a la personas y empresas es uno de los ciberdelitos más comunes en el mundo y existe una gran necesidad de crear medidas que permitan contrarrestar de alguna forma toda esta ola creciente de ataques para así poder brindarle seguridad a los usuarios o algún tipo de respaldo.

2. METODOLOGÍA

- **Método y/o Procedimiento metodológico**

En este capítulo se describirá la metodología de investigación aplicada en el estudio de los ciberdelitos y sus regulaciones en Panamá. Se explicará el enfoque, diseño y la técnica de recolección de datos usada para obtener los resultados que se analizarán más adelante dentro de este artículo. En general, este capítulo ofrecerá una visión de la metodología de investigación aplicada dentro de la presente investigación.

Esta investigación se encuentra bajo un enfoque cuantitativo ya que el objetivo general de la misma fue medir el índice con la que es probable que ocurra un ciberdelito en Panamá. Los enfoques cuantitativos son aquellos que *"el objetivo es describir ciertas características de un grupo mediante la aplicación de un cuestionario, el análisis estadístico más elemental radica en la elaboración de una tabla de distribución de frecuencias absolutas y relativas o porcentajes, para luego generar un gráfico a partir de dicha tabla"* [14].

El diseño que se abordó es de tipo no experimental transversal, puesto que es *"aquel en el que el investigador no manipula directamente las variables independientes, sino que observa y mide los fenómenos tal como se presentan en su ambiente natural"* [15], por lo que las variables de estudio no han sido modificadas o alteradas, ya que, dentro de la investigación las variables estudiadas han sido observadas y analizadas, pero no se ha interferido de ninguna forma con las mismas, se busca establecer, una estadístico que permita conocer la incidencia de los ciberdelitos para desde ahí analizar la efectividad de los entes reguladores en su control y prevención de los mismos.

Al mismo tiempo se considera de descriptiva y de campo ya que *"es el proceso que se usa en el método científico, y sirve para la extracción de información y datos de la realidad, usando técnicas de recolección, como las encuestas y entrevistas"* [16].

Como técnica de recolección de se construyó una encuesta, la cual fue aplicada mediante un cuestionario de preguntas cerradas, que permitió medir las variables de estudio. El instrumento consistió en 15 ítems dirigido a docentes y especialistas del área de ciberseguridad, cabe destacar que la encuesta se puede definir como *"una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de sí mismos, o en relación con un tema en particular"* [16], por lo que la misma fue la más apropiada para obtener el tipo de datos necesarios para la investigación, el cuestionario como instrumento de recolección de datos se puede conceptualizar como *"la modalidad de encuesta que se realiza de forma escrita mediante un instrumento o formato en papel contentivo de una serie de preguntas. Se le denomina cuestionario autoadministrado*

porque debe ser llenado por el encuestado, sin intervención del encuestador" [15], tomando como punto la tecnología de la información el cuestionario fue aplicado bajo la aplicación de google forms.

3. RESULTADOS Y DISCUSIÓN

El análisis de la información obtenida de los ciberdelitos en panamá y sus entes reguladores ha permitido lograr el objetivo principal de esta investigación, que es determinar la tasa de incidencia de los ciberdelitos en la provincia de panamá, y esto ha dado como resultado que:

- En el periodo 2019-2020: 29.95 de cada 100,000 habitantes en la provincia de Panamá fueron víctimas de algún tipo de ciberdelito.
- En el periodo 2020-2021: 49.64 de cada 100,000 habitantes en la provincia de Panamá fueron víctimas de algún tipo de ciberdelito.
- En el periodo 2021-2022, 35.76 de cada 100,000 habitantes en la provincia de Panamá fueron víctimas de algún tipo de ciberdelito.

Por otra parte, las encuestas también han mostrado puntos interesantes, como: el motivo principal para cometer un ciberdelito es el Beneficio financiero, así como los principales ciberdelitos en Panamá son: el fraude, la venta y difusión de contenido intimo sin autorización, el phishing, el intrusismo, la extorsión; y la mayoría de los encuestados coinciden en que las políticas creadas por los entes reguladores de la República de Panamá no funcionan correctamente y deben mejorarse además de realizarse capacitaciones constantes a la población.

Finalmente, los resultados concluyeron que los entrevistados coinciden en un mayor porcentaje que el motivo más común por el que se comete un ciberdelito en panamá es el beneficio financiero, esto seguido en partes iguales por motivos personales y hacktivistmo, afirmación que tiene sentido dado que el fraude, estafa y extorsión son unos de los delitos más comunes dentro del país. Así, se pueden establecer que los ciberdelitos más comunes en panamá, según los entrevistados, es la venta, difusión o exhibición de contenido intimo sin autorización, el fraude y los delitos de ciberextorsión, phishing e intrusismo, por lo que es fácil comprender que los delitos más comunes son al acceso sin autorización, engaño y estafa, y los menos probables de ocurrir en Panamá serían el Keylogging y Malware.

En cuanto a las medidas tomadas por los distintos entes reguladores como la creación de nuevas divisiones, leyes y procesos no han resultados realmente eficientes en su tarea de contrarrestar o acabar con todos los ciberdelitos nuevos y los ya existentes, la mayoría de los encuestados, consideraron que existe deficiencia en el manejo de los ciberdelitos por parte de los distintos entes

reguladores encargados y es por ello que a su vez concuerdan en que las medidas tomadas por los entes reguladores han sido ineficientes, por lo que los entrevistados coinciden en que panamá es un país que requiere de mejoras en las regulaciones existentes relacionadas al área de la ciberseguridad o ciberdelitos para poder considerarse como un país seguro.

Los resultados llevan a concluir que los encuestados coinciden en un 100% en que la realización de charlas, seminarios y talleres contribuiría mejorar la problemática de los ciberdelitos en Panamá, así como la implementación de nuevas metodologías para el manejo de los ciberdelitos y la creación de nuevas leyes ayudaría a solventar esta problemática.

4. CONCLUSIONES

Tras la investigación y el análisis de los datos hallados, se puede concluir que los ciberdelitos son un problema existente dentro de la República de Panamá y que específicamente dentro de la provincia de Panamá se cuenta con una tasa de incidencia de ciberdelitos es de:

29.95 por cada 100,000 habitantes en el periodo 2019-2020,
49.64 por cada 100,000 habitantes en el periodo 2020-2021 y
35.76 por cada 100,000 habitantes en el periodo 2021-2022

La investigación ha permitido establecer que los ciberdelitos más comunes en Panamá entre los años 2019-2022, fueron el fraude, la venta y difusión de contenido intimo sin autorización, el phishing, el intrusismo y la extorsión. Cabe destacar que Panamá cuenta con distintos entes reguladores encargados de controlar, prevenir y desarrollar políticas que trabajen en pro a la reducción de los ciberdelitos y la penalización de los mismos, estos organismos son: el Ministerio Publico a través del código penal, contempla la ley sobre delitos contra la seguridad informática; la Dirección de Investigación Judicial (DIJ) en la división de ciberdelito y la Autoridad Nacional para la Transparencia y el Acceso a la Información(ANTAI) con la Ley 81 de Protección de Datos Personales.

Finalmente, con base a lo investigado se muestra la realidad del problema existente en cuanto a seguridad de la información y se ratifica la preocupación de las personas por conocer las medidas de seguridad que están tomando los entes responsables en su área, para controlar este problema de inseguridad creciente que afecta no solo a un país sino al mundo entero, dado que el espacio en que los ciberdelincuentes se desenvuelven es prácticamente infinito y extremadamente cambiante; a modo de conclusión, esta investigación muestra como las políticas de seguridad informática se deben mantener en constante revisión y actualización debido a la naturaleza de los delitos en sí, además que, el factor humano es pieza fundamental para combatir este problema, por lo

que las entidades responsables de la seguridad publica tienen la obligación de estar en constante preparación.

Referencias Bibliográficas

- [1] N. Latto, "¿Qué es el ciberdelito?". 2020. Disponible en: https://www.avast.com/es-es/c-cybercrime#topic-1
- [2] J. Quiroz, "Panamá, víctima de 767 millones de intentos de ciberataques entre enero y noviembre - Tecnología | TVN Panamá," 2020. Disponible en: https://www.tvn-2.com/entretenimiento/tecnologia/panama-millones-intentos-ciberataques-noviembre_1_1126146.html.
- [3] Procuraduría General de la Nación - Ministerio Público De Panamá. "Informe de Gestión. 2023. Disponible en: https://ministeriopublico.gob.pa/organizacion/publicaciones/informe-de-gestion
- [4] Fortinet. "Fortinet Threat Intelligence Insider Latin America". 2020. https://www.fortiguardthreatinsider.com/
- [5] M. Moreno García. "Gestión de incidentes de ciberseguridad, 1". RA-MA Editorial, 2022. [En Línea] Disponible en: https://elibro.net/es/ereader/umecit/222669?page=14
- [6] AIG. "Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica," 2013. Disponible en: https://aig.gob.pa/documentos/?csrt=12077054836007395267
- [7] D. Fernández Bermejo y G. Martínez Atienza, Ciberdelitos. Barcelona: Ediciones Experiencia, 2020. [En Línea] Disponible en: https://elibro.net/es/ereader/umecit/167811?page=28
- [8] Código Penal Acusatorio de Panamá. Título VIII, Cap. I Delitos contra la Seguridad Informática. Artículos 285-286-287, pág. 52-53
- [9] ANTABI. "Ley 81 de Protección de Datos Personales". 2021. https://www.antai.gob.pa/reglamentan-ley-81-de-proteccion-de-datos-personales/
- [10] J.-M. Aguilar, "Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad", Urvio, n.º 25, pp. 24–40, nov. 2019.
- [11] V. Pons Gamon, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity", Urvio, n.º 20, pp. 80–93, jun. 2017.
- [12] J. H. Rojas Parra, "Análisis de la penalización del cibercrimen en países de habla hispana". Rev. Logos cienc. tecnol., vol. 8, n.º 1, pp. 220–231, dic. 2016.
- [13] M. G. Acosta, M. M. Benavides y N. P. García, "Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios.", Revista Venezolana de Gerencia, vol. 25, n.º 89, pp. 351–368, 2020.

- [14] Arias, F. “Proyecto de Investigación”. 6ta ed. Editorial Episteme. Caracas. 2014.
- [15] R. Hernández, C. Fernández y P. Baptista. “Metodología de la Investigación”. https://archive.org/details/hernandezetal.metodologiadelainvestigacion/page/n5/mode/2up: Mc.Graw Hill 2014.
- [16] investigaciondecampo.com. “Qué es la investigación de campo”. 2021. Disponible en https://investigaciondecampo.com/