¿Cómo el ciberdelito afecta a las empresas e instituciones bancarias en Panamá?

Martínez, Yarnelys
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
yarnelysmartinez@gmail.com

Cerezo, Jislaine
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
jislainecerezo@gmail.com

Quirós, Anabelis
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
anabelisq2020@gmail.com

DOI: 10.37594/sc.v1i5.1380

Resumen

El Ciberdelito es un tipo de delito que se comete en el ámbito digital, a través de medios electrónicos, como internet en páginas web. Consiste en actividades ilegales realizadas con el objetivo de obtener información confidencial, causar daño y cometer fraudes; y el impacto que tiene a nivel mundial es significativo. Por ello, en esta investigación se analizó el impacto negativo que tiene el ciberdelito en las empresas, personas e instituciones a nivel general. También se indagó en por qué sucede esto, y cómo se ha visto afectado nuestro país "Panamá" por este delito. Se conoció más sobre los tipos de ciberdelitos que afectan a las instituciones bancarias y empresas en Panamá, y las medidas que se han implementado para prevenir este tipo de delitos. Para la realización de esta investigación se procedió a utilizar varios elementos: Se consultó libros y artículos científicos, además de páginas web. Los hallazgos más relevantes fueron que las consecuencias que tiene el ciberdelito en las empresas son desastrosas; hay pérdidas económicas directas debido al robo de datos financieros, ya que su restablecimiento y recuperación de los sistemas pueden requerir una inversión significativa. Imagine *"La delincuencia informática mundial tiene un costo de 114 mil millones de dólares anuales"*. Así que, podemos ver la importancia de que Panamá implemente medidas de seguridad, haga cambios en el Código Penal y adopte prácticas avanzas de ciberseguridad

para que así de esta manera se pueda enfrentar a la sofisticación de los ciberdelincuentes.

Palabras clave: Ciberdelito, Empresas, Información, Seguridad, Tecnología.

How does Cybercrime affect Companies and Banking Institutions in Panama?

Abstract

Cybercrime, a type of crime that is committed in the digital sphere, through electronic means, such as the Internet on web pages. It consists of illegal activities carried out with the objective of obtaining confidential information, causing damage and committing fraud; and the impact it has worldwide is significant. Therefore, this research analyzed the negative impact that cybercrime has on companies, people and institutions at a general level. We also investigated why this happens, and how our country "Panama" has been affected by this crime. More was learned about the types of cybercrimes that affect banking institutions and companies in Panama, and the measures that have been implemented to prevent this type of crimes. To carry out this research, several elements were used: The "materials and method" method was used, where we consulted books and scientific articles, as well as web pages. The most relevant findings were that the consequences that cybercrime has on companies are disastrous; There are direct economic losses due to the theft of financial data, as its restoration and recovery of systems may require significant investment. Imagine *"Global cybercrime costs $114 billion annually."* So, we can see the importance of Panama implementing security measures, making changes to the Penal Code and adopting advanced cybersecurity practices so that it can confront the sophistication of cybercriminals.

Keywords: Cybercrime, Companies, Information, Security, Technology.

1. INTRODUCCIÓN

- **Justificación**

Hoy en día, los ciberataques se han convertido en una forma de robo muy común debido a los avances en la tecnología y los procesos de internet en las empresas, organizaciones y principalmente bancos, infiltrándose directamente en la seguridad de todo tipo de corporaciones en Panamá y el mundo; y Panamá es uno de los países más vulnerables para los ciberdelincuentes. Es por ello que mediante esta investigación vamos a ver cómo mediante el uso indebido de la tecnología, los delincuentes ciberneticos pueden llevar a las empresas a la ruina e incluso arruinar la vida a las personas. Y ahora más que nunca muchos países y organizaciones de todo el mundo luchan para poner un alto a los delincuentes cibernéticos y contribuir a la seguridad de los sistemas de información.

El aumento del ciberdelito puede poner en riesgo la seguridad de la información personal y financiera de los ciudadanos.

Y como mencionamos, las empresas y las Instituciones bancarias son blancos frecuentes de ciberataques, lo que puede resultar en la pérdida de propiedad intelectual, datos comerciales y financieros. Esto puede tener un impacto negativo en la economía y la competitividad del país. Por ello, un conocimiento más profundo del ciberdelito puede impulsar el desarrollo de capacidades tecnológicas y la implementación de mejores prácticas de seguridad, contribuyendo al crecimiento y la innovación en el sector tecnológico. *"La concientización pública y empresarial es clave para prevenir el ciberdelito".*

Por eso es importante obtener información actualizada de fuentes locales, como organismos gubernamentales de ciberseguridad, fuerzas del orden y organizaciones de seguridad cibernética, para comprender la situación específica en Panamá y las medidas que se están tomando para abordar las amenazas cibernéticas.

Este artículo nos ayudará a conocer más sobre el ciberdelito en Panamá, ya que es fundamental para así poder proteger la seguridad nacional, la privacidad de los ciudadanos, el desarrollo económico y la infraestructura crítica, así como también para fortalecer las capacidades de ciberseguridad y la conciencia pública.

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

En Panamá, según las estadísticas de la Procuraduría General de la Nación, se ha dado un repunte de 421% en los casos de ciberdelitos. Desde el 2016 hasta el presente año la incidencia con más porcentaje ha sido el año pasado con 794 denuncias, de esas el 68% fueron estafas, mientras el 2020 cerró con 423 casos de extorsión. 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.

En otra encuesta realizada por La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODOC) se señala que la victimización individual es considerablemente superior a otras formas de delitos convencionales, además muestra algunos datos o tasas porcentuales de victimización de algunos delitos informáticos (2013):

> Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a una tentativa de *"pesca de datos" o "phishing"*, o sufrir el acceso no autorizado al correo electrónico varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, mientras que las tasas de delitos típicos, como robo, hurto y robo

de coches, son en esos mismos países inferiores al 5%. Las tasas de victimización en el caso de delitos cibernéticos son más altas en los países con menores niveles de desarrollo, lo que indica la necesidad de aumentar las medidas de prevención en esos países (p.3).

Y a medida que las organizaciones adoptan tecnología y almacenan una gran cantidad de datos electrónicos, se vuelven más vulnerables a los ciberdelincuentes, lo que puede tener consecuencias financieras y de reputación negativas. Algunos de los efectos que el ciberdelito tiene son: Las pérdidas económicas directas debido al robo de datos financieros, fraudes o rescates de datos. Además, el restablecimiento de la seguridad y la recuperación de los sistemas pueden requerir una inversión significativa. El ciberdelito también supone la pérdida o robo de propiedad intelectual valiosa, como secretos comerciales, estrategias de negocio o información confidencial. Esto puede afectar la ventaja competitiva de la empresa y disminuir su valor en el mercado.

Interrupción de operaciones: Los ataques cibernéticos pueden causar interrupciones en los sistemas y redes de una empresa, lo que resulta en una paralización de las operaciones. Esto puede provocar pérdida de productividad, tiempo de inactividad y retrasos en la entrega de productos o servicios. Causan daño a la reputación: La divulgación de una brecha de seguridad o el compromiso de datos de los clientes puede dañar la reputación de una empresa. La pérdida de confianza de los clientes y socios comerciales puede tener un impacto duradero en el éxito y la viabilidad de la organización. Sabemos que las organizaciones pueden ser legalmente responsables de garantizar la protección de la información confidencial de sus clientes y cumplir con las regulaciones de protección de datos.

Para mitigar los riesgos asociados con el ciberdelito, las empresas e instituciones bancarias deben implementar medidas de seguridad adecuadas, como el cifrado de datos, la autenticación de múltiples factores y la capacitación en concienciación sobre seguridad para el personal. También es importante contar con planes de respuesta a incidentes cibernéticos para minimizar el impacto en caso de un ataque.

Frente a esto, la abogada especialista en Derecho y Nuevas Tecnologías, Katiuska Hull Hurtado, afirma que en Panamá urge la necesidad de realizar cambios al Código Penal Vigente, para incorporar estos nuevos tipos penales, los cuales cada vez son más comunes, ya que los mismos no están calificados como delitos.

De acuerdo con un informe de la empresa de seguridad Kaspersky elaborado en agosto de 2021, los ataques cibernéticos en Latinoamérica aumentaron un 24% en los primeros meses del

año pasado. Así mismo, el portal de Cyber Economía *"Cyber Magazine"* estimó que para el 2025, las pérdidas causadas por el cibercrimen podrían costar 10,5 billones de dólares a la economía del mundo.

- **Antecedentes investigativos**

La delincuencia informática mundial tiene un costo de 114 mil millones de dólares anuales, y se determinó que más de dos tercios de los adultos en línea (69%) han sido víctimas de la ciberdelincuencia alguna vez en la vida. Cada segundo, 14 adultos son víctimas de un crimen cibernético, lo que deja como resultado más de un millón de víctimas del cibercrimen todos los días. El 10% de los adultos en línea han experimentado la ciberdelincuencia en los teléfonos móviles. El Symantec Internet Security Threat Report revela que en 2010 hubo un 42% más de vulnerabilidades móviles en comparación con la cantidad reportada en 2009. El número de nuevas vulnerabilidades de sistemas operativos móviles aumentó de 115, en 2009, a 163, en 2010. (Esta información es a nivel mundial).

Y nuestro país no escapa de estos problemas, desde hace algunos años los ciberdelitos en Panamá están en aumento. De acuerdo con los datos, durante el 2022, en Panamá se dieron unos 1,415 ataques en los sectores de banca y finanzas, seguido de 1,228 en las entidades del gobierno. Y ahora en el 2023, según datos de la agencia de ciberseguridad de Soluciones Seguras que indica que, durante los últimos seis meses, la banca panameña reportó 1.313 ataques por semana de ciberataques, mientras que el sector de gobierno presentó 803.

Según un informe de la empresa de ciberseguridad, por lo menos en Panamá, en los últimos seis meses, el sector banca y finanzas ha sido los más atacados por los ciberdelincuentes. Agregó que, a nivel global, los bancos sufrieron 1.131 ataques por semana, un aumento del 52% en el último año. Según Reluz, Panamá se ubicó entre los principales países con origen de amenaza junto a Estados Unidos, Ecuador y Rusia.

Para Reluz es crucial que los bancos y los usuarios sepan por qué es importante que estén protegidos y qué hacer cuando están bajo ataques. Por tal motivo, el ingeniero de ciberseguridad de Soluciones Seguras durante el III Congreso Internacional de Ciberseguridad, Prevención de Fraudes y Seguridad Física, tuvo un encuentro, cuyo objetivo es el intercambio de conocimientos, innovaciones y prácticas más avanzadas en el mundo, para así colaborar en la detección, análisis y mitigación de riesgos, y mejorar la seguridad de los recursos e información que los bancos custodian para beneficio de sus clientes.

Por eso, ¿Qué pueden hacer las personas para protegerse de estos ataques cibernéticos?

- Entre otras medidas use antivirus en sus dispositivos, no solo es para el equipo, tenga claro que el virus es el mecanismo que usa el delincuente para acceder a usted y sus pertenencias.
- Por otro lado, desconfíe y confirme la procedencia de correos, llamadas, mensajes incluso a las páginas que accede para hacer transacciones.
- Jamás, comparta sus contraseñas y trate de cambiarlas, actualizarlas con frecuencia. Evite conectarse a redes públicas que no son seguras.
- Otra sugerencia válida es tener a mano la información de contacto de los organismos para denunciar el ciberdelito.
- Si desconoce de ciberseguridad consulte con su proveedor de red para que le indique el tipo de protección que cubre la red de su hogar o negocio.
- Y algo muy sencillo, pero que se olvida, cierre todas las sesiones de sus dispositivos al terminar de utilizarlos.

¿Y …qué protección existe frente a ciberdelitos en Panamá?

Primero, en Panamá se creó en el 2011 el CSIRT (Computer Security Incident Response Team, |siglas en inglés), organismo de la Autoridad Nacional para la Innovación Gubernamental. ¿A qué se dedica? El CSIRT-Panamá se encarga prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país. De tal manera que se alerte a los usuarios a tiempo. Y hace ya algunos años, en marzo 2013, Panamá aprueba la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas que establece acciones para mejorar y brindar protección. Además, fue el segundo país de Latinoamérica que se adhirió y ratificó el Convenio sobre la Ciberdelincuencia llamado Convenio de Budapest, a través de la Ley 79 del 22 de octubre de 2013.

Poco a poco, la legislación se está adaptando a las modalidad de delitos en la red, pero parece que los ciberdelitos permanecerán en el ojo público durante mucho tiempo. Por ello, es mejor estar preparados.

- **Formulación de la interrogante**

¿Cuál es la situación actual del ciberdelito en Panamá y cuáles son las medidas que se están tomando para combatirlo?

- **Objetivo o propósito**

El propósito del estudio fue comprender el impacto negativo que tiene el ciberdelito en las personas, empresas e instituciones bancarias en Panamá y a nivel mundial.

- **Breve desarrollo teórico y conceptual**

Si bien no existe una definición especifica sobre el ciberdelito, desde la década del 70 se crearon distintas acepciones en cuanto al alcance del término. Según el Manual de Recursos de Justicia Criminal del Departamento de Justicia de los Estados Unidos de 1979 se entienden por estas conductas a *"cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución"*. (Shjolberg, Stein - 2018).

Según una definición brindada por la Organización de Cooperación y Desarrollo Económico en 1983, el delito informático o Ciberdelito es *"cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos*9"*. (Estrada Garavilla – 2018).

Para el Consejo de Europa, según una definición de 1995, es *"cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas computacionales o sistemas de procesamiento electrónico de datos"*. (Shjolberg, Stein - 2018).

Para el criminólogo Majid Yar, la ausencia de una definición especifica sobre el fenómeno del cibercrimen se debe fundamentalmente a que *"la delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar"*. (Yar Majid - 2006).

Al analizar estas definiciones según diversos autores, podemos decir que el ciberdelito o delito informático es un acto ilegal realizado por un ciberdelincuente en el espacio digital, dichos actos ilegales atentan la integridad y confidencialidad de los datos; este va en crecimiento y se aprovecha de la vulnerabilidad, la interconexión, y el avance de las tecnologías informaticas. Y además puede tener consecuencias tanto a nivel personal como empresarial.

Pero…¿Cómo afecta el ciberdelito a las personas, la banca e instituciones panameñas ahora que sabemos que es?

Según Mauro Reluz, ingeniero de ciberseguridad de Soluciones Segura comentó que el El phishing y el ransomware se ubicaron como los ciberataques más comunes que sufre actualmente la banca panameña. ¿Cómo afecta cada uno? Reluz explicó que el phishing es un método para engañar a los clientes y hacer que compartan contraseñas, números de tarjeta de crédito, y otra información confidencial, haciéndose pasar por una institución de confianza en un mensaje de

correo electrónico o llamada telefónica. Mientras que los ransomware se usan para capturar y secuestrar información para después pedir rescate por la misma.

También es importante que conozcamos que existen otros tipos de ciberdelitos que afectan a redes y dispositivos informáticos: Entre estos se encuentran:

- El Malware o dispositivo malintencionado: El malware es un término general que se le da a todo aquel software diseñado intencionalmente para perjudicar a la computadora. El malware incluye virus, gusanos, troyanos, spyware, adware, bots y otros software dañinos que pueden usarse para robar información, interrumpir operaciones u obtener acceso no autorizado. La palabra malware proviene del término en inglés malicioso software, y en español es conocido con el nombre de código malicioso.

- El robo de identidad, también es otro ciberdelito muy frecuente: Este delito consiste en el uso no autorizado de la información personal de una persona, como números de seguro social o datos financieros, generalmente para obtener ganancias financieras. Los ciberdelincuentes emplean diversas tácticas, incluido el phishing, el malware y la ingeniería social, para robar y hacer mal uso de información personal para actividades fraudulentas.

- Ataques de denegación de servicio: (Denial of Service, DoS). En seguridad informática, un ataque de denegación de servicio, es un ataque a una red o a un sistema, que causa que un servicio o recurso sea inaccesible. Este tipo de virus ocasiona una pérdida de la conectividad de la red debido a que genera un consumo del ancho de banda de la red ocasionando muchos problemas o la sobrecarga de los recursos del sistema, produciendo que la maquina este ocupada con múltiples procesos y no se pueda realizar los trabajos, en algunos casos muchos usuarios llegan a pensar que la computadora está dañada.

Otro tipos de ciberdelitos son:

- El Ciberacoso:
- Fraude y Suplantación de Identidad:
- Estafas de phishing (como ya mencionamos) y guerras de información.

"Estas son las tendencias que buscan los ciberdelincuentes", advirtió el ingeniero de ciberseguridad de Soluciones Seguras. Todos estos códigos maliciosos pueden ser modificados por ciberdelincuentes y usarlos como un medio para robar dinero y en algunos casos copiar información que tengan derecho de propiedad intelectual tanto a particulares como a empresas.

Y debido a la ausencia de autoridad alguna, que controle y regule el internet, hace que se compliquen aún más los problemas. De ahí que podamos decir que las regulaciones o leyes de las nuevas tecnologías y en especial de internet van a estar siempre en un constante vacío, que será cubierto paulativamente mediante la autorregulación, a no ser que existan normas que establezacan una seguridad jurídica. Y todo esto es debido a que el internet evoluciona, avanza a gran velocidad, se transforma, siempre está en un constante desarrollo y crecimiento.

Y Panamá no escapa de esta realidad; es así como lo menciona el ingeniero Mauro Reluz … *"Panamá dentro de la región representa cierto volumen de ataque porque es uno de los lugares más importantes por la cantidad de información que se maneja a nivel bancario"*, señaló el ingeniero de ciberseguridad.

Frente a esta realidad, Otto Wolfschoon, presidente de la junta directiva de la Asociación Bancaria de Panamá (ABP), comentó que los ciberataques son un tema permanente porque los hackers siempre están inventando nuevos métodos, por eso cree en la necesidad de que el sector bancario esté a la vanguardia para mitigar riesgos. Y Defendió que actualmente *"los bancos panameños cuentan con los equipos para la protección contra ciberdelitos".*

Aunque sabemos que las herramientas descritas y los métodos para enfrentarse a los ciberdelitos que existen no solucionaran todos los problemas que se presenten; a pesar de todo, la influencia entre culturas así como la afluencia e intercambio conjunto de ideas y soluciones puede ser nuestra principal ventaja en la corrección de muchas de las dificultades.

2. METODOLOGÍA

Metodología (Materiales y Método)

2.1. Procedimiento metodológico

Este trabajo se desarrolló de la siguiente manera:

★ Sección I: Introducción

Desarrollar y comprender el concepto de ciberdelito

✯ Se generó el tema de investigación, luego se desarrolló y comprendió el tema del ciberdelito y cómo este afecta a las empresas e instituciones bancarias y a las personas en general en Panamá; todo esto por medio de la recolección de información de noticias y artículos científicos de otros autores, aclarando esto mediante el desarrollo de los siguientes puntos:

✓ Justificación para elaborar dicha investigación

✓ Descripción de la problemática o problema de Investigación

- ✓ Los Antecedentes Investigativos
- ✓ Formulación de la interrogante
- ✓ Se plantearon los objetivos o el propósito del artículo
- ✓ Se formó un breve desarrolló teórico y conceptual
- ★ Sección II: Metodología de la investigación
- ✓ En el Método y/o Procedimiento Metodológico se describieron los pasos y/o la estructura que se siguió.
- ✓ Aspectos éticos
- ★ Sección III: Resultados y Discusión
- ✯ Se hizo una Valoración interpretativa y explicativa desde una perspectiva analítica
- ✓ de los diferentes puntos del desarrollo de la investigación.
- ✓ Sección IV: Conclusiones, gracias al desarrollo de los objetivos se generaron las conclusiones.
- ✓ Bibliografía

Esta investigación se llevó a cabo para la expansión de nuestros conocimientos referente a este tema muy poco tocado en la sociedad, el cuál puede afectarnos en cualquier momento de nuestras vidas sin tomar en cuenta la posición en que nos encontremos, en cuanto a su desarrollo; se empleó un método analítico y razonamiento inductivo a base de investigaciones documentales y páginas de información de ciertas instituciones.

- **Aspectos éticos**

Los aspectos éticos de la investigación fueron resguardados según los principios éticos planteados por el Comité de Bioética de la UMECIT. De manera que este trabajo y su desarrollo se dio a través de la revisión documental donde se respetó los derechos intelectuales de cada una de las afirmaciones teóricas aquí propuestas siendo así congruente con el artículo 4 del capítulo I donde se hace mención que el comité de Bioética de la UMECIT es garante de la ardua tarea de humanizar los procesos de generación de conocimiento científico desde los espacios universitarios de la institución, tomando como base los valores humanos, que incluye el respeto al derecho de autor.

De allí lo importante de una ética que nos responsabilice como sociedad, que esta nos sirva como guía para rescatar los valores y demostrarlos en la utilización de las tecnologías informáticas.

La mayoría de las personas se vuelven cada día más vulnerables al mal uso de las tecnologías por parte de sujetos que cometen actividades ilegales como estafas, suplantación de datos, amenazas o acoso; cuyo único fin es llevar a cabo los llamados delitos informáticos o ciberdelitos.

Según Moor (1985) la ética al momento de manejar la información conlleva valores humanos y sociales; estos son: salud, riqueza, trabajo, libertad, privacidad, seguridad o la realización persona. Estos valores son importantes para dirigir nuestras acciones, y hacer un uso ético de estas tecnologías.

Y según Joyanes (1997) el desarrollo de una ética aplicada al uso de la información es una vía para combatir los delitos informáticos. Una de las tareas más importantes de esta ética informática es plantear la formulación de nuevas normas y leyes que protegen la información privada y los procesos de trabajo, ya que se ameritarán principios morales, éticos o profesionales para las organizaciones de esta sociedad.

3. RESULTADOS Y DISCUSIÓN

En síntesis, la problemática del ciberdelito en Panamá plantea desafíos significativos que afectan no solo a las empresas y entidades financieras, sino también a la seguridad nacional y la privacidad de los ciudadanos. Las estadísticas revelan un aumento alarmante en los casos de ciberdelitos, con consecuencias que van más allá de las pérdidas económicas directas, incluyendo la interrupción de operaciones y la pérdida de propiedad intelectual valiosa.

La respuesta a este desafío requiere una acción coordinada y proactiva, tanto a nivel gubernamental como empresarial. La implementación de medidas de seguridad robustas, como el cifrado de datos y la autenticación de múltiples factores, emerge como una necesidad urgente. La concientización pública y empresarial se presenta como un pilar fundamental en la prevención del ciberdelito, destacando la importancia de la formación y la actualización constante en materia de seguridad digital.

Además, la legislación debe evolucionar para abordar de manera efectiva las nuevas modalidades de delitos en línea, como sugiere la propuesta de cambios al Código Penal Vigente por expertos en el campo legal y tecnológico. La colaboración entre sectores, la participación activa en organismos de ciberseguridad, y la adopción de prácticas avanzadas son esenciales para enfrentar la sofisticación de los ciberdelincuentes.

En última instancia, el análisis de la situación actual del ciberdelito en Panamá no solo subraya la magnitud del problema, sino que también resalta la necesidad imperante de una respuesta integral que involucre a la sociedad en su conjunto. La protección efectiva contra los ciberdelitos no solo garantiza la seguridad financiera y la continuidad de las operaciones comerciales, sino que también preserva la confianza y la integridad de las instituciones y la infraestructura crítica del país. En

conclusión, el párrafo inicial destaca la creciente amenaza de los ciberataques en Panamá y a nivel mundial, señalando la vulnerabilidad del país ante estos delitos. La investigación propuesta busca abordar cómo el mal uso de la tecnología por parte de los ciberdelincuentes puede tener consecuencias devastadoras para empresas, individuos y la seguridad nacional. El aumento de los ciberdelitos, especialmente en el sector financiero y gubernamental, se refleja en estadísticas alarmantes, con un repunte del 421% en casos de ciberdelitos en Panamá. La pérdida económica, la interrupción de operaciones y el daño a la reputación son algunos de los efectos perjudiciales identificados. La concienciación pública y empresarial se presenta como una clave para prevenir el ciberdelito. Además, se destaca la importancia de obtener información actualizada de fuentes confiables y la necesidad de implementar medidas de seguridad adecuadas. En este contexto, la legislación actual en Panamá se está adaptando gradualmente a las modalidades de delitos en línea, pero la persistencia de los ciberdelitos sugiere la importancia de estar preparados para enfrentar esta creciente amenaza.

4. CONCLUSIONES

Luego de realizada la investigación pudimos cumplir los obejtivos que se tenían planeado desarrollar en el principio del artículo:

- Desarrollamos y comprendimos el impacto que tiene el ciberdelito en las empresas, la tecnología y las instituciones bancarias; ya que a medida que las organizaciones adoptan tecnología y almacenan una gran cantidad de datos electrónicos, se vuelven más vulnerables a los ciberdelincuentes, y esto trae consecuencias financieras y de reputación negativas a la empresa o institución. Algunos de los efectos son: Las pérdidas económicas directas debido al robo de datos financieros, fraudes o rescates de datos. El ciberdelito también supone la pérdida o robo de propiedad intelectual valiosa, como secretos comerciales, estrategias de negocio o información confidencial. Vimos que los ataques cibernéticos también pueden irrumpir en los sistemas y redes de una empresa, lo que resulta en una paralización de las operaciones. Esto puede provocar pérdida de productividad. También causan daño a la reputación de la empresa y esto trae como consecuencia muchas veces la pérdida de confianza de los clientes y socios comerciales.
- Analizamos la situación actual del ciberdelito en Panamá, y es que de acuerdo a los datos, desde hace algunos años el ciberdelito va en aumento en la República de Panamá; segun las Estadisticas de la Procuraduría General de la Nación la República de Panamá reportó un aumento en denuncias por el delito contra la seguridad informática y medios tecnológicos. Desde el 2016 se dió un repunte de 421% en los casos de ciberdelitos. Y desde el 2016 hasta el 2022 la incidencia con más porcentaje fue el año 2021 con 794 denuncias. Mintras que el 2020 cerró con más de 423 casos de extorsión. (Ministerio Público de Panamá, 2021). Y

de acuerdo con los datos, durante el 2022, en Panamá se dieron unos 1,415 ataques en los sectores de banca y finanzas, seguido de 1,228 en las entidades del gobierno. Y ahora en el 2023, según datos de la agencia de ciberseguridad de Soluciones Seguras que indica que, durante los últimos seis meses, la banca panameña reportó 1.313 ataques por semana de ciberataques, mientras que el sector de gobierno presentó 803.

- Conocimos los Ciberdelitos qué más afectan a las empresas e Instituciones bancarias en Panamá; Y es así ya que, según Mauro Reluz, ingeniero de ciberseguridad de Soluciones Seguras. El phishing y el ransomware se ubicaron como los ciberataques más comunes que sufre actualmente la banca panameña. También conocimos otros tipos de ciberdelitos que afectan a redes y dispositivos informáticos: Entre estos se encuentran:

- El Malware o dispositivo malintencionado: término general que se le da a todo aquel software diseñado intencionalmente para perjudicar a la computadora.
- El robo de identidad, los ataques de denegación de servicio, el ciberacoso, el fraude y la suplantación de identidad entre otros más.

"Estas son las tendencias que buscan los ciberdelincuentes" como un medio para robar dinero y en algunos casos copiar información que tengan derecho de propiedad intelectual tanto a particulares como a empresas.

- Y presentamos las medidas que se están implementando en Panamá para prevenir y combatir este tipo de delitos. Primero, Panamá creó en el 2011 el CSIRT (Computer Security Incident Response Team, |siglas en inglés), organismo de la Autoridad Nacional para la Innovación Gubernamental. Este se encarga de prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país. De tal manera que se alerte a los usuarios a tiempo. Además, fue el segundo país de Latinoamérica que se adhirió y ratificó el Convenio sobre la Ciberdelincuencia llamado Convenio de Budapest, a través de la Ley 79 del 22 de octubre de 2013. También vimos algunas medidas que pueden tomar las personas para evitar caer en estos robos. Entre otras medidas usar antivirus en los dispositivos, también desconfiar y confirmar la procedencia de correos, llamadas, mensajes incluso a las páginas que se accede para hacer transacciones, jamás compartir las contraseñas, tratar de cambiarlas, y actualizarlas con frecuencia.

REFERENCIAS BIBLIOGRÁFICAS

- Ellerbeck, S; (2022) Casi la mitad de las empresas se ven afectadas por la delincuencia económica, siendo la ciberdelincuencia la amenaza más grave. ¿Qué pueden hacer al

respecto? Recuperado de https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/

- Brown, Jefrena r; (2022). 6 formas en que la ciberdelincuencia afecta a las empresas. Recuperado de https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
- Pegas de Ali; (2016). Instituciones financieras y cibercrimen: amenazas, desafíos y oportunidades. Recuperado de https://www.rusi.org/explore-our-research/publications/rusi-newsbrief/financial-institutions-and-cybercrime-threats-challenges-and-opportunities
- Misceláneas. (2022). Panamá es uno de los países más vulnerables para los ciberdelincuentes. Recuperado de https://decisionespanama.com/panama-es-uno-de-los-paises-mas-vulnerables-para-los-ciberdelincuentes/
- LA ESTRELLA DE PANAMÁ. (2022). La Estrella de Panamá: Losciberdelitos aumentan más del 50% en prepandemia, banca y finanzas los mayormente afectados. Recuperado de https://www.sseguras.com/noticias/soluciones-seguras-en-las-noticias/la-estrella-de-panama-los-ciberdelitos-aumentan-mas-del-50-en-prepandemia-banca-y-finanzas-los-mayormente-afectados
- Oficina de las Naciones Unidas contra la Droga y el Delito UNODOC. (2020). Serie de módulos universitarios, Ciberdelincuencia. Recuperado de https://www.unodc.org/e4j/es/tertiary/cybercrime.html#:~:text=Mediante%20el%20uso%20indebido%20de,la%20seguridad%20de%20los%20sistemas
- Flores Villacrés, E.J., Asanza Molina, MI., Berrones Miguez, M; (2014). Contribuciones a las Siencias Sociales. Ciberdelincuencia, un mal que afecta a la sociedad Actual. Recuperado de https://www.eumed.net/rev/cccss/29/ciberdelincuencia.html#:~:text=Este%20tipo%20de%20virus%20ocasiona,los%20trabajos%2C%20en%20algunos%20casos
- José R Godoy T. (2020, enero 15). Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Inform ación Contables Administrativos (SICA). Universidad de Panamá, Panamá.
- García Armuelles, L; (2023).'Phishing' y 'Ransomware', los ciberataques más comunes a la banca panameña. Recuperado de https://www.laestrella.com.pa/economia/230324/phishing-ransomware-ciberataques-comunes.
- Tigobusiness. (2023). Ciberdelitos en Panamá. Recuperado de https://www.tigo.com.pa/empresas/blog/ciberdelitos-en-panama