# UNIVERSIDAD DE PANAMÁ
## VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
## FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD
## PROGRAMA DE DOCTORADO EN CIENCIAS EMPRESARIALES

**“IMPACTO EN LOS SISTEMAS DE INFORMACIÓN CONTABLES POR EFECTO DE LOS DELITOS INFORMÁTICOS A LAS OPERACIONES DE BANCA POR INTERNET EN LA CIUDAD DE PANAMÁ”**

**AUTOR:**
**JOSÉ RENÉ GODOY TROYA**
**8-442-236**

**TESIS DOCTORAL PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR POR EL GRADO ACADÉMICO DE DOCTOR EN CIENCIAS EMPRESARIALES CON ÉNFASIS EN CONTABILIDAD**

**DIRIGIDA POR**
**DRA. MARICELA SEVILLA CARO**

**PANAMÁ, REPÚBLICA DE PANAMÁ**

**2021**

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

**Tabla 18**

# ÍNDICE DE FIGURAS

# INTRODUCCIÓN

En las sociedades del mundo, el uso de las TIC se ha convertido en el día a día, producto de los grandes avances tecnológicos como de la globalización, los cuales han jugado un papel trascendental en el crecimiento económico del mundo. No obstante, estos adelantos provocan incalculables ventajas y desventajas que han sido de gran provecho a usuarios y organizaciones. Fue toda una revolución la utilización de redes de comunicación como de sistemas de información; su creciente vínculo trasciende las fronteras de los países, proporcionando espacios a diferentes ámbitos de la vida, y a una amplia variedad de negocios, entre otros.

Al mismo tiempo, existen numerosos riesgos, todos ellos producto de la característica intrínseca que posee el internet, la inexistencia de fronteras, la cual ofrece un mayor número de oportunidades a que cibercriminales puedan realizar diferentes comportamientos antisociales y el desarrollo de novedosas y complejas formas de infringir la Ley, de entre las cuales destaca, las agresiones mal intencionadas a los sistemas de información, por lo que muchos gobiernos han tenido que hacer frente ante esta circunstancia aportando respuestas expeditas que faciliten la protección de los usuarios, tanto empresas como particulares.

A este respecto, Téllez (2008) manifiesta que

> Los ataques adoptan diversas formas, entre ellas, el acceso ilegal, la difusión de programas maliciosos, así como la denegación de servicios en las operaciones que se realizan a través de la banca en línea. Por lo que dichos ataques pueden atentar contra la libertad de seguridad y justicia que merece la sociedad de la información,

> ya que pueden ser lanzados en cualquier momento y desde cualquier lugar del mundo debido a los crecientes, novedosos e inesperados avances tecnológicos. (p.187)

Por otro lado, Reyna (2002) afirma que

> La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen, lo que resulta más dramático en las sociedades informatizadas, en la medida que éstas resulten tecnológicamente vulnerables. Más aun, 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 y control en estos. (p.125)

Díaz (2010), señala que “desde hace tiempo se hace énfasis en que las fronteras nacionales constituyen un obstáculo evidente para la detección, investigación, persecución y castigo de los autores de delitos perpetrados mediante el uso de nuevas Tecnologías de Información y Comunicación (TIC). En cambio, Internet está configurada como un espacio sin fronteras para aquellos” (p.183).

Díaz (2010), amplia “La dimensión supranacional juega, por tanto, una importancia crucial en el tratamiento de los delitos informáticos. Es imperativa la ejecución de políticas conjuntas, generales, que integren a todos los Estados y sectores de la sociedad” (p.183).

Por lo que se hace evidente, que para una sociedad desarrollada o en vías de serlo, es necesaria la implementación de nuevas técnicas dirigidas a la correcta

visualización de los delitos económicos, financieros y contables, así como lograr el adecuado manejo de la investigación de estos.

Panamá no escapa a esta problemática, la evolución de la tecnología y del internet pone elementos y medios a disposición de las organizaciones para desarrollar mejores estrategias que aseguren su permanencia en el mercado. La introducción de nuevos negocios en ambientes computacionales mejor conocidos como "*e*-comerce" a nuestra llamada sociedad de consumo y la proliferación de opciones de compra para los clientes, han impulsado a usuarios y organizaciones al uso de nuevos mecanismos tecnológicos ofrecidos.

El sector bancario no se queda atrás, la necesidad de competir con empresas de clase mundial hace imprescindible la búsqueda de un alto desempeño en sus operaciones, así como la entrega de productos y servicios de gran calidad; productos como la banca electrónica o banca en línea, que operan de forma electrónica o digital para efectuar pagos, realizar trasferencias entre otros, facilitando así la internacionalidad de sus operaciones; al mismo tiempo, este es el campo de acción de personas mal intencionadas que buscan las oportunidades o vulnerabilidades de los usuarios (en muchas ocasiones inexpertos) para efectuar sus actos ilícitos. Es así como, "La investigación científica daba inicio allí donde alguien advierte de la existencia de ciertos fenómenos" (Aristóteles, citado por Mardones & Ursúa, 1991, 21).

Los hechos antes señalados, son el motivo que impulsó indagar investigaciones anteriores, para así fundamentar y dar bases sólidas a este trabajo, cuyo objetivo general es valorar el impacto que generan los delitos informáticos en los sistemas de información contables usados en operaciones de banca por internet, de clientes que manejan este

tipo de servicio en la ciudad de Panamá. Para ello, nos apoyamos de modernas herramientas de análisis, con el fin específico de identificar los crímenes más recurrentes a este tipo de operaciones, y cuáles de ellos causan mayores impactos o afectaciones. Y con los resultados obtenidos, determinar la forma de mitigar sus riesgos y así dejar las bases, mecanismo y herramientas, para crear a futuro, un modelo conceptual, el cual, a través de software, pueda remediar la ocurrencia y afectación a los sistemas de información, en harás y beneficio de nuestra sociedad, la cual se encuentra igual o más vulnerable respecto a otros países.

De igual manera, se dio respuesta a las preguntas e hipótesis planteadas en la investigación, como lo son: ¿Cuáles son los tipos de delitos informáticos más comunes que impactan a los sistemas de información?, ¿Cuáles son los tipos de delitos informáticos que causan mayores afectaciones a las operaciones de banca por internet?, ¿Cuáles son los tipos de delitos informáticos más frecuentes a los servicios de banca por Internet?, además, si ¿Poseen los cuentahabientes y usuarios de la banca por Internet conocimientos sobre los delitos informáticos que pueden afectar sus bienes?, y si ¿La entidad Bancaria o financiera donde posee su cuenta le brinda información de los riesgos producto del mal uso de la banca por Internet?; El análisis de las preguntas anteriores, contribuyó a dar solución a la hipótesis planteada, la cual es: La recurrencia, porcentaje, afectaciones contables y tipos de delitos informáticos, impactan los sistemas de información a través de operaciones de banca por Internet de cuentahabientes en la ciudad de Panamá.

Para el desarrollo de este estudio, se planteó como alcance y delimitación, el área de la ciudad de Panamá, hasta 2020, por lo que se realizaron entrevistas a organizaciones y consultores locales que poseen gran conocimiento del tema, como la

Súper Intendencia de Bancos (SBP), máximo ente regulador del sector bancario en nuestro país. Además, se complementó con encuestas a clientes usuarios de la banca por Internet de los diferentes bancos de nuestra ciudad contrastados con datos estadísticos de fuentes secundarias relacionadas.

La principal limitación que influyó en el desarrollo de la investigación fue la llegada a nuestro país y al mundo entero de la Pandemia denominada Covid-19, a inicios del año 2020, motivo por el cual el Gobierno Nacional presentó medidas de restricción para mitigar los efectos causados por esta. Entre las principales medidas que se implementaron se puede mencionar la suspensión de toda actividad económica por cuarentena total, lo que provocó el cierre de las oficinas bancarias y el cese de todas las actividades en la urbe de la ciudad de Panamá, dificultando la toma de entrevistas y encuestas, tanto a cuentahabientes como a expertos en el tema.

Entre los resultados más relevantes, destaca que, sin importar el nivel de conocimientos que tengan los cuentahabientes sobre el uso de redes de comunicación, sistemas de información o cualquier mecanismo o medio electrónico, estos seguirán utilizándolos con mucha frecuencia y los cibercriminales se aprovecharán de estos usuarios inexpertos que realizan transacciones u operaciones por estos medios o canales electrónicos.

Por otro lado, en lo que se refiere a experiencias de compras por Internet seguras, sin importar los tipos de servicios ofrecidos por los bancos, llámese banca electrónica o por internet, estos no se ven afectados por el conocimiento o desconocimiento del cuentahabiente, en el uso de redes de comunicación, sistemas de información y cualquier medio o mecanismo electrónico.

En cuanto a, la estructura de la investigación, la misma consta de cinco capítulos, de los cuales en el primero se abordarán los antecedentes de esta y del problema, justificaremos su relevancia y los objetivos que nos guiarán a la consecución de la meta, la delimitación y limitaciones producto de la investigación y por último formularemos nuestra pregunta de hipótesis.

En el segundo capítulo, se presentará el marco teórico; en él, los conceptos, características, evolución y descripción del contexto de las unidades de análisis; en el tercer capítulo, los aspectos metodológicos, ya sea tipo, diseño de investigación, fuentes de información, población, muestra y tipo de muestra, las variables su conceptualización y operacionalización; en el capítulo cuarto, se presentarán los resultados obtenidos y el análisis de estos, y en el quinto capítulo las conclusiones y recomendaciones pertinentes.

# RESUMEN

Los grandes avances Tecnológicos, la característica intrínseca del Internet, (inexistencia de fronteras), y el aumento de usuarios inexpertos, se han convertido en el principal campo de acción de cibercriminales que están al asecho para crear novedosas y complejas formas de infringir la ley. A su vez, estos adelantos, los que han contribuido a lo que conocemos como “Globalización”, han jugado un papel trascendental en el crecimiento económico del mundo ya que conllevan un sin número de ventajas y desventajas que han sido de provecho a usuarios y organizaciones. Su creciente vínculo traspasa las fronteras de los países, creando espacios suficientes a diferentes ámbitos de la sociedad, negocios diversos, entre otros. Por otro lado, la mencionada inexistencia de fronteras ofrece un mayor número de oportunidades a cibercriminales, de perpetrar diferentes actos o comportamientos antisociales, principalmente, agresiones mal intencionadas a sistemas de información.

Estos, han motivado a los gobiernos, a hacer frente a tal circunstancia, aportando respuestas expeditas, que faciliten la protección de sus usuarios, ya sean empresas como particulares, a través de regulaciones las cuales desde hace mucho tiempo se han tratado de unificar para que exista una misma normativa en todos los países.

Lo anterior es lo que impulsa realizar esta investigación, cuyo objetivo general es identificar el impacto de los delitos informáticos a los sistemas de información por operaciones de banca por Internet y por ende a organizaciones y usuarios que utilicen este tipo de servicio, ya que Panamá, un país en vías de desarrollo, y por consiguiente

endeble ante este tipo de actos, puede sufrir afectaciones. Para ello, se utilizó herramientas modernas de análisis, con el fin de identificar estos delitos, sus afectaciones y la forma de mitigarlos, y así sentar bases, mecanismo y herramientas, que sirvan para crear a futuro, un modelo conceptual, el cual, pueda remediar la ocurrencia y afectación de estos hechos delictivos a los sistemas de información, en harás y beneficio de nuestra sociedad.

Palabras clave: Avances tecnológicos, cibercrimen, sistemas de Información delitos informáticos, regulaciones, operaciones banca por Internet, afectaciones.

# ABSTRACT

The great technological advances, the intrinsic characteristic of the Internet (non-existence of borders), and the increase in inexperienced users, have become the main field of action of cybercriminals who are on the lookout to create novel and complex ways of breaking the law. In turn, these advances, which have contributed to what we know as "Globalization", have played a transcendental role in the economic growth of the world since they entail a number of advantages and disadvantages that have been of benefit to users and organizations. Their growing bond goes beyond the borders of countries, creating sufficient spaces for different areas of society, diverse businesses, among others. On the other hand, the aforementioned non-existence of borders offers a greater number of opportunities for cybercriminals to perpetrate different acts or antisocial behaviors, mainly malicious attacks on information systems.

These have motivated governments to face such a circumstance, providing expeditious responses, which facilitate the protection of their users, whether companies or individuals, through regulations which have long tried to unify so that there is the same regulation in all countries.

The foregoing is what drives this research, whose general objective is to identify the impact of computer crimes on information systems due to Internet banking operations and therefore on organizations and users who use this type of service, since Panama, a developing country, and therefore weak in the face of this type of act, may be affected. For this, modern analysis tools were used, in order to identify these crimes, their effects and the way to mitigate them, and thus lay the foundations, mechanism and tools that

serve to create a conceptual model in the future, which can remedy the occurrence and impact of these criminal acts on information systems, to the benefit of our society.

Keywords: Technological advances, cybercrime, Information systems, computer crimes, regulations, Internet banking operations, affectations.

# CAPÍTULO I

# EL PROBLEMA

## Antecedentes

En el siguiente apartado se expondrán algunos antecedentes de la situación problemática desde la perspectiva de investigaciones relacionadas al tema los cuales de alguna forma previa han realizado estudios y dejado sus aportes y contribuciones para ayudar a mitigar los estragos acaecidos por este flagelo mundial el cual es nuestro objeto de investigación.

Los delitos informáticos cometidos haciendo uso de las nuevas Tecnologías de la Información y la Comunicación (TIC), no han hecho más que incrementarse año tras año. Estos no sólo aumentan en número, lo hacen también en diversidad debido al auge tecnológico y al creciente uso de internet por los ciudadanos.

Por un lado, la propia evolución y desarrollo de nuevas tecnologías ha hecho posible la aparición de nuevas formas de actos delictivos a través de Internet, formas cada vez más sofisticadas y efectivas; Por otro lado, su uso, son cada vez más las personas, organizaciones e instituciones que utilizan las nuevas tecnologías e internet aplicadas a ámbitos de la vida y negocios mucho más diversos lo cual deja abierto un gran campo de oportunidades para que los cibercriminales puedan actuar.

Con relación al primer punto, Almagro (2019), secretario general de la Organización de los Estados Americanos (OEA), señala en el libro, Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, que

> Internet ha revolucionado el mundo que nos rodea y la forma en que interactuamos con los demás. Esto es particularmente cierto en América Latina y el Caribe, ya que casi 70% de la población está en línea y la tasa de crecimiento de usuarios de Internet es la tercera más alta del mundo – es decir, 2,4% entre 2000-2019.1 En las Américas y el Caribe, se utiliza Internet para relacionarse con las personas, compartir ideas, gestionar negocios y realizar transacciones. Por todo ello, el sector financiero fue uno de los primeros en adoptar las tecnologías y ofrecerlas a sus clientes. (p.8)

Conocedores de la situación que está ocurriendo día a día, presentan investigaciones relacionadas que abordan el tema, en atención al desarrollo de sus variables, las que se presentarán en adelante.

Dicho lo anterior, la investigación de la Universidad Complutense de Madrid titulada *Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma*, elaborada por González (2013), señala que

> Estamos ante un fenómeno relativamente novedoso, que además tiene una característica inherente al desarrollo tecnológico; la tecnología avanza a un ritmo vertiginoso, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho, esa misma característica. Prueba de ello son los interesantes informes elaborados por el IC3 (Internet Crime Complaint Center) norteamericano donde se encuentran tablas cronológicas referidas al

> aumento de este tipo de delitos, e igualmente a las estadísticas que manejan las empresas privadas en cuyos múltiples informes, también, se recoge el indudable crecimiento exponencial de estas conductas prohibidas, o la recentísima puesta en funcionamiento del EC3 (European Cybercrime Centre) en la Unión Europea para coordinar la respuesta ante ciberataques en los Estados de la Unión. (p.351)

De igual modo, la investigación que se presentó en la Universidad Ramón Llull, titulada *La Prueba electrónica: sus implicaciones en la seguridad de la empresa*, a cargo de Puig (2014), afirma que

> El siglo XXI es el de la implantación general de las tecnologías de la información que son las que caracterizan esta nueva era de desarrollo tecnológico que se inicia en las últimas décadas del siglo pasado. El desarrollo de la informática y la computarización ha impulsado las redes de comunicación que se extienden por todos los ámbitos sociales desde la administración hasta las relaciones sociales y, especialmente, en el comercio electrónico. Las nuevas tecnologías se imponen en una sociedad caracterizada por la expansión de redes, servicios y aplicaciones digitales que determinan la competitividad de las empresas en un entorno cada vez más global. (p.369)

Como afirmamos en líneas anteriores, una de las principales problemáticas que dificulta ejercer un debido control de estos, y en el que se viene haciendo énfasis desde hace ya mucho tiempo, son las fronteras nacionales, el problema de la supra nacionalidad.

De manera semejante, afirma la investigación realizada en la Universidad Complutense de Madrid, titulada *El Delito en la ciber sociedad y la justicia penal internacional*, presentada por Rincón (2015) que

> Al igual que en la persecución y sanción de cualquier otra categoría de delito, las fronteras creadas no solo por el territorio sino por el concepto de jurisdicción y competencia que son los delimitantes del ejercicio punitivo de los Estados, impiden que se investigue, juzgue y sancione a un sujeto que ha cometido la conducta desde un territorio pero con consecuencias en otro, o por el contrario la cometió desde un Estado pero las víctimas o el daño se materializan en otro, teniendo en cuenta este concepto, no podrá ni debe haber fronteras en la búsqueda de terminar la impunidad en los delitos informáticos. (p.487)

Además, añade Rincón (2015) que

> El planteamiento anterior nos lleva a determinar la necesidad de buscar un sistema de justicia universal que permita la investigación juzgamiento y sanción de los delitos informáticos o delitos que atentan contra la información y los datos. Es en este sentido que hemos concluido que la mejor forma para lograrlo es que los Estados de forma voluntaria renuncien a esta categoría de su Ius Puniendi, de forma que la persecución de esta clase de delitos, para cada Estado, no sea de tipo principal, sino que esta función recaiga de manera primaria sobre una organización internacional. (p.488)

Todas estas observaciones se relacionan también con lo que señala Díaz (2010), el cual afirma que, “Las fronteras nacionales crean obstáculos para la detección, investigación, persecución y castigo de los autores de delitos perpetrados mediante el

uso de nuevas Tecnologías de Información y Comunicación (TIC). En cambio, Internet está configurada como un espacio sin fronteras para estos" (p.183).

De ahí que, como señala Almagro (2019), secretario general de la Organización de los Estados Americanos

> El sector financiero ha experimentado uno de los mayores índices de digitalización en los últimos años. Cada día un mayor número de clientes usan medios no presenciales para realizar transacciones por internet, pagos a través de dispositivos móviles o cualquier otro tipo de trámites bancarios. En Colombia, se estima que la población bancarizada dentro del universo de internautas es de 81%, y que 79,4% de la población bancarizada internauta ha consultado o hecho operaciones bancarias en línea en 2018 (p.8).

Al mismo tiempo, añade Almagro (2019) que

> Por eso, los bancos también son pioneros en la adopción de medidas para asegurar la protección de sus clientes. De hecho, el sector financiero es tradicionalmente uno de los principales blancos de las amenazas cibernéticas. De acuerdo con el estudio de la OEA "El Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe," publicado en octubre de 2018, el 92% de las entidades bancarias identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital, y el 37% de entidades bancarias manifestaron que sí fueron víctimas de ataques exitosos. La principal motivación de dichos ataques durante el año 2017 fueron motivos económicos (79% de las entidades bancarias víctimas). (p.8)

Avanzando en el razonamiento, señala Castro (2019), presidente de la Asociación Bancaria Colombiana, en el Libro, Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, que

> El ciberespacio es un sistema complejo a nivel físico, de red y cognitivo. Tradicionalmente, estos sistemas están altamente interconectados y estrechamente acoplados, por lo que las interrupciones pueden conectarse en cascada fácilmente. Este tipo de riesgos son la razón por la cual el ciberespacio es capaz de tener eventos muy impredecibles y de consecuencias altas. Aun no existen modelos que permitan entender y gestionar de forma organizada la complejidad de este riesgo sistémico. Si bien ningún ataque hasta la fecha ha generado inestabilidad financiera, el impacto potencial de un ataque cibernético programado para desestabilizar las funciones y vulnerabilidades de los canales tradicionales del sistema financiero no se ha examinado lo suficiente. Es claro que la ciberseguridad ya no puede considerarse un tema técnico que se delegue en el departamento de sistemas, sino que debe abordarse como un tema estratégico que alcanza a toda la organización. (p.13)

Con respecto al primer punto, Castro (2019), amplia señalando que

> En el mundo, gran parte de las comunicaciones y procesos son digitales, con lo cual la ciberseguridad no es una alternativa, sino un requisito. Los riesgos cibernéticos que afectan al sector gobierno, al sector privado y a las personas tienen unos impactos y una problemática distintos. No obstante, cada uno debe aplicar medidas de seguridad, adecuándolas a su naturaleza y su propio contexto (p.13).

Por otro lado, con relación a las operaciones de banca electrónica, señala la investigación de la Universidad de Surrey, titulada *Mejora de la autenticación de transacciones de la banca en línea mediante el uso de pruebas de manipulación indebida y computación en la nube*, presentada por Elhag (2015) que

> El término Banca Electrónica o Banca por Internet es un concepto avanzado y completo que surgió a principios de los años noventa como un concepto de servicios financieros por control remoto, banca electrónica remota o banca en casa. Los clientes requieren que el banco cree servicios con acceso restringido. El banco le proporciona al cliente un paquete de software, ya sea gratuito o por una tarifa, lo que le permite utilizar los servicios bancarios a cierta distancia. Alternativamente, el cliente compra un paquete de software conocido como software de gestión financiera personal (PFM). Por lo tanto, el concepto de servicios financieros se basa en la banca a distancia entre el Banco y la computadora personal del cliente. (p.1)

De manera semejante, Elhag (2015) señala que

> La seguridad de un sistema puede verse como una cadena de métodos de protección, y el nivel global es tan fuerte como su eslabón más débil. En el mundo financiero existen herramientas, como el perfil de comportamiento del usuario, que están comenzando a ser consideradas y que, de hecho, han sido utilizadas por los bancos durante muchos años en el "mundo real" en forma de controles de back-end. (p.150)

Sírvase de ejemplo, el señalado por Elhag (2015) en el cual añade que, “Todo esto empeora en los casos de identidad del usuario o robo de credenciales, que requieren medidas más avanzadas y, curiosamente, se debe esperar un retorno a los controles

tradicionales de back-end. En el último término, los métodos de protección exclusivamente técnicos parecen no ser capaces de resolver completamente la situación" (p.150).

De ahí que, concluya Elhag (2015) indicando que

> Al estudiar las fortalezas de la seguridad en el sector financiero y el ciberdelito en general, obviamente el cibercrimen sigue existiendo y el riesgo para el sector financiero está empeorando, especialmente en el lado del cliente. Las preocupaciones de seguridad aún existen, aunque la topografía de la banca ha cambiado dramáticamente con el inicio de la banca en línea como un nuevo enfoque para dirigir el negocio bancario. Sin embargo, los clientes de los bancos buscan mayor comodidad para acceder a las instalaciones bancarias y esperan que sus bancos ofrezcan servicios de valor agregado a través de canales como la banca en línea. (p.2)

Valverde (2015), en la investigación de la Universidad de Valladolid, Titulada: *Análisis de la banca por Internet entre los usuarios particulares.* Un Modelo dinámico de sistemas, a su vez, afirma que, "Las entidades bancarias están viendo un importante potencial en la conexión mediante el teléfono móvil, este ha ido ganando terreno hasta llegar a ser el dispositivo más utilizado para conectarse a Internet" (p.256).

Por otra parte, añade Valverde (2015) que, "Esta moda beneficia de nuevo al servicio ofrecido en banca, ahora con un acceso más fácil y lo consideran como una oportunidad de negocio, por ello, cada vez son más las aplicaciones bancarias ofrecidas

mediante este soporte, aunque el gran desarrollo de la banca móvil todavía está por llegar" (p.256).

Se debe agregar, lo señalado por Valverde (2015) en donde afirma que

> La apuesta de las entidades por la tecnología no solo está sirviendo para generar nuevos contratos. En estos momentos tiene un papel muy importante sobre sus cuentas anuales ya que además de ahorrar costes gracias a la digitalización de los procesos, permite incrementar los ingresos con productos y servicios que no serían posibles en la oficina física. Entre los ingresos cabe destacar una partida que por el momento no es muy significativa, pero que puede llegar a ser importante. Nos referimos a los ingresos a través de las operaciones de pago en un momento en el que el comercio electrónico está en auge ya que cada vez se compra más por este canal y lo hacen más personas. La apuesta de las entidades por la incorporación del móvil para operaciones de pago puede llegar a tener gran importancia no solo por los ingresos que atrae, sino porque este servicio ya está siendo demandado por los clientes y ofrecido por grandes empresas de tecnología; si no se oferta, puede incrementarse el traspaso a otros canales y, en el peor de los casos a otro tipo de financiación no bancaria. (p.256)

De acuerdo con lo anterior, señala Castro (2019) que, es prácticamente un hecho que los ataques cibernéticos, el cibercrimen y los incidentes de seguridad no van a disminuir; por el contrario, aumentarán de forma exponencial en los próximos años. Según el Foro Económico Mundial, los ataques en contra de empresas casi se han duplicado en cinco años y los incidentes que antes se consideraban algo fuera de lo común se están volviendo más y más recurrentes. Además, el impacto financiero de la ciberdelincuencia va en aumento (p.13).

Por lo que, Echenique (2008), en su apartado, Delitos por computadora, del libro Auditoría Informática, señala que

> En la situación actual de criminología, en los delitos de “cuello blanco” se incluye la modalidad de los delitos hechos mediante la computadora o los sistemas de información, de los cuales 95% de los detectados han sido descubiertos por accidente, y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como la computadora ha modificado las circunstancias tradicionales del crimen. Muestra de ello son los fraudes, falsificaciones y venta de información hechos a las computadoras o por medio de estas. (p.192)

Amplía, Echenique (2008), indicando que, “Existen diferentes estimaciones sobre el costo de los delitos de cuello blanco, las cuales dependerán de la fuente que haga estas estimaciones, pero en todos los casos se considera que los delitos de cuello blanco en Estados Unidos superan los miles de millones de dólares” (p.192).

Así mismo, la Encuesta Global sobre Delitos Económicos de PWC, Capítulo Argentina, titulada, Hacia una nueva ética en los negocios. Delitos económicos e informáticos (2016), en su apartado titulado, ¿Cuál es el costo de sufrir un fraude?, señala que

> Desde el punto de vista del costo delito en sí mismo, el 43% de las víctimas estimaron un impacto financiero mayor a USD 100.000. Comparado con nuestra encuesta anterior, donde solo el 21% de las empresas sufrió una pérdida mayor a USD 100.000, se ha duplicado el porcentaje de organizaciones que soportaron una

> mayor pérdida económica. También, resulta mayor si lo comparamos con América Latina (31%). (p.12)

En este sentido, la Encuesta Global sobre Delitos Económicos de PWC, Capítulo Argentina (2016), señala que

> Debe agregarse que el costo no solamente se limita a la pérdida económica, sino también, a los recursos internos y externos dedicados para combatir el fraude. En tal sentido, 1 de cada 3 organizaciones manifestaron haber invertido más de USD 50.000 en investigar los casos de fraude ocurridos en los últimos 24 meses. Definitivamente, además de las propias consecuencias inherentes de sufrir un delito, resulta oneroso para las víctimas conocer la modalidad del ilícito y encontrar a los responsables. Más allá de la pérdida económica y los recursos dedicados para investigar un fraude, es casi imposible cuantificar el verdadero impacto de un delito en el valor de la compañía. • ¿Cuántos clientes potenciales se pierden si la compañía resulta responsable de un escándalo de corrupción? • ¿Cuántos talentos abandonan la organización al observar la impunidad de un colega al cometer un ilícito? • ¿Cuántas empresas innovadoras y competitivas dejan de participar en las licitaciones porque para ganarlas es necesario pagar una coima? • ¿Cuán eficaz y eficiente es la gestión de un área, si el gerente responsable de la misma fue elegido por ser el hijo de uno de los directores de la compañía y no por sus capacidades y credenciales? (p.18)

En síntesis, se puede afirmar que las investigaciones internacionales antes citadas, indican que por una parte el cibercrimen sigue existiendo y en aumento mientras que el riesgo en el sector financiero está empeorando, y más con relación a sus clientes, ya que estos con el inicio de la banca en línea como un nuevo enfoque para dirigir el

negocio bancario, buscan mayor comodidad para acceder a las instalaciones bancarias y esperan de sus bancos se ofrezcan servicios de valor agregado, a través de canales como la banca electrónica o banca en línea, siendo este el principal campo de acción de los ciberdelincuentes, los cuales están al acecho de toda aquella vulnerabilidad, principalmente, de usuarios inexpertos, que usan estos sistemas sin las debidas precauciones y controles de seguridad.

Dicho lo anterior, la Encuesta Global sobre Delitos Económicos de PWC, Capítulo Argentina, (2016), realiza notables señalamientos en su apartado titulado, La importancia de la defensa, entre los cuales están:

> Las amenazas a los sistemas informáticos y sus respectivos controles mitigantes son responsabilidad de toda la compañía, pues cada integrante cumple un rol clave. Si bien se observa una gran evolución en la gestión de los sistemas de información, la mayoría de las empresas aún no conoce los riesgos que enfrentan, ni saben cómo anticiparse o responder frente a un potencial incidente. Son muchas las organizaciones que sufren daños informáticos debido a debilidades básicas como, falta de involucramiento por parte de los directivos, configuraciones de sistema deficientes y carencia de control sobre aquellos terceros con acceso a la red y/o a los datos de la organización. (p.40)

Más aún, esta Encuesta Global sobre Delitos Económicos de PWC, Capítulo Argentina, (2016) amplia, señalando que

> Es vital que los directivos incorporen los delitos informáticos en sus evaluaciones de riesgo, comuniquen los pasos a seguir a todos los sectores de la organización y planifiquen con el sector de TI en qué medida quieren ser alertados en caso de

> existir un incumplimiento o un fraude. Las amenazas informáticas deben ser consideradas y planificadas de igual manera que cualquier otra amenaza de negocio: con un plan de respuestas ante incidentes, con roles y responsabilidades establecidos, con un plan de monitoreo y con la planificación de distintos escenarios. Es por eso que las compañías líderes están incorporando ejercicios de gestión de crisis, como elemento central de su estrategia de respuesta ante potenciales incidentes en materia de seguridad informática. Realizan ejercicios que consisten en reunirse y analizar posibles escenarios, evaluando distintos planes de respuesta e identificando los respectivos errores y debilidades. (p.40)

Por todo lo antes señalado, se puede confirmar, de acuerdo a toda la evidencia investigada y presentada, que las actuales legislaciones de nuestro país y la de muchos países de la región, no son acordes a la realidad acelerada que estamos viviendo en cuanto a los avances tecnológicos, hecho que ha provocado que la Súper Intendencia de Bancos de Panamá (SBP), para dar seguridad al sector financiero, cree acuerdos de protección a nuestro Sistema Bancario con la finalidad minimizar los riesgos provocados por delitos informáticos a los sistemas de información de los bancos.

Se deba agregar, en cuanto a la situación Penal en Panamá, lo que señalan expertos en este ramo como, Parodi (2014), en su apartado, Breve Análisis de los Principales Delitos Financieros en Panamá, de la revista Ministerio Público de Panamá, que

> El desarrollo de las sociedades modernas ha provocado complejos fenómenos sociales, políticos, económicos y jurídicos. Desde el ámbito criminológico, esto se ha traducido en un aumento del número de delitos patrimoniales tradicionales y especialmente en el nacimiento de nuevas formas delincuenciales con contenido

> económico, como ya pusiera de manifiesto E. H. Sutherland en su obra Delitos de cuello blanco. (p.92)

A su vez, amplía Parodi (2014), señalando que

> Estamos inmersos en una sociedad compleja, en un sistema económico cada vez más planificado e intervencionista, relaciones económicas veloces, aumentos en el otorgamiento de créditos, etc., y todo ello provoca mayores oportunidades en el mundo económico y de los negocios y, por tanto, una elevación de las oportunidades para cometer ilegalidades. Si a ello se añade la mayor complejidad de las estructuras económicas nacionales e internacionales, es fácil entender que estos cambios actúen como factores criminógenos que provocan formas de delincuencia novedosas. (p.92)

Por lo que, Parodi (2014), culmina, en este sentido, señalando que

> El afrontar la fenomenología delictiva en materia económica no es tarea fácil, a pesar de los esfuerzos de legisladores y penalistas, toda vez que resulta difícil definir qué es el Derecho Penal Financiero, sus fines y fundamentos. Existen pocos estudios criminológicos que ofrezcan datos fiables sobre su número y efectos; la ya mencionada complejidad del fenómeno dificulta la tipificación de las conductas delictivas, requiriendo el uso de normas penales en blanco, como veremos al llegar al análisis de los delitos financieros. (p.93)

Al mismo tiempo, se puede coincidir con lo señalado en el apartado anterior, sobre la poca existencia de estudios sobre esta temática, ya que en revisión al sistema de biblioteca de la Universidad de Panamá (SIBIUP) y la biblioteca de la Universidad

tecnológica de Panamá, no se encontró investigación alguna en nuestro país, relacionada a este asunto, por lo que es de nuestro interés contribuir y crear precedente respecto a este flagelo que afecta a nuestra sociedad.

## Antecedentes del problema

## Planteamiento del problema

En el siguiente apartado se enuncian los rasgos de la situación problemática, motivo por el cual se ha despertado nuestro interés de investigar la misma.

Cerda (1998) “Enunciar” en este caso es el acto de expresar el conjunto de ideas y datos que componen un problema” (p.162).

El informe llamado “Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno” Oficina de Naciones Unidas contra la Droga y el Delito (UNODC 2013), señala que

> En 2011, al menos 2.300 millones de personas, equivalente a más de un tercio de la población total del mundo, tuvo acceso a Internet. Más del 60% de todos los usuarios están en los países en desarrollo y el 45% de todos los usuarios de Internet tienen menos de 25 años. Se estima que para 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70% de la población mundial. Para 2020 el número de dispositivos interconectados por la red (“Internet de las cosas”) será seis veces mayor al número de personas, lo que transformará la concepción actual

> de Internet. En el mundo híper conectado del futuro será difícil no imaginar un “delito informático”, o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo Internet. (p.2)

> Acorde a lo antes presentado, a nivel mundial la diversidad de actos delictivos cibernéticos es muy variada, así podremos encontrarnos con los motivados por intereses financieros, los relacionados con el contenido informático, los que atentan contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos, también en relación a la amenaza y riesgo relativos, estos son percibidos de forma distinta por los gobiernos y las empresas privadas, lo que dificulta hacer comparaciones entre países puesto que los datos estadísticos manejados por la policía *no representan base sólida para realizar las mismas*, inclusive dos tercios de los países participantes manifestaron que sus sistemas policiales son deficientes para registrar los delitos informáticos, por lo que puede existir una disparidad ya que los datos policiales se ven afectados por factores como los niveles de desarrollo de un país y la capacidad policial especializada en esta área, más que con las tasas de delincuencia existentes. (p.2)

Mientras tanto, el mismo estudio (UNODC 2013) señala que las encuestas de victimización *sí son consideradas como base sólida para realizar comparaciones*, es así como se demuestra que la victimización individual es considerablemente superior a otras formas de delitos convencionales, además señala algunos datos o tasas porcentuales de victimización de determinados delitos informáticos:

> 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)

Dicho de otra manera, Shick & Toro (2017), señalan en su libro Cibercriminología, Guía para la investigación del cibercrmen y mejores prácticas en seguridad digital, que: "El concepto de fraude en Internet cubre una amplia gama de esquemas fraudulentos "; Además, entre los principales tipos de victimización por fraude están el "robo de identidad o *phishing,* fraude de subastas, estafa nigeriana y secuestro de información *o ransomware"* (p.105).

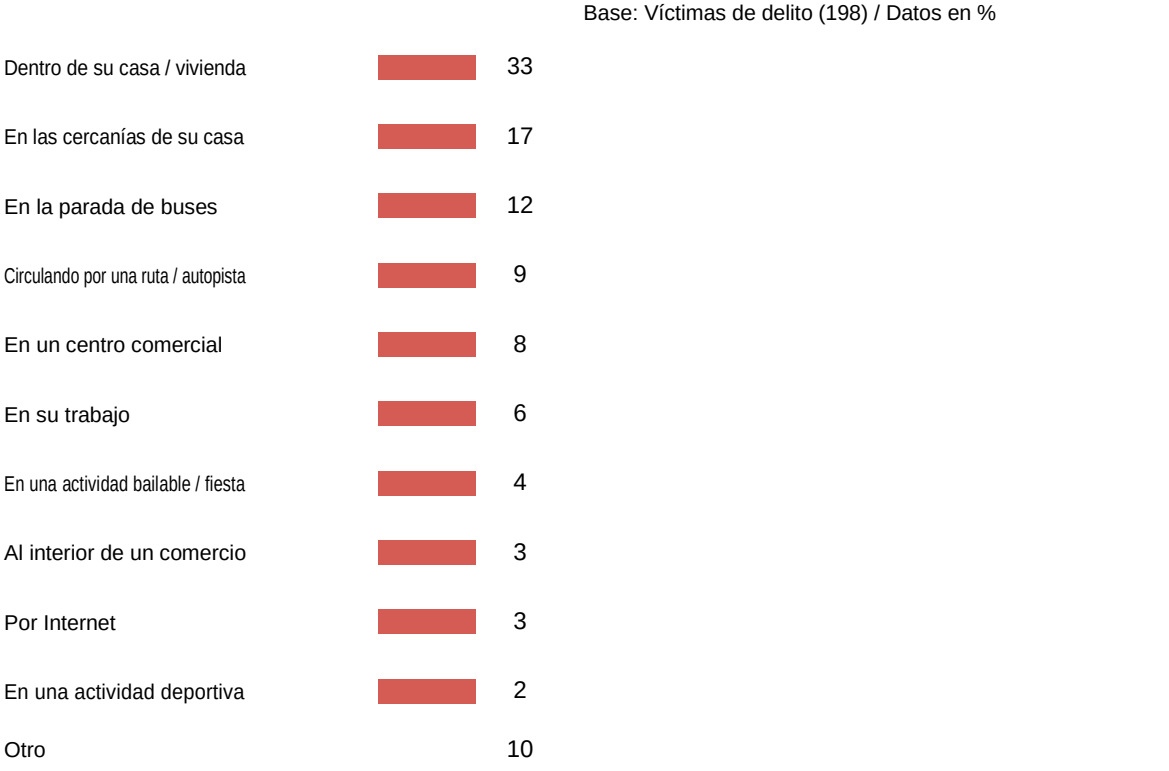
Se debe agregar, que según el VIII Informe de Seguridad Ciudadana (2017), por Cámara de Comercio Industrias y Agricultura de Panamá (CCIAP) y Programa de las Naciones Unidas para el Desarrollo (PNUD) "Las encuestas de victimización son herramientas conocidas que ayudan a los gobiernos y a su público a comprender el problema delictivo y la mejor manera de abordarlo" (p.7).

Por otra parte, este mismo informe afirma, sobre la imposibilidad de que alguna fuente provea por si sola una medición definitiva de la seguridad ciudadana, por lo que como mencionamos en líneas anteriores, es muy conocido que las cifras estadísticas policiales o judiciales, en cuanto a sus registros administrativos, no son base confiable para ofrecer por sí mismas un análisis suficientemente y exhaustivo del delito (CCIAP, PNUD 2017, p.7).

Algo semejante ocurre, con las tasas de victimización presentadas en la IV Encuesta de victimización y percepción social de la seguridad, denominada La Victimización y percepción de la seguridad ciudadana en Panamá, la cual está contenida en el VIII Informe de Seguridad Ciudadana (2017), organizado y preparado por la Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP), Observatorio de Seguridad Ciudadana, el Programa de las Naciones Unidas para el Desarrollo (PNUD), entre otras, en el cual se señala en su gráfica #8, Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples, que el 3% de los mismo fueron por Internet. (p.12)

**Figura 1**

*Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples.*




Nota: En esta figura se observa que el 50% de los casos ocurrió en la vivienda o en las cercanías a ésta. El 33% de los hechos reportados sucedió en la casa y 17% en las cercanías a la misma. Preocupa esta situación porque el hogar se

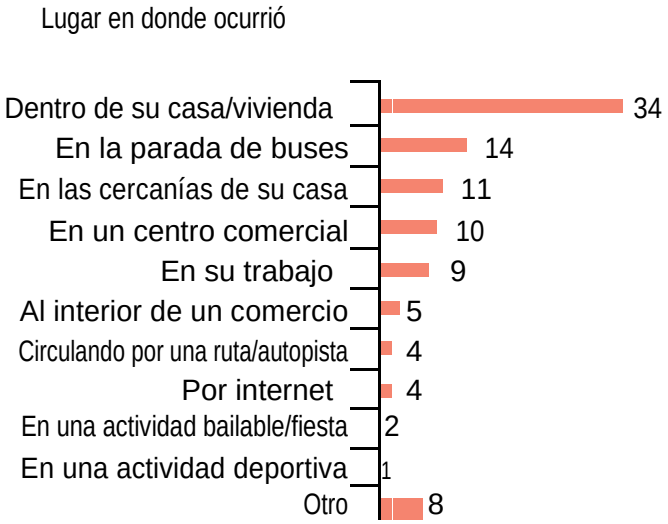
convierte en un sitio vulnerable, generando una doble victimización, debido a que involucra al sujeto residente, familiares y a la misma residencia.

En la Grafica #12, de este informe, Hurto, Lugar donde ocurrió (p.13), el 4% circulando por una ruta/ autopista y por internet, cabe resaltar que en este informe en relación con ciberdelincuencia hay muy poco aporte; podemos apreciar que los delitos ocurridos por internet no se desglosan, por lo que no podemos saber que o a cuál tipo de delito se refiere.

**Figura 2**

*Hurto, Lugar donde ocurrió.*

Base: Víctimas de hurto (103) / datos en %



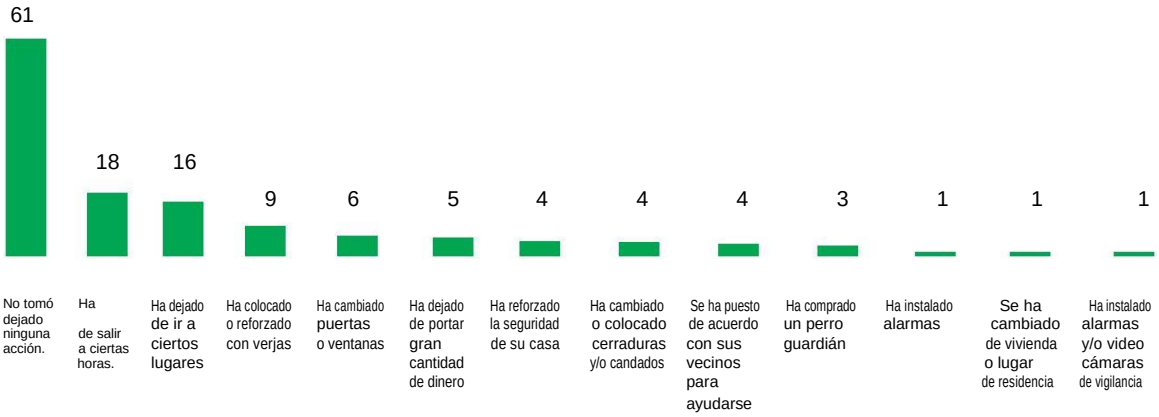

Nota: esta figura muestra las cifras por lugar donde ocurrió el delito, ya sea vivienda o en las cercanías a ésta, un 34%, 14% en la parada de buses, 10% en un centro comercial y 9% en su trabajo. En menor proporción, en el interior de un comercio (5%), 4% circulando por una ruta/autopista y por Internet, 2% en una actividad bailable o fiesta y 1% en una actividad deportiva.

Además, en cuanto a la gráfica #32, Acciones o medidas para prevenir la delincuencia (p.22), no se observa ninguna que guarde relación a la prevención de los delitos informáticos; Sin embargo, se presentan los diferentes programas de seguridad

al servicio de la ciudadanía y podemos apreciar que tampoco existe alguno que asesore, guíe o ayude a prevenir los mismos.

**Figura 3**

*Acciones o medidas para prevenir la delincuencia.*




Nota: En esta figura se observa que el 61% de las personas encuestadas no ha tomado ninguna medida de prevención. De aquellas que han toma medidas se destaca:
18% “He dejado de salir a ciertas horas”.
16% “He dejado de ir a ciertos lugares”.
9% “Ha colocado o reforzado con verjas”.
6% “Ha cambiado puertas y ventanas”.
5% “Ha dejado de portar cierta cantidad de dinero”.
4% “Ha reforzado la seguridad de su casa, cambiado o colocado cerraduras y se ha puesto de acuerdo con los vecinos para ayudarse”.
3% “Ha comprado un perro guardián”.
1% “Ha instalado alarmas, cambiado de viviendas o lugar de residencia y/o instalado alarmas o video vigilancias”.

Todavía cabe señalar, que el Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC), en su Informe de Criminalidad año (2016), señala que

> El sexto lugar de incidentes y denuncias para el año 2016, corresponden a los Delitos contra el Orden Económico: registrando 826 casos, entre los que se destacan girar cheques sin fondos, uso indebido de tarjetas de crédito o débito, blanqueo de capitales [...], por lo que podemos apreciar que en este informe

tampoco se desglosan por tipo o clase de delito informático (p.18), ver a continuación en el Cuadro N° 01, de SIEC 2016.

Al mismo tiempo, en el Cuadro N° 01. (SIEC 2016) Número, tasa y porcentaje de cambio en la tasa de incidencias y denuncias registradas en la República de Panamá por año, según clase de incidentes: años 2015 - 2016 (Continuación), si se ubica una línea para los delitos informáticos la cual señala que:" en 2016, se dio una incidencia de 35 casos en comparación con 2015, en la cual se dio una incidencia de 26 casos" (p.21).

**Tabla 1**

*Número, Tasa y Porcentaje de cambio en la tasa de incidencias y denuncias registradas en la República de Panamá por año, según clase de incidentes*: *AÑOS 2015 – 2016.*

| CLASE DE INCIDENTES Y DENUNCIAS | Años | | | | Porcentaje de Cambio en la Tasa |
|---|---|---|---|---|---|
| | 2015 | | 2016 | | |
| | Número | Tasa por 100 mil Habitantes | Número | Tasa por 100 mil Habitantes | |
| **Contra el Orden Económico** | **736** | **18.51** | **826** | **20.46** | **10.51** |
| Retención Indebida de Cuotas | 23 | 0.58 | 129 | 3.20 | 452.31 |
| Delitos Financieros | 4 | 0.10 | 0 | 0.00 | -100.00 |
| Blanqueo de Capitales | 2 | 0.05 | 60 | 1.49 | 2,854.19 |
| Derecho de Autor | 31 | 0.78 | 27 | 0.67 | -14.23 |
| Derechos de Propiedad Industrial | 33 | 0.83 | 15 | 0.37 | -55.24 |
| Girar Cheque sin Fondo | 140 | 3.52 | 159 | 3.94 | 11.84 |
| Clonación de tarjeta | 21 | 0.53 | 14 | 0.35 | -34.35 |
| Delitos Informáticos | 26 | 0.65 | 35 | 0.87 | 32.56 |
| Uso Indebido de Tarjeta de Débito | 37 | 0.93 | 182 | 4.51 | 384.38 |
| Uso Indebido de Tarjeta de Crédito | 419 | 10.54 | 204 | 5.05 | -52.06 |
| Otros delitos Contra el Orden Económico | 0 | 0.00 | 1 | 0.02 | 100.00 |

Nota: esta tabla muestra las clases de incidentes y el número de denuncias para los años 2015 y 2016 y su porcentaje de cambio en la tasa.

Más aun, en el Cuadro N° 02. (SIEC 2016) Incidencias y denuncias registradas en la República de Panamá por provincias y comarcas, según clase de incidentes: al mes de diciembre, año 2016 (p.25), muestra que, de los 35 casos, 24 fueron ocurridos en la provincia de Bocas del Toro, lo que indica que esta es la provincia con mayor número de casos o incidencias registradas, seguida de Panamá con 8 casos y las provincias de Colón, Chiriquí y Herrera con un caso respectivamente.

**Tabla 2**

*Incidencias y denuncias registradas en la República de Panamá por provincias y comarcas, según clase de incidentes: al mes de diciembre, año 2016.*

| CLASE DE INCIDENTES | Total | Provincias | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Bocas del Toro | Coclé | Colón | Chiriquí | Darién | Herrera | Los Santos | Panamá | Veraguas | Panamá | Guna Yala | Emberá | Ngäbe Buglé |
| **Contra el Orden Económico** | **826** | **27** | **47** | **93** | **63** | **0** | **30** | **12** | **455** | **33** | **66** | **0** | **0** | **0** |
| Retención Indebida de Cuotas | 129 | 1 | 22 | 53 | 6 | 0 | 20 | 6 | 1 | 16 | 4 | 0 | 0 | 0 |
| Delitos Financieros | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Blanqueo de Capitales | 60 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 60 | 0 | 0 | 0 | 0 | 0 |
| Derecho de Autor | 27 | 0 | 3 | 0 | 8 | 0 | 1 | 0 | 14 | 0 | 1 | 0 | 0 | 0 |
| Derechos de Propiedad Industrial | 15 | 0 | 1 | 0 | 2 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 |
| Girar Cheque sin Fondo | 159 | 2 | 14 | 28 | 33 | 0 | 8 | 6 | 24 | 11 | 33 | 0 | 0 | 0 |
| Clonación de tarjeta | 14 | 0 | 0 | 7 | 2 | 0 | 0 | 0 | 4 | 0 | 1 | 0 | 0 | 0 |
| Delitos Informáticos | 35 | 24 | 0 | 1 | 1 | 0 | 1 | 0 | 8 | 0 | 0 | 0 | 0 | 0 |
| Uso Indebido de Tarjeta de Débito | 182 | 0 | 1 | 1 | 4 | 0 | 0 | 0 | 162 | 1 | 13 | 0 | 0 | 0 |
| Uso Indebido de Tarjeta de Crédito | 204 | 0 | 6 | 3 | 6 | 0 | 0 | 0 | 170 | 5 | 14 | 0 | 0 | 0 |
| Otros delitos Contra el Orden Económico | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Nota: esta tabla muestra las incidencias y denuncias por clases y las cifras por provincias para el año 2016.

Seguido, el Cuadro N° 03. (SIEC 2016) Incidencias y denuncias registradas en la República de Panamá por mes, según clase de incidentes: al mes de diciembre año 2016, en el cual señala que el mes en que más incidencias se registraron fue en abril con 24, seguido de junio y septiembre con 2 respectivamente y enero, marzo, mayo, octubre y noviembre con 1 caso respectivamente.

**Tabla 3**

*Incidencias y denuncias registradas en la República de Panamá por mes, según clase de incidentes: al mes de diciembre año 2016.*

| CLASE DE INCIDENTES | Total | Mes | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Enero | Febrero | Marzo | Abril | Mayo | Junio | Julio | Agosto | Septiembre | Octubre | Noviembre | Diciembre |
| **Contra el Orden Económico** | **826** | **68** | **52** | **87** | **91** | **60** | **91** | **89** | **65** | **38** | **62** | **73** | **50** |
| Retención Indebida de Cuotas | 129 | 10 | 5 | 8 | 16 | 1 | 36 | 17 | 14 | 8 | 6 | 5 | 3 |
| Delitos Financieros | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Blanqueo de Capitales | 60 | 17 | 1 | 10 | 8 | 2 | 6 | 4 | 2 | 3 | 3 | 4 | 0 |
| Derecho de Autor | 27 | 1 | 0 | 4 | 0 | 1 | 1 | 6 | 3 | 5 | 3 | 3 | 0 |
| Derechos de Propiedad Industrial | 15 | 0 | 0 | 2 | 1 | 0 | 0 | 5 | 6 | 1 | 0 | 0 | 0 |
| Girar Cheque sin Fondo | 159 | 12 | 13 | 23 | 3 | 25 | 17 | 17 | 13 | 9 | 8 | 11 | 8 |
| Clonación de tarjeta | 14 | 2 | 2 | 4 | 1 | 1 | 2 | 1 | 1 | 0 | 0 | 0 | 0 |
| Delitos Informáticos | 35 | 1 | 0 | 1 | 24 | 1 | 2 | 0 | 0 | 2 | 1 | 1 | 2 |
| Uso Indebido de Tarjeta de Débito | 182 | 10 | 13 | 12 | 12 | 7 | 12 | 20 | 11 | 5 | 21 | 37 | 22 |
| Uso Indebido de Tarjeta de Crédito | 204 | 15 | 18 | 23 | 26 | 22 | 15 | 19 | 15 | 4 | 20 | 12 | 15 |
| Otros delitos Contra el Orden Económico | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |

Nota: Esta tabla muestra las cifras de incidencias registradas en la República de Panamá por mes del año 2016, en la que se puede apreciar los delitos informáticos.

Todas estas observaciones se relacionan con, lo que señala SIEC (2016), en su apartado titulado Delitos Contra el Orden Económico, el cual indica lo siguiente:

> Para efectos de análisis y fines consiguientes la ENVI estimó que 11,458 personas de 18 años de edad o más, fueron víctimas del delito de fraude bancario, calculando una prevalencia delictiva de 7 víctimas por cada mil habitantes, con un estimado en pérdidas de USD 9.2 millones, lo que hace obligante analizar y estudiar los actuales procedimientos internos de los cuenta habientes con el objetivo de robustecer aún más la tecnología inherente con el objetivo principal de reducir las incidencias en estos delitos. (p.116)

Habría que mencionar, además lo que señalan Shick & Toro (2017) en su apartado titulado Tendencias: principales clases de fraude en Internet

> Nuestra sociedad está cambiando significativamente a través de Internet en las maneras como comercializamos cosas, como nos comunicamos y donde conseguimos entretenimiento. Al mismo tiempo los ciberdelincuentes están utilizando los enormes beneficios de Internet para defraudar a las personas que inocentemente utilizan la red de redes como un método de comunicación y una herramienta de comercio. Los criminales de hoy han integrado métodos altamente técnicos con delitos tradicionales y han desarrollado y creado nuevos tipos de crímenes. A pesar de que es difícil para la policía aprehender y enjuiciar este nuevo tipo de delincuente, se puede afirmar que no hay diferencia significativa entre los criminales de la calle y los cibercriminales, con la excepción que los ciberdelincuentes utilizan nuevas clases de armas. Estas armas son nuevas formas de estafa en línea, entre las cuales se encuentra el *ransomware*, robo de identidad, *phishing,* la estafa nigeriana y el fraude de subastas en Internet. (p.109-110)

Ahora bien, lo señalado por Contreras et al (2019), en su apartado titulado, El Estado de la Ciberseguridad en el Sector Financiero en Latinoamérica y el Caribe del libro Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, que

> Uno de los retos, al abordar los aspectos de seguridad cibernética, es entender su dinámica y de este modo priorizar acciones para fortalecerla. A lo largo del tiempo y con la evolución de las TIC, el sector financiero, y en particular el sector bancario, ha sido una de las industrias con mayores índices de digitalización. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica,

> realizan transacciones por internet o pagos a través de dispositivos móviles y las tendencias mundiales actuales son resultado de los procesos de adaptación que se vienen requiriendo para que los mercados financieros estén en sintonía con los nuevos patrones de la economía digital (p.16, 17).

Otro punto clave es, el ampliado por Contreras et al. (2019) en el que indica que:

> Esta evolución de los modelos de negocio y el aprovechamiento de canales digitales pretenden servirse de las ventajas de las tecnologías, las cuales ofrecen ventajas invaluables, pero a la vez traen consigo la aparición de nuevos riesgos que están llamados a ser prevenidos y enfrentados con el fin mitigar los posibles ataques y situaciones de fraude a los que están expuestos actualmente el sector financiero y, por supuesto sus usuarios. (p.17)

## Formulación del problema

Por todas las situaciones antes planteadas, se da la necesidad que a través de esta investigación, se puedan brindar soluciones a las dificultades que emergen de la problemática actual de los delitos informáticos, con la finalidad de reducir o mitigar este fenómeno y su impacto a los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá y los daños económicos que estos dejan en nuestra sociedad, por lo que es preciso de alguna manera dar respuesta a la siguiente interrogante: ¿Cuáles son los tipos de delitos informáticos más comunes que impactan a los sistemas de información?, ¿Cuáles son los tipos de delitos informáticos que causan mayores afectaciones a las operaciones de banca por internet?, ¿Cuáles son los tipos de delitos informáticos más frecuentes a los servicios de banca por Internet?, además, si ¿Poseen los cuentahabientes y usuarios de la banca por Internet conocimientos sobre

los delitos informáticos que pueden afectar sus bienes?, y si ¿La entidad Bancaria o financiera donde posee su cuenta le brinda información de los riesgos producto del mal uso de la banca por Internet?.

## Justificación

Si bien es cierto, el tema de delitos informáticos no es para nada novedoso, numerosos artículos se han escrito sobre el mismo, ya que es un flagelo el cual como mencionamos con anterioridad posee una particularidad o característica intrínseca que ha heredado del gran impacto e influencia de Internet, y es que Internet, “trasciende fronteras”, por tanto, estos delitos se pueden realizar desde cualquier parte del mundo ya que usan el Internet como vehículo. Otra de sus peculiaridades es que se desarrolla a la par del dinámico crecimiento de los avances tecnológicos, de ahí que, constantemente abre el marco a la realización de nuevos estudios. Como bien sabemos, los sistemas financieros no escapan de estos impactos, lo que conocemos hoy como la sociedad de consumo hace uso de medios electrónicos o digitales para realizar sus pagos.

Es así como surgen modernos sistemas de información conocidos en nuestro país comúnmente como “Banca en línea”, los que facilitan a millones de cuentahabientes y organizaciones realizar diferentes operaciones a nivel local, regional, nacional e internacional, permitiendo el dinamismo y expansión del comercio en el plano mundial, lo que trae como consecuencia, grandes cambios en la economía de la sociedad actual.

Sin embargo, a este gran progreso tecnológico en las operaciones financieras, se le suman amenazas permanentes y cada vez más sofisticadas en cuanto a la comisión

de delitos informáticos, relacionados con el uso de los sistemas de información bancarios, afectando no sólo a las organizaciones sino a los usuarios y cuentahabientes que emplean la tecnología para sus diferentes operaciones financieras. Frente a este fenómeno, se justifica la necesidad de investigar cuáles son los principales delitos que impactan a los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá, tomando como punto de partida, la revisión de investigaciones para determinar su tratamiento a nivel internacional por parte de algunos países y organismos especializados en esta materia, su incidencia, afectaciones financieras para posteriormente examinar su tipificación en la legislación Panameña, las regulaciones por parte del centro bancario de nuestro país, máximo ente regulador la Superintendencia de Bancos de Panamá (SBP) y así determinar la influencia y daños económicos que ocasionan estos a nuestra sociedad.

Su componente teórico se enmarca en el propósito de coadyuvar al conocimiento existente, sobre los efectos que causan los delitos informáticos a los sistemas de información, a través de las operaciones de banca por Internet, ya que sus resultados podrán ofrecer guías de gran importancia, con miras a la creación de herramientas que faciliten su incorporación a un modelo, el cual apoyado de verdaderos cambios en las legislaciones y de softwares especializados, contribuyan a reforzar, mitigar y ejercer un mayor control de estos; modelo que quizás también, a futuro, sirva para detener los crímenes de esta índole, cometidos en otros campos.

La conveniencia implícita de este estudio radica en la construcción a futuro de regulaciones y controles actualizados, los cuales, a través de un modelo conceptual, contribuya a mitigar las afectaciones de los delitos ocurridos hasta hoy, y también con miras a futuro, a las operaciones financieras por medio de banca por Internet en bancos

de la ciudad de Panamá, el cual ayude a evitar pérdidas a este sector empresarial y principalmente a sus usuarios y la sociedad.

Será de gran impacto a la sociedad y el crecimiento económico de los países, ya que, al ejercer un mayor control en las operaciones de banca en línea o por Internet realizadas a través de los sistemas de información de organizaciones y cuentahabientes, se podrá mitigar el impacto de los delitos ocurridos a través de estas y por consiguiente disminuir el temor de sus usuarios, contribuyendo así a su aumento, lo que redundaría en grandes beneficios a las economías locales, regionales, nacionales y por ende mundiales, siendo un gran aporte a la humanidad.

Con los resultados de esta investigación, se podrá impulsar la creación de un moderno instrumento o método para la recolección y análisis de datos actualizados que contribuyan a nuevas investigaciones a futuro.

## Objetivos generales y específicos

### Generales

Valorar el impacto que generan los delitos informáticos en los sistemas de información contables a través de las operaciones de banca por internet en la ciudad de Panamá para lograr ejercer un mayor control de estos.

### Específicos

Identificar cuáles son los tipos de delitos informáticos que afectan los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá hasta 2020.

Analizar cuáles son los tipos de delitos informáticos más recurrentes a los sistemas de información a través de las operaciones de Banca por Internet.

Determinar la forma de mitigar los riesgos subyacentes a los sistemas de información producto de los delitos informáticos a las operaciones de banca por Internet.

## Alcance, delimitación y limitaciones

### Alcance y delimitaciones

Con la realización de esta investigación se pretende evaluar el impacto que tiene los delitos informáticos a los sistemas de información, a través de las operaciones de banca por Internet de cuentahabientes que manejen este tipo de medios o canales, solamente en la ciudad de Panamá hasta 2020, partiendo de la Identificación de los mismos y cuáles son sus afectaciones, para luego analizar cuáles son los más recurrentes y posteriormente hacer una evaluación de estos, como están tipificados en las legislaciones, acuerdos y normas de seguridad que utilizan los bancos Panameños para protección de sus sistemas de información y así sentar las bases para alcanzar nuestra meta que es encontrar una nueva forma, instrumento o herramienta, para que a futuro, a través de un modelo conceptual de sistema de información, coadyuve a mitigar estos.

## Limitaciones

Para el desarrollo de esta investigación, la principal limitación fue, la llegada a nuestro país y al mundo entero de la Pandemia denominada Covid-19, a inicios del año 2020, lo que motivo al Gobierno central de Panamá, a través del Ministerio de Salud, la presentación de medidas de restricción con el fin de mitigar los efectos causados por esta. Entre las principales medidas que se dieron y que afectaron la investigación, la cual se programó para desarrollarse en 2020, se puede mencionar el cierre de todas las actividades económicas del país por cuarentena total, el cual incluyó también las oficinas bancarias y de los usuarios de estas actividades en la urbe de la ciudad de Panamá, dificultando la toma de entrevistas y encuestas, tanto a cuentahabientes como a expertos en el tema.

## Viabilidad

Por otra parte, en cuanto a la recolección documental, las condiciones se dieron de forma favorable, ya que en este se analizaron diferentes estudios, como el denominado, Encuestas de victimización (UNODC 2013), el cual es considerado como base sólida para realizar comparaciones; y que demuestra que la victimización individual es considerablemente superior a otras formas de delitos convencionales, además, señala algunos datos o tasas porcentuales de victimización de determinados delitos informáticos (p.3); por lo que encontramos viable investigar cómo impactan estos delitos a los sistemas de información a través de las operaciones de banca por Internet, de bancos que manejen este tipo de operaciones en la ciudad de Panamá para el año 2020, ya que

estando inmersos en una sociedad de consumo, se precisa saber, ¿Cómo afectan estos a sus cuentahabientes, organizaciones y a la sociedad en sí?, insistiendo una vez más con nuestro aporte, a generar conciencia por parte de los Gobiernos, sobre la necesidad urgente de regulaciones que coadyuven a mitigar este flagelo y su contribución a nivel internacional.

## Hipótesis

Hi: La recurrencia, porcentaje, afectaciones contables y tipos de delitos informáticos, impactan los sistemas de información a través de operaciones de banca por Internet de cuentahabientes en la ciudad de Panamá.

Ho: La recurrencia, porcentaje, afectaciones contables y tipos de delitos informáticos, no impactan a los sistemas de información a través de operaciones de banca por Internet de cuentahabientes en la ciudad de Panamá.

# CAPÍTULO II

# MARCO TEÓRICO

En este apartado se desarrolla y presenta la aportación teórica o aspecto constitutivo de la investigación, producto de la revisión bibliográfica como de otros tipos de fuentes, el cual reforzará el acervo o caudal de información que nos permitirá dar solidez al trabajo.

Señala Giddens (1996) que

> Las instituciones modernas difieren de las anteriores formas de orden social, en primer lugar, en su dinamismo, fruto del cual se desgastan los hábitos y costumbres tradicionales, y, en segundo lugar, en su impacto global. Sin embargo, estas no son únicamente transformaciones extensivas: la modernidad altera radicalmente la naturaleza de la vida cotidiana y afecta a las dimensiones más íntimas de nuestra experiencia. (p.33)

## Conceptos

Para adentrarnos en los conceptos que guardan relación con esta investigación, se abordan los que se enmarcan en el contexto de esta, tomando como punto de partida el Internet, los delitos informáticos y los sistemas de información; además de otros conceptos, como comercio electrónico (e-commerce), transmisión de datos, redes de comunicación y operaciones bancarias los que se relacionan o funcionan de forma implícita dentro de los primeros.

Teniendo en cuenta esto, indica Cohen (2009), en su libro Tecnologías de Información en los Negocios, que

> Con la aparición del Internet, a principios de la década de los años noventa, las relaciones comerciales por medios electrónicos entre empresas mediante los estándares desarrollados para el servicio World Wide Web se han denotado como e-business. En un sentido general, de acuerdo con Global Business Solution, e-business es una organización que conecta sus sistemas de misión crítica con sus principales entidades (clientes, proveedores y empleados) a través de intranets, extranets y la Web. (p.61)

Según, Jeffrey Rayport, citado por Cohen (2009), el comercio electrónico se define como: "intercambios mediados por la tecnología entre diversas partes (individuos, organizaciones o ambos), así como las actividades electrónicas dentro y entre organizaciones que faciliten esos intercambios" (p.61).

Ahora veamos, lo que señala Donadío (2004), respecto a el comercio electrónico: "El comercio electrónico consiste en la transacción de compraventa a través de Internet, considerando solamente el intercambio que se produce" (p.2).

En cuanto a la transmisión de datos, señala Forouzan (2007), que: “la palabra datos se refiere a hechos, conceptos e instrucciones presentadas en cualquier formato, acordado entre las partes que crean y utilizan dichos datos” (p.3).

Amplia, Forouzan (2007), indicando que: “La transmisión de datos es el intercambio de datos entre dos dispositivos a través de alguna forma de medio de transmisión, como un cable. Para que la transmisión sea posible, los dispositivos de comunicación deben ser parte de un sistema de comunicación formado por hardware (equipo físico) y software (programas)” (p.4)

Mientras tanto, Pinilla (1994), en su apartado, Conocimiento del área de comunicación de datos, que en cuanto al hardware: “Un ambiente de comunicación de datos implica normalmente la interconexión de terminales remotas con un sistema central y/o con las diversas partes de un circuito en línea distribuido” (p.178); en lo referente al software o sistema de información, señala en el apartado el Software Operacional, que: “Está constituido por todos los programas que manejan el sistema computacional. Tales como: Los programas servidores del sistema, Los programas de carga e inicio del sistema y los programas utilitarios” (p.209).

En cuanto a, el concepto de Internet señala Forouzan (2007), que: “Internet es un sistema estructurado y organizado” […] “es una colaboración de cientos de miles de redes interconectadas” […] “Individuos privados, organizaciones gubernamentales, escuelas, centros de investigación, corporaciones y bibliotecas de más de 100 países que usan

Internet. Tiene millones de usuarios. Aunque este extraordinario sistema de comunicación se inventó en 1969" (p.15, 16).

De igual manera, señala Norton (2006) en su libro Introducción a la computación que: "Internet es una red de redes (un sistema de comunicaciones global que enlaza a miles de redes individuales)" (p.49).

Amplia, Norton (2006), reafirmando sobre el Internet:

> Actualmente, Internet conecta miles de redes y cientos de millones de usuarios en todo el mundo. Es una comunidad colaboradora enorme que no tiene un dueño. Esta falta de propietario es una característica importante de Internet, debido a que significa que no existe una sola persona o grupo que controle la red. Aunque existen varias organizaciones (por ejemplo, la Sociedad de Internet y el Consorcio World Wide Web) que proponen estándares para las tecnologías relacionadas con Internet y lineamientos básicos para su uso apropiado […] Como resultado, Internet está abierto para cualquier persona que obtenga el acceso ella. (p.51)

Ahora veamos, otro factor de mucha importancia y que representa un punto neurálgico en esta investigación, las redes de comunicación, e iniciaremos dando respuesta a la pregunta, ¿Qué es una red de computadoras?, por lo que responde Laudon & Laudon (2008), advirtiendo que: "Las redes de computadoras fueron construidas originalmente por las empresas de computación que buscaban transmitir datos entre

computadoras ubicadas en diferentes lugares" (p.262) […] amplia, "en su forma más sencilla, una red consiste en dos o más computadoras conectadas" (p.264).

En este sentido, Forouzan (2007), amplia en cuanto al concepto de redes señalando que: "Una red es un conjunto se dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red" (p.7).

En cuanto a, los delitos informáticos, la inexistencia de una definición en particular o de carácter universal para este término, ha motivado a que expertos a nivel internacional que han trabajado en el tema, formulasen conceptos funcionales en atención a realidades nacionales específicas, algunas de las cuales se señalan a continuación.

Para la organización, Cooperación Económica y el Desarrollo, citada por Temperini (2018), el delito informático se define como: "cualquier conducta, no ética, no autorizada, que involucra el procesamiento automático de datos y /o la transmisión de datos", además, Leiva, también citada en este artículo, los define como: "…Toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma" (p.54)

Conviene subrayar, en lo que se refiere a las definiciones que se han intentado dar en México, la de Téllez (2008) la cual señala que

> Dar un concepto acerca de delitos informáticos no es labor fácil, debido a que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión 'delitos informáticos' esté consignada en los códigos penales, lo cual, en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún. (p.187)

Para Sarzana, citado por Estrada (2008), en su obra Criminalita e Tecnología, "los crímenes por computadora comprenden, cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo" (p.4).

Callegari, también citada por Estrada (2008), define al delito informático como: "aquel que se da con la ayuda de la informática o de técnicas anexas" (p.4).

Fernández Calvo citado por Estrada (2008) define al delito informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española" (p.4).

Lima citada por Estrada (2008) manifiesta que “el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin” (p.4).

Como señala, Estrada, y en vista de que, cada uno de los autores mencionados con anterioridad conceptualizan o definen el delito informático de manera conducente a un concepto general: “son acciones delictivas las cuales se dan con la ayuda de la informática o de técnicas modernas anexas”, para el desarrollo de esta investigación presentamos nuestra definición de delitos informáticos como: “Cualquier comportamiento o conducta ilícita en la que están involucradas las computadoras, software o cualquier medio tecnológico con la finalidad de afectar a estos o a datos contenidos en estos, teniendo como consecuencia daños o lesiones a bienes ajenos”.

En cuanto a, los sistemas de información, “Un sistema es un conjunto de elementos, entidades y componentes que se caracterizan por ciertos atributos identificables que tienen relación entre sí y que funcionan para lograr un objetivo común” (Catacora, 1997, p.25).

Por otro lado, “Los sistemas de información permiten que las personas, la tecnología y la información se integren de manera coordinada para producir conocimiento de manera relevante y oportuna” González et al. (2010).

Para el desarrollo de esta investigación, presentamos nuestra definición de sistemas de información como: “Conjunto de elementos estrechamente correspondientes entre sí, con un fin colectivo”.

Otro punto es, las operaciones bancarias, factor de mucha relevancia en esta investigación, por lo que presentamos algunos conceptos que se manejan conexos a este, como lo son: Sistema financiero, operaciones o transacciones y riesgos.

Por lo que, Mercado (2014) define sistema financiero como el “conjunto de instituciones, mercados y normas que permiten captar y administrar el ahorro de los agentes económicos para ser canalizados hacia la inversión y el consumo de empresas, familias y gobiernos” (p.50).

Por otro lado, De Latouche & Maldonado en su libro Estudio de la Contabilidad General (2013), definen las operaciones bancarias como: “todas aquellas operaciones de crédito practicadas por un banco de manera profesional, como eslabón de una serie de operaciones activas y pasivas similares” (p.97).

De manera semejante, Paz (2015), en su apartado, Transacciones comerciales y sus registros, define la transacción como: “La actividad o acontecimiento que se da en un negocio o empresa. Ejemplo: ventas al contado o a crédito, compras al contado o a crédito, etc.” (p.100).

En relación con, las operaciones de banca electrónica, la Superintendencia de Bancos de la República de Panamá, define en su tabla Ban08 de Banca Electrónica, Glosario de Términos (2014) Ver cuadro# 16, como

> La prestación de servicios bancarios a través de medios o canales electrónicos, la cual involucra los servicios ofrecidos por: Banca por Internet, Banca Móvil, Banca por teléfono, Terminales de puntos de venta (POS), Mensajería instantánea (Chat), Redes sociales, Correo electrónico, firma electrónica, dinero electrónico, red ACH, redes especializadas, Cajeros automáticos, monedero o pago móvil, tarjeta bancaria con circuito integrado, medios de pago electrónico cualquier otro medio o canal electrónico. (s.n.)

Acorde a, todo lo antes señalado, se define para esta investigación los sistemas financieros, como: “todo aquel establecimiento autorizado que se dedica a absorber ahorros de diferentes entes económicos los cuales con posterioridad serán utilizados en inversiones y consumo en la sociedad, en el que se dan todas aquellas operaciones de crédito activas y pasivas similares”.

Habría que decir también, que, según Mercado (2014), “los activos bancarios están sujetos a diferentes tipos de riesgos […] los que provienen de fraudes, errores, omisiones, ineficiencias, fallas en los sistemas, realización de actividades no autorizadas (riesgo operacional)” (p.104).

A su vez, Mercado (2014), define el riesgo operacional como:

> La pérdida potencial por fallas o deficiencias en los controles internos, por controles en el procesamiento y almacenamiento de las operaciones o en la trasmisión de información, así como por resoluciones administrativas y judiciales adversas, fraude o robos y comprende, entre otros, al riesgo tecnológico y al riesgo legal, en el entendido que el riesgo tecnológico se define como la perdida potencial por daños, interrupción, alteración o fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información en la prestación de servicios bancarios a los clientes de la institución. (p.105)

En cuanto a, lo que respecta al estudio del fraude, señala Arens et al (2007), que este, desde el punto de vista de la auditoría financiera se define como:

> Si bien el fraude es un concepto legal amplio, en el contexto de la auditoría de estados financieros, el fraude se define como un error intencional en los estados financieros. Las dos principales categorías de fraude son: informes financieros fraudulentos y malversación de activos (p.314).

Mientras tanto, Arens et al. (2007), destaca que

> La malversación de activos es el fraude que involucra el robo de los activos de una entidad. En varios casos, las cantidades involucradas no son materiales para los estados financieros. Sin embargo, la pérdida de los activos de la compañía es una preocupación importante de la administración, […] El término de malversación de activos, por lo general, se utiliza para referirse al robo que involucra a empleados y otras personas dentro de la organización. Por ejemplo, la Association of Certified Fraud Examiners estima que el promedio que la compañía pierde por fraude es el 6% de sus ingresos. (p.314)

Respecto a lo anterior, señala Arens et al. (2007), en su apartado titulado, Mitigación de los riesgos de fraude que: “La administración es responsable de diseñar y aplicar programas y controles para mitigar los riesgos de fraude. La administración puede cambiar las actividades de negocios y procesos propensos al fraude con el propósito de reducir incentivos y oportunidades para el fraude” (p.325).

En síntesis, se puede observar que los activos de las entidades del sistema financiero, llámese los bancos, son objeto de diferentes tipos de riesgos entre los cuales los que repercuten en nuestra investigación son los definidos con antelación como riesgo operacional. Además, dentro de este, hay una clasificación en la que se menciona de forma directa los delitos a clientes del sistema financiero por la prestación de servicios bancarios, denominada riesgo tecnológico; en base a esta, nuestra definición será: “todo aquel desperfecto, perjuicio, obstáculo que en

consecuencia afecte la transferencia de información de los servicios bancarios a clientes de la entidad, a través de su hardware, software, sistemas de información redes entre otras relacionadas".

## Características de delitos informáticos y operaciones bancarias

Por lo que se refiere a, los delitos informáticos podemos señalar algunos rasgos característicos como: son comportamientos en el que la computadora o cualquier medio tecnológico, ya sea software o hardware y cualquiera de sus funciones han estado involucradas y en el que se tiene como consecuencia daños a bienes ajenos.

Con respecto a, las características de las operaciones bancarias, añade Mercado (2014) que "los mercados financieros están constituidos por espacios físicos y virtuales (teléfono, fax, diversos medios informáticos y telemáticos)" […] (p.51), por lo que podemos con este señalamiento afirmar la existencia de un vínculo entre los sistemas financieros y los espacios virtuales, el cual ampliaremos en líneas posteriores.

## Tipos de delitos informáticos

En relación con lo anterior, Téllez (2008) presenta los tipos de delitos que son reconocidos por la Organización de las Naciones Unidas (ONU) (p.193), los cuales se detallan a continuación:

**Manipulación de los datos de entrada:** este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de estos.

**La manipulación de programas**: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

**Manipulación de los datos de salida:** se efectúa fijando un objetivo al funcionamiento del sistema informático.

**Fraude efectuado por manipulación informática:** aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

**Como objeto:** cuando se alteran datos de los documentos almacenados en forma computarizada.

**Como instrumentos:** las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas.

Daños o modificaciones de programas o datos computarizados.

**Sabotaje informático:** es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

**Virus:** es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

**Gusanos:** se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

**Bomba lógica o cronológica:** exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

**Acceso no autorizado a servicios y sistemas informáticos**: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

**Piratas informáticos o hackers:** el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso.

**Reproducción no autorizada de programas informáticos de protección legal:** ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

**Acceso no autorizado:** uso ilegitimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.

**Destrucción de datos:** los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

**Infracción al copyright de bases de datos:** uso no autorizado de información almacenada en una base de datos.

**Interceptación de correo electrónico**: lectura de un mensaje electrónico ajeno.

**Estafas electrónicas:** a través de compras realizadas haciendo uso de la red.

**Transferencias de fondos:** engaños en la realización de actividades bancarias electrónicas.

**Espionaje**: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

**Terrorismo:** mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

**Narcotráfico:** transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

**Otros delitos:** las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

Otros autores como, Shick & Toro (2017), presentan algunas definiciones para algunos de los delitos catalogados como los más comunes a las operaciones de banca por Internet. Señala que el delincuente utiliza nuevas clases de armas por lo que:" Estas armas son nuevas formas de estafa en línea, entre las cuales se encuentran el *ransomware,* robo de identidad, *phishing,* la estafa nigeriana y el fraude de subastas en Internet" (p.110).

**Fraude contra el reloj-(ransomware).** el fraude por Internet generalmente se refiere a cualquier tipo de esquema de fraude que combina uno o más aspectos de

la funcionalidad de Internet (por ejemplo, salas de chat, correo electrónico, tableros de mensajes o sitios web). El fraude en Internet puede tomar diferentes formas, como presentar solicitudes engañosas a posibles víctimas, realizar transacciones falsas o transmitir el producto de una estafa a instituciones privadas o públicas y a particulares.

**Robo de identidad.** El robo de identidad es una forma específica de fraude que implica el uso ilegal de los datos personales de alguien, tales como nombre, números de documentos de ciudadanía o licencias de conducir para obtener dinero, mercancía o servicios por engaño, y requiere uso ilegal en la identificación robada que pertenece a otra persona (Flinkea 2010), citado por Choi (2017).

**Phishing.** Actualmente el *phishing* es uno de los métodos de obtención de datos personales más rápidos y proliferantes en fraudes. Los correos electrónicos de *phishing* involucran nuestra principal herramienta de comunicación unido a técnicas de ingeniería social, con lo cual apuntan a usuarios en línea que no sospechan sobre las intenciones criminales al responder un mensaje no solicitado con información personal.

**Fraude de subasta en Internet.** Estos esquemas de fraude de subastas, y esquemas similares para los productos al por menor en línea, típicamente pretenden ofrecer artículos de alto valor, que van desde ordenadores portátiles a objetos coleccionables, tales como sellos raros o monedas. Estos últimos, usualmente atraen muchos consumidores. Estos planes inducen a sus víctimas a enviar dinero por los artículos prometidos, pero luego no entregan nada o solo un artículo mucho menos valioso de lo que se prometió, incluyendo productos falsificados o alterados.

## Evolución de la temática

Para dar seguimiento al análisis, en la actualidad, la utilización de redes de comunicación como de sistemas de información ha sido toda una revolución, su creciente vínculo trasciende las fronteras de los países, proporciona ventajosas e incalculables oportunidades, espacio a diferentes ámbitos de la vida y negocios cada vez más diversos, entre otros, lo cual ha contribuido a lo que hoy día conocemos como “Globalización”; pero también existen desventajas y riesgos, producto de la característica intrínseca que posee el Internet, la inexistencia de fronteras, la cual crea una coyuntura para que cibercriminales puedan realizar diferentes comportamientos antisociales y el desarrollo de novedosas y complejas formas de infringir la Ley, entre los que figura como principal las agresiones mal intencionadas a los sistemas de información, sumado a estos señala González (2013), en su investigación doctoral para la Universidad Complutense de Madrid, que

> El comercio electrónico va superando las barreras impuestas por una sociedad clásica que desconfía de los cambios -cuyas dudas sobre los nuevos modos de actuar no son siempre infundadas- y está convirtiéndose cada día más en una práctica habitual, de la que cabe esperar que tarde o temprano sustituya completamente al comercio tradicional. Mucho se ha desarrollado el campo relativo a la seguridad en la red a través de diferentes técnicas, pero no podemos olvidar que tales avances no impiden la aparición de nuevas formas de criminalidad sujetas al propio progreso tecnológico. Han aparecido nuevos sujetos que están dispuestos a utilizar en su beneficio (entendido en un sentido amplio) este mundo que, a pesar del tiempo transcurrido, parece que todavía sigue dando sus primeros pasos. (p.8)

Dicho lo anterior, se hace referencia a la Teoría de la modernidad como sustento para esta investigación, iniciando con una visión retrospectiva de Bula (1994), en su publicación "John Rawls y la teoría de la modernización. Una retrospectiva analítica", que

> La modernización, en tanto proceso evolucionista de las sociedades humanas, se basa en lo que algunos autores llaman evolucionismo social [Tipps 1976, Hulme y Turner 1990] o darwinismo social [Huntington 1976, Mazrui 1968], concepto que se insinúa, ya en los siglos dieciocho y diecinueve, en los trabajos de Kant y Hegel [Smart 1991, 17]. En el Origen de las Especies, Charles Darwin concebía la evolución como un proceso de transformación desde las formas más simples a las especies superiores más desarrolladas. Su trabajo influyó en las reflexiones de los evolucionistas sociales, quienes consideraban que las sociedades evolucionaban de las formas más arcaicas hacia las más desarrolladas y que las sociedades occidentales habían alcanzado un carácter universal que rompía el particularismo de las tradicionales y pre-modernas. (p.70)

Igualmente, Bula (1994), señala que entre los principales aspectos de la Teoría de la Modernización esta

> La modernización se entiende como el proceso que lleva las sociedades tradicionales hacia la modernidad y que se refleja en una serie de cambios generales: urbanización, industrialización, secularización, racionalidad, diferenciación social, aumento del alfabetismo, extensión de los medios de comunicación, mayor control del entorno natural y social, crecimiento económico, una más compleja división del trabajo, un desarrollo político expresado en mayor movilización social y mayor participación política. Estas serían las principales

> características del advenimiento de la modernidad [Huntington 1976, 28-29; Leys 1982, 333-334; Tipps 1976,65-67; Harrison 1988, 15-17]. (p.71,72)

Simultáneamente, los postulados de la Teoría de la Modernidad y Reflexividad de Giddens, citado por Carreño, (2015), profundizan y caracterizan la modernidad, señalando que: “asume los temas de *seguridad* frente al *peligro* y *fiabilidad* frente al *riesgo* como dos componentes que conllevan un costo de oportunidad en la vida moderna. Además, advierte sobre el enorme potencial destructivo de la misma” (p.95).

De ahí que, Giddens, citado por Carreño (2015), en otro de sus postulados señala que

> La modernidad no es la búsqueda permanente de lo nuevo, sino la aplicación del conocimiento reflexivo a la propia sociedad. La reflexión en la vida social moderna consiste en el hecho de que las prácticas sociales son examinadas constantemente y reformadas con base en la nueva información sobre las propias prácticas, y de esta manera las prácticas modifican su carácter constituyente (p.95).

De manera que, se respalda la investigación en esta teoría, ya que nos ayuda a dar base o sustento, ya que los delitos informáticos son malas y modernas prácticas sociales, las cuales desde hace mucho vienen siendo examinadas y estudiadas con la finalidad de modificar su carácter integrante a través de regulaciones y leyes que mejoren o transformen este tipo de conductas.

Es así como, sobre lo antes señalado, amplia Giddens citado por Carreño (2015) indicando que

> Las estadísticas sobre la sociedad no son sólo un instrumento para conocer esa realidad y por ello para controlarla mejor –como ocurre en el caso de la naturaleza-, sino que sus resultados se incorporan al hacer cotidiano de las personas objeto de estudio. El conocimiento que producen los científicos sociales, una vez apropiado por las organizaciones e instituciones, pasa a constituir lo social, contribuyendo así a su reestructuración y transformación. (p.95)

En definitiva, Giddens citado por Carreño (2015) “precisa que esta reflexividad o circularidad del conocimiento hace que el mundo social moderno no pueda ser estable, debido a la permanente incorporación de nuevos conocimientos” (p.95).

Como causa de los anteriores señalamientos, los gobiernos han tenido que hacer frente a esta circunstancia aportando respuestas expeditas que faciliten la protección de los usuarios, tanto empresas como particulares; es por ello que en su teoría, citada en el párrafo anterior, Giddens afirma la inestabilidad del mundo social moderno, es por ello que, la evolución de los delitos informáticos producto de los grande avances tecnológicos, hace que la sociedad este constantemente ingresando nuevos conocimientos en la búsqueda de su reestructuración o transformación.

Se ha procurado que, dicha transformación o respuestas se den en forma de regulaciones, las cuales representan para este estudio uno de los factores fundamentales en la problemática de los delitos informáticos y que desde hace mucho tiempo se han

tratado de unificar con el fin que exista una misma normativa para todos los países. Es por ello, que el Consejo de Europa asumió este reto, el cual fue aceptado por muchos de los países de ese continente como de América, tratando así de buscar solución para mitigar el problema de la supranacionalidad (Consejo de Europa, 2001), del cual se profundiza en líneas posteriores.

Teniendo en cuenta que, de acuerdo con el estudio exhaustivo realizado por la (UNODC 2013), relacionado a esta temática, “el verdadero foco del problema son los países menos desarrollados, pues estos son los mayormente vulnerables al cibercrimen” (p.2).

Respecto a ello, fue aprobado por este consejo en noviembre de ese mismo año, lo que hoy conocemos mundialmente como el Convenio de Budapest, o convenio sobre la Ciberdelincuencia, el cual representa el primer intento internacional de unificar y regular los delitos cometidos en el ciberespacio y que pretende entre sus objetivos principales la creación de estándares en materia de Derecho Penal, el establecimiento de adecuadas normativas y procedimientos al entorno digital y la formulación de mecanismos para la cooperación internacional en esta materia, con la finalidad única de establecer criterios para la investigación y persecución de estos delitos en todo el mundo, creando un marco regulatorio en aspectos del Derecho, lo que facilitará en su momento la persecución penal y su debida sanción (Consejo de Europa, 2001).

Ahora se presenta brevemente, un análisis específico de algunos países que presento Rojas-Parra (2016), en el que muestra mucha información relevante para este

estudio, la cual profundizaremos en líneas posteriores de la investigación, por el momento solo mencionaremos algunos países a nivel internacional y de la región, iniciando con España, en el que señala lo siguiente

> España es un modelo de referencia en este campo, debido a su condición de Estado miembro del Concejo Europeo, firmó el convenio del cibercrimen el 23 de noviembre del 2001, realizando su última ratificación el 3 de junio de 2010, y entrada en vigor el 1.º de octubre del mismo año. Además, señala que: "El delito informático con mayor pena de prisión en este país es la "Alteración, copia, reproducción o falsificación de tarjetas de crédito o débito o cheques de viaje (Verdú, 2005; Vergel, Martínez, Zafra, 2014); así como la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de la conducta referida (las Cortes Generales y el rey de España, 1995). (p.221)

Por otra parte, República Dominicana es el primer país latinoamericano en ratificar el Convenio sobre la Ciberdelincuencia, debido a que a principios de 2013, ratificó su adhesión como Estado no miembro del Consejo de Europa, convenio que entró en vigor en junio del mismo año, siendo a partir de ese momento un modelo para Sur y Centroamérica. (Rojas-Parra, 2016, p.221)

No solo sino también, Rojas-Parra (2016), afirma que, aquellos delitos informáticos con mayor pena de prisión en ese país son

> El sabotaje, espionaje o suministro de informaciones, a través de un sistema informático, electrónico, telemático o de telecomunicaciones, atentando contra los intereses fundamentales y seguridad de la Nación […] además de ejercer actos de terrorismo, con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones (Congreso Nacional de la República Dominicana, 2007). (p.222)

Se debe mencionar, además que, México fue invitado a adherirse al Convenio de Budapest, adhesión pendiente debido a que cuenta con el Estatuto de Observador ante el Consejo de Europa desde 1999, lo que le ha permitido tanto la realización de reformas constitucionales en telecomunicaciones, estrategias digitales nacionales, como ganar experiencia en el Comité Especializado en Seguridad de la Información del Consejo de Seguridad Nacional, y que en este país, el delito informático con mayor pena de prisión es: Transmitir, elaborar, reproducir, vender, arrendar, exponer o publicitar material que contenga grabaciones de actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de 18 años (Gobierno de México, 2007)" (Rojas-Parra, 2016, p.224).

En cuanto a Panamá, se puede señalar que, su legislación da protección al sistema financiero, la cual está contenida en el Capítulo III, titulado Delitos Financieros,

Artículo 243, comentado por Candanedo (2016), en el Texto Único del Código Penal de la República de Panamá, en el que se señala lo siguiente

> Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita o haga uso indebido de dinero, valores u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que se le hayan confiado, o realice esas conductas a través de manipulación informática, fraudulenta o de medios tecnológicos, será sancionado con prisión de cuatro a seis años. La sanción será de seis a ocho años de prisión, cuando el hecho punible es cometido por un empleado, trabajador, directivo, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno. (p.194)

Por otra parte, y para dar continuidad al análisis de nuestra legislación, señala Parodi (2014), en su examen al artículo 243, lo que considera un hecho contradictorio de este y algunos elementos que deben ser considerados por los operadores de justicia, los cuales se presentan a continuación:

(a) La protección de esta norma al sistema financiero es tan amplia que puede abarcar fraudes informáticos que conlleven desde el apoderamiento de recursos financieros y falsedad de documento, hasta hurtos con abuso de confianza. Destacamos el hecho que, si bien en un principio la penalidad era elevada con respecto a las tipologías tradicionales (hurto, estafa y falsedad), dicha situación ha cambiado, toda vez que el hurto con abuso de confianza, la estafa y la falsedad de documento, tienen penas hasta de diez años de prisión,

y el delito financiero hasta 8 años, lo que a mi concepto entra en contradicción con el interés de la creación de la norma, que estaba dirigida a tipificar conductas tradicionales, bajo un paraguas especial con penas más graves, en vista de la importancia o el perjuicio colectivo que involucraba su infracción. Y es que si un sujeto cometiese un fraude en perjuicio de un banco o empresa financiera superior a B/.100,000.00, la pena máxima a imponer sería la de 8 años y no la de 10 años que establece el tipo tradicional de estafa; igual situación ocurre con el apoderamiento de dinero que entregan los clientes a una institución bancaria, sustraídos por parte de un empleado del banco utilizando ocultamiento de información o presentación de informes falsos, conducta que entraría fácilmente dentro de los delitos financieros y no bajo los tipos tradicionales de hurto con abuso de confianza cuya penalidad máxima es superior a la del delito financiero. (p.94)

(b) el significado de “recurso financiero”, toda vez que el tipo penal hace referencia a dineros y valores e equipara el mismo al concepto de recursos financieros, el cual se refiere a las fuentes de financiación, recogidas en el pasivo de una empresa, que se materializan en inversiones o activos de está. ¿En qué se traduce esto dentro del ámbito penal? En que solo los dineros y valores que están relacionados con una fuente de financiación han de ser objeto de los delitos financieros; y es que los tipos penales relativos a los delitos financieros tienen como fin primario proteger a los ahorradores, que han confiado su dinero a las entidades financieras a través de figura de captación de dinero, que se dan a través de operaciones crediticias en las que la entidad financiera acepta recursos de los particulares para luego utilizar los mismos en otra operación crediticia en la cual funge como acreedor, he ahí la clave de la función intermediadora de las entidades financieras. (p.95)

(c) En este orden de ideas, cobra importancia el conocimiento de los “contratos bancarios”, ya que si bien, pareciera ser similar el depósito bancario a la figura del depósito tradicional, en realidad estamos frente a una figura jurídica distinta, que algunos han señalado que debe ser denominada de otra manera y que hoy de manera doctrinal se ha identificado como “contrato de depósito irregular” para diferenciarlo del depósito regular, identificado como aquél contrato en el cual una persona entrega una cosa mueble a otra para que esta la conserve en su poder y se le restituya cuando el depositante así lo requiera. En esa línea, el depositario no puede usar el bien que se ha recibido, pero sobre todo no puede consumirlo, ni disponer del mismo, contrario al depósito irregular llamado “depósito bancario” en el cual el depositario adquiere la propiedad de los bienes que recibe y puede disponer libremente de ellos, quedando solo obligado a devolver una cantidad equivalente. (p.95)

Con todos los elementos antes presentados, Parodi (2014), nos ofrece su observación de la siguiente forma:

Explicada la división anterior, se observa entonces que cuando el depositante o ahorrador entrega dinero a un banco bajo el marco de figura jurídica conocida como “contrato de depósito bancario”, lo que hace en realidad es una operación de crédito, en la cual el deudor es el banco y el acreedor el depositante o ahorrista, en la que este último traspasa la propiedad del dinero o título valor dado en depósito, a cambio que le devuelva una cantidad equivalente y del mismo valor en un determinado tiempo, que puede ser a la vista o a un plazo determinado. Explico todo esto para dar paso a la siguiente relación casuística, y es que hay quienes consideran que si por la razón que sea una persona logra penetrar en la cuenta bancaria de una persona ya sea natural o jurídica y le sustrae X cantidad de dinero, el perjudicado

> directo es el cuentahabiente o ahorrista; no obstante, no toman en cuenta que el ahorrista tiene a través de esa cuenta bancaria no una suma de dinero, sino un crédito a su favor que puede ser cobrado según las circunstancias del contrato y que el hecho que se haya vulnerado la cuenta bancaria por algún fraude no debe de ser interpretado como el apoderamiento de dinero del ahorrista, sino a la institución financiera afectada, que indirectamente en atención a la operación de crédito existente con el cliente y el banco resulten perjuicios al ahorrista que igualmente se convierte en víctima, el principal afectado es el banco, ya que independientemente de la afectación debe honrar sus compromisos con el cuentahabiente, salvo que la contratación establezca elementos distintos. (p.95)

Visto desde otra perspectiva, las normativas legales que se enmarcan en nuestro país para hacerle frente a los delitos informáticos, indican, de acuerdo al análisis anterior, que el principal afectado, en la eventualidad de delitos financiero, debería ser el banco y no así los ahorristas, pues a todas luces se da la existencia de un contrato que le otorga a este último un crédito con la entidad financiera y al primero una responsabilidad o compromiso que debe honrar al cuentahabiente o ahorrista.

El siguiente punto trata de, las normativas que existen en Panamá, para hacer frente a los delitos informáticos, por lo que, en materia internacional, este forma parte de los cuatro primeros países del continente americano en estar adherido y ratificado al convenio de Budapest. En particular, la Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013, que fue publicada en la Gaceta Oficial No. 27403-A del 25 de octubre del mismo año, su texto, aprobado sin restricciones ni modificaciones y posteriormente depositado el

documento de adhesión ante la Secretaría del Consejo Europeo, convierte a nuestro país en el segundo en Latinoamérica en ratificar este, después de República Dominicana.

Por lo que señala Rojas-Parra (2016), que

> El Código Penal de Panamá, adoptado por la Ley 14 de 2007, con las modificaciones y adiciones introducidas por las leyes 26 de 2008, 5ª de 2009, 68 de 2009 y 14 de 2010, tipifica, principalmente, los delitos informáticos en su título VIII, "Delitos contra la seguridad jurídica de los medios electrónicos", regula los delitos contra la seguridad informática. Del artículo 289 al 292 encuadra 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. (p.222)

También, advierte Rojas-Parra (2016), sobre los delitos informáticos con mayor pena de prisión para nuestro país, los cuales son:

> Fabricar, elaborar, producir, ofrecer, comercializar, exhibir, publicar, publicitar, difundir o distribuir a través de Internet o de cualquier medio masivo de comunicación o información, material pornográfico; presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, reales o simuladas (Gobierno de Panamá, 2010), y Utilizar Internet, para el entrenamiento en la construcción de artefactos explosivos o el reclutamiento de

> personas, para la ejecución de actos con fines terroristas (Gobierno de Panamá, 2010, p.222).

Se debe agregar que, según Fratti (2018), en su artículo, Un país con la necesidad de una legislación sobre cibercrimen, señala que

> Factores como las categorías inadecuadas de los tipos penales que van de la mano con las exigencias de la gran demanda de nuevas conductas que no se encuentran reglamentadas, traen como consecuencia que no se puede cumplir con el desarrollo de investigaciones dentro de procesos penales y el logro de imposiciones acordes a dicha conducta debido a que no contamos con mecanismos correctivos que imponga una sanción luego de una investigación. Se debe agregar que, el impedimento de solicitar colaboración o ayuda a otros Estados, pues dentro de la legislación nacional no se encuentren regulados estos tipos penales y la carencia de un marco jurídico de protección de datos personales, el cual se encuentra todavía en discusión en su comisión correspondiente, agrega otro vacío por resolver. (p.4)

Todavía cabe señalar que, según Fratti (2018)

> La falta de preparación y capacidad adecuada para la investigación criminal de delitos realizados por medios tecnológicos ha generado que Panamá, a través del Ministerio Público, estableciera como mecanismos de investigación y persecución penal en materia de ciberdelincuencia los estándares usuales aplicados a delitos comunes"; dicho de otra manera, lo que señala Fratti es que se pierden las características y el elemento definitivo de ciberdelincuencia, por el hecho de

> fiscalizar una actuación común; Sin embargo, añade que esto únicamente puede realizarse en aquellos actuares que constituyen un delito, sin la componenda de su particularidad digital. Como consecuencia, aquellos delitos que se desarrollan en el marco del ciberespacio, por su naturaleza, no pueden ser investigados ni juzgados bajos sus parámetros específicos en Panamá. (p.4)

El ejemplo, que a continuación subraya Fratti (2018), basta para ilustremos lo dicho con anterioridad

> En el caso de la captura ilegal de datos bancarios *(phishing o pharming*) bajo la conceptualización de los verbos rectores del tipo penal, en la actual legislación panameña, no podría ser sancionado el mero hecho de la captura ilegal de los datos personales, se debe esperar a que el delincuente utilice la información obtenida de manera ilegal, para que el Ministerio Público de Panamá tenga la capacidad legal de iniciar el proceso de investigación por el delito. (p.4)

Todo lo presentado anteriormente, es esclarecido con lo presentado por Parodi (2014), en su apartado Breve análisis de los principales delitos financieros en Panamá, en el cual afirma que

> Desde el punto de vista de represión penal en Panamá, se tiene la idea que el delincuente de “cuello blanco” regularmente actúa impunemente, en vista de las deficiencias del sistema normativo represivo, que resulta inaplicable e ineficaz, sumado al hecho que nuestro sistema penal, al igual que el de la mayoría de otros

> países, es criticado por ser de corte clasista ya que reprime severamente los delitos que son llevados a cabo por delincuentes con carencia económica y con niveles bajos de educación; sin embargo, es benigno y a veces nulo con la delincuencia practicada por antisociales que presentan un buen nivel económico y social. (p.93)

Todo esto parece confirmar, la evidente falta de realización de un análisis exhaustivo a nuestras normativas, tomando en consideración los factores antes señalados, por lo cual Parodi (2014), amplia indicando que

> La incorporación en nuestra norma penal de los delitos financieros, no es más que las experiencias vividas por el país en esta materia, por lo que la tipificación de conductas penales ha de ser un traje a la medida de las necesidades de nuestra plaza financiera; y es que hemos incorporado en nuestra norma penal conocidos fraudes financieros que si bien fueron enmarcados dentro de tipos comunes como estafa y falsificación, los mismos fueron ineficientes si tomamos en cuenta el daño causado y la complejidad de la adecuación de la conducta al tipo. Los delitos financieros no tienen como principal objetivo −aunque algunos así lo piensen− proteger los intereses de un banco o de una entidad financiera en particular, sino los dineros de los ahorradores representados por créditos a su favor, y también la confianza en el sistema financiero panameño. (p.93)

Todas estas observaciones se relacionan con, otros resultados de la investigación de Temperini (2013), en la cual afirma que

> a) los países latinoamericanos presentan una falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos. b) Que, los países latinoamericanos han optado por diferentes posturas con relación a sus formas de regular. Algunos han optado por la sanción de leyes especiales, donde en los casos más destacados (caso de República Dominicana) incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso se han generado los organismos dedicados a su investigación y persecución. Otros tantos países (mayoría) han optado por modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos. c) Que la falta de armonización reconoce diferencias en dos niveles. En el primero de ellos, se puede observar diferencias entre los países sobre los criterios políticos para la consideración sobre si tal acción lesiva debe ser o no sancionada como delito penal. En un segundo nivel, dentro de aquellos países que han dado respuesta positiva al primer nivel, pueden observarse diferencias en cuanto a los criterios penales considerados como necesarios para la configuración del tipo. d) Que se destaca la necesidad de mejorar los niveles de armonización y actualización legislativa en la materia, a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia. (s.n.)

En definitiva, y como señala Concepción (2014), ha y que destacar que

> La fenomenología delictiva vinculada a las nuevas tecnologías de la información y las comunicaciones es cada vez más variada y abundante y que cualquier

> regulación queda pronto anticuada, porque sus formas de perpetración van cambiando con el tiempo adaptándose a las nuevas posibilidades que ofrece el estado de la técnica. Ciertamente la realidad delictiva siempre va por delante de la regulación legal y la correspondiente sanción punitiva de las conductas reprobables pero, en estos casos en los que intervienen las nuevas tecnologías, muchísimo más dada la rapidez del desarrollo tecnológico, la facilidad del intercambio de la información, la comunicación inmediata entre lugares lejanos, la fugacidad de las acciones y la facilidad para conseguir su anonimato, la dificultad para identificar las huellas digitales, la fácil alteración de los rastros de la comisión de unos hechos, dificultad en la detección y la persecución de las conductas dañosas, el carácter transnacional de estas conductas delictivas junto con su insuficiente regulación legal y la escasa conciencia de los usuarios sobre la necesidad de mantener unas mínimas medidas preventivas de seguridad. (p.213, 214)

Podemos coincidir entonces, y de acuerdo con todo lo antes presentado e investigado por diferentes autores, con lo que señala Concepción (2014)

> Efectivamente, todos estos factores facilitan la impunidad de estas conductas. Y a ello hay que añadir aspectos jurídicos tales como la problemática derivada de la determinación espacial de la ley penal, el tribunal competente o la dificultad de practicar las pruebas tradicionalmente utilizadas para identificar el rastro de la conducta delictiva. (p.214)

En contraste, las operaciones de banca electrónica son reguladas por la Superintendencia de Bancos (SBP), máximo ente regulador del negocio de Banca en la

República de Panamá, creado bajo el Decreto Ley 9 de 26 de febrero de 1998, introduce un cambio en la filosofía de autorregulación que permitió el desarrollo del Centro Bancario Internacional durante las dos décadas anteriores, para adaptar el sistema a las nuevas realidades económicas.

Con la intensión de, ofrecer un ambiente prístino y de claridad, se crea la junta directiva de esta entidad; veamos lo que señala la Superintendencia de Bancos de Panamá, en su informe, Plan Estratégico 2015 – 2019, SBP (2015): “La Junta Directiva de la Superintendencia de Bancos está conformada por distinguidos profesionales y empresarios sin vínculos con el sector bancario, ni posibilidad de ser funcionarios” (p.4).

Entre las principales funciones de la Junta Directiva están, según SBP (2015): “aprobación de normas prudenciales, interpretación en el ámbito administrativo de disposiciones legales y reglamentarias en materia bancaria, resolver las apelaciones contra resoluciones emitidas por el Superintendente, asesorar al Gobierno Nacional en torno al desarrollo del sistema bancario de Panamá” (p.4), todas estas en el marco de las normas y principios del Comité de Basilea.

De la misma forma, las principales funciones del Superintendente se encuentran, según SBP (2015), “velar por la estabilidad del sistema bancario, supervisar los bancos y a los grupos económicos de los cuales formen parte, otorgar y cancelar licencias bancarias, decretar medidas correctivas respecto a los bancos (designación de asesores, intervención, reorganización, liquidación forzosa, imposición de multas, etc.), además de

autorizar fusiones de bancos y la administración de las tareas diarias de la Superintendencia" (p.4).

Por otro lado, esta Superintendencia, emite acuerdos de carácter mandatorio, relacionados al tema de la ciberdelincuencia, que todos los bancos a nivel nacional que deseen preservar su licencia, indistintamente el tipo que sea, deberán seguir; estos acuerdos regulan y controlan las operaciones de lo que ellos tipifican como Banca electrónica y sus diferentes tipos de riesgos, las cuales profundizaremos más adelante.

Cabe señalar, que en el Plan Estratégico 2015-2019, se presentan los pilares que la SBP planea reforzar, de acuerdo con un estudio de fortalezas y debilidades (FODA), entre los que podemos mencionar:

- Pilar I: Mejorar la calidad de la supervisión basada en riesgos.
- Pilar II: Actualizar el marco regulatorio de acuerdo con estándares internacionales.
- Pilar III: Fortalecer la gestión institucional.

Entre las metas que se plantea llegar la SBP, con el desarrollo de este plan estratégico mencionamos las que consideramos guarden alguna relación con nuestra investigación, entre ellas están:

- Señala este informe que una de las principales metas del Pilar I, es el posicionamiento del proceso de supervisión bancaria tanto nacional como internacionalmente, para ello se propone, una mejora continua del Manual único de Supervisión Basado en Riesgos (MUSBER),

- Otra meta importante planteada para este pilar es, la certificación internacional de colaboradores de la SBP, en materia de riesgos, NIIF, NIA, Basilea III y Riesgos, lo que conlleva a una mejora sustancial, ya que aumenta los niveles de conocimiento sobre los riesgos y estándares internacionales, que se enmarcan a los delitos informáticos.

- En cuanto al Pilar II, señala el informe que tiene como propósito fortalecer y actualizar la regulación con la finalidad de adoptar estándares internacionales, que estén orientados en gran medida al aseguramiento y la protección de los bancos frente a situaciones de riesgos financieros y operativos.

Con la adopción de estos estándares, lo que SBP se plantea como meta es, la ruta hacia Basilea III; con relación a esto, señala Finel-Honigman & Sotelino (2015), en el apartado titulado International bank regulation and supervisión, del libro International Banking for New Century, que

> El colapso de las hipotecas subprime de 2007–09 en los Estados Unidos y su impacto devastador en las instituciones financieras de todo el mundo puso de manifiesto tanto los fallidos procedimientos internos de medición y gestión del riesgo como la supervisión reguladora externa. En respuesta a esta evidencia, el Comité de Supervisión Bancaria de Basilea emitió su nuevo conjunto de pautas oficiales para la regulación bancaria a nivel mundial, en junio de 2011. Titulado Basilea III: un marco regulatorio global para bancos y sistemas bancarios más resistentes. Basilea III representó un endurecimiento severo de las pautas de Basilea II para los pilares 1, 2 y 3. Además, impuso dos nuevas normas financieras - liquidez mínima y apalancamiento nominal máximo - que deben cumplir todos los bancos, y

> estableció la necesidad de requisitos de capital adicionales para las llamadas instituciones financieras sistémicamente importantes (SIFI). (p.145)

Otra de las metas de este pilar, según, son las adopciones institucionales en materia técnica, las cuales consisten en: implementar la Clasificación Industrial Nacional Uniforme de todas las Actividades Económicas (CINU) que permitirá la comparabilidad de las estadísticas económicas, a nivel nacional e internacional, al proporcionar un marco, para clasificar los datos según las actividades económicas, cumpliendo de esta forma con los estándares estadísticos internacionales (SBP, 2015, p.20).

Lo anteriormente señalado sería de gran beneficio, pues actualmente y como fue mencionado en otros apartados, no se pueden hacer comparaciones precisas debido a que los países manejan la información de manera dispar.

Para finalizar, otra meta es la emisión y actualización de normas en base a estándares internacionales, en la que se resaltan las transferencias bancarias, la modernización de medios de pago, en la que en primera instancia se destaca la evaluación de aspectos legales y proponer adecuaciones al marco regulatorio, lo que sería muy beneficioso, toda vez que se ampliarían las medidas de control (SBP, 2015, p.20).

En cuanto al Pilar III, podemos mencionar que

> la SBP, compila en esta área lo concerniente a las tecnologías de la información, entre otras y en el que “se busca hacer más eficiente la labor de SBP, desde su

> marco supervisor de los sectores regulados, mediante la medición de este desempeño" (SBP, 2015, p.21). Dentro de la lista de proyectos en este pilar, se puede mencionar la implementación de procesos de continuidad de operaciones, este consiste en: "velar por la estabilidad del sistema bancario, supervisando a los bancos y a los grupos económicos de los cuales formen parte", y es precisamente, en el que se tiene como metas, realizar pruebas de los procesos críticos e implementar mejoras a la Infraestructura Tecnológica.

Señala la Superintendencia de Bancos de Panamá (2015), que este proyecto busca

> Colocar las estrategias más adecuadas para la rápida recuperación del negocio ante un evento desafortunado, identificando los procesos críticos y claves de la Superintendencia de Bancos de Panamá, integrando procedimientos actuales al Programa de Continuidad de Negocios y definiendo a las partes interesadas en comités de continuidad enfocados en la metodología de administración de Continuidad de Negocios (BCM). (p.25)

En vista que, con la creación de las estrategias mencionadas, lo que se busca es reforzar la estabilidad del sistema bancario y la continuidad de las operaciones, SBP (2015), plantea lo siguiente

> La revisión y evaluación del Plan de Continuidad de Negocios de la Superintendencia de Bancos que se realizará, contempla reforzar en los funcionarios de la institución, estar preparados ante un evento que interrumpa sus operaciones, salvaguardando vidas humanas, protegiendo información y activos de la institución, mediante un rescate óptimo de sus operaciones claves. (p.25)

Igualmente, en cuanto a estándares de seguridad a los sistemas de información, mejores prácticas y marcos metodológicos más implementados por el sector bancario y financiero en Panamá, podemos mencionar las Normas ISO, en especial las del grupo ISO 27000.

Pero ¿Qué son las Normas ISO?, respecto al tema, señala Gutiérrez (2014), que estas se representan de la siguiente manera:

> En la actualidad es una red de institutos nacionales de normalización de 159 países, con un miembro por país y un secretariado central que coordina el sistema desde la sede en Ginebra, Suiza. La ISO es una organización no gubernamental, es decir, sus miembros no son, como en el caso de la ONU, delegados de los gobiernos nacionales. No obstante, ocupa una posición especial entre los sectores público y privado, ya que, por un lado, muchos miembros son parte de la estructura gubernamental de sus países o son designados por sus dirigentes. Por otra parte, otros miembros provienen del sector privado y son propuestos por las asociaciones de industriales. Los comités técnicos de ISO se encargan de la preparación de las normas internacionales. Cada organismo miembro, interesado en una materia para la cual se estableció un comité técnico, tiene el derecho de estar representado en dicho comité. De esta manera, los Borradores Finales de Normas Internacionales (FDIS, del inglés Final Draft International Standard) adoptados por los comités técnicos se envían a los organismos miembros para su votación. La publicación como Norma Internacional requiere la aprobación de al menos 75% de los organismos requeridos a votar. Desde su fundación en 1947 hasta 2009, la ISO ha publicado más de 17, 500 estándares internacionales y otro tipo de documentos

> normativos, que comprende áreas tan variadas como agricultura, construcción, ingeniería mecánica, equipo médico, hasta aspectos relacionados con tecnologías de la información. (p.72)

En lo que nos compete, al área tecnológica, se debe agregar que, en la página oficial de La Organización Internacional de Estandarización (ISO), señala que, a través de las normas recogidas en **ISO / IEC 27000**, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas **ISO 27001.**

Ampliamos, los puntos anteriores con lo presentado por Landino et al (2011), en su artículo, Fundamentos de ISO 27001 y su aplicación en las empresas, que

> El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido. Sin embargo, toda esta cercanía y facilidad de uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio. Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que

> deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. La definición de SGSI se hace de manera formal en la norma ISO 27001, donde están los estándares y mejores prácticas de seguridad de la información. (p.334)

Por otra parte, en su apartado titulado, Importancia de la seguridad de la información, Landino et al (2011), señala que

> La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento de la utilización del internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad. “La organización Anti-Virus Test, que presta servicios de consultoría a empresas de seguridad informática, dice que en el 2008, había 9 millones de Software malicioso en el mundo. En el 2009 la empresa registraba 22 millones, sólo de esta amenaza”. Con este panorama las empresas deben diseñar e implantar estrategias que les permita mejorar la seguridad de la información en su organización. (p.334, 335)

Habría que decir, también, que COBIT 5, publicado en 1995, por la Organización ISACA, a través de su fundación, es una herramienta de gobierno de tecnologías de la

información (TI) que permite evaluar la calidad de la estructura de tecnología de información actual de una organización, a través del diagnóstico que permite definir metas desde el punto de vista de seguridad y control para cada proceso en la organización.

Algo parecido ocurre, según Montaño et al (2017), relacionado a COBIT 5, en su artículo, Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Prácticas TI en cumplimiento de la Ley Sarbanes–Oxley, en su apartado titulado, Marco De Referencia De Cobit 5, que

> Es el conjunto de mejores prácticas para el manejo de información, creado por la Asociación para la Auditoría y Control de Sistemas de Información – ISACA, en particular, por el Instituto de Administración de las Tecnologías de la Información – ITGI. COBIT 5, provee un marco de referencia de Gobierno y Gestión de TI en las empresas y herramientas de soporte que permiten a la alta dirección reducir la brecha entre las necesidades de control, los asuntos técnicos y los riesgos del negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones, enfatizando en el cumplimiento normativo, ayudando a las organizaciones a aumentar el valor obtenido de TI, facilitando su alineación y simplificando la implementación del marco de referencia (ISACA-COBIT 5, 2012). (s.n.)

En síntesis, se puede afirmar que, debido a la falta de interés en cuanto a la legislación por parte de nuestros gobernantes, a causa de los grandes vacíos aún pendientes por resolver, entre otros, evidencian la gran problemática latente en relación a la ciberdelincuencia en nuestro país, afectando de una forma u otra los sistemas de

información utilizados para las operaciones de banca electrónica de cuentahabientes en la ciudad de Panamá; lo que ha obligado en cierta forma a las entidades reguladoras de los bancos a la creación de acuerdos y el uso de las Normas Internacionales de seguridad y mejores prácticas bancarias, con el fin de colaborar a mitigar este flagelo, los cuales profundizaremos en apartados posteriores.

En ese orden de ideas, señala el Gobierno de la República de Panamá (2014), en su Plan Estratégico de Gobierno-PEG 2015-2019, “Especial atención merece el fortalecimiento del Sector Financiero, los aspectos de contexto que el país debe abordar en los próximos años (GAFI, lavado de dinero, otros), así como el impulso de una Ley de Asociación Público-Privada” (p.27).

Dicho lo anterior, amplia el PEG 2015-2019 (2104), que

> La importancia del mantenimiento de los equilibrios fiscales, económicos y financieros básicos del país para la continuidad del proceso de desarrollo es un hecho generalizadamente admitido. Panamá ha sabido posicionar como fortaleza de país, específica en el contexto americano e internacional, su estabilidad y su seguridad económico-financiera, la cual constituye condición necesaria para la continuidad de su desarrollo como plaza económico-financiera, de gran importancia directa e indirecta para el desarrollo económico del país. La orientación y concreción de las políticas públicas habrá de prestar, complementariamente, gran atención a la promoción del protagonismo de la inversión privada en el proceso de desarrollo, una vez realizado un esfuerzo de inversiones públicas cuya dinámica resulta insostenible a corto y medio plazo. (p.27)

Por un lado, en cuanto al posicionamiento y seguridad económico-financiero, podemos señalar como uno de los factores de éxito y que ofrece mayor seguridad y respaldo al sistema financiero de nuestro país, lo que señala la SBP (2015), en su Plan estratégico 2015-2019, “Cabe señalar que la moneda oficial de la República de Panamá es el balboa, la cual tiene un valor a la par del dólar de los Estados Unidos de América y según la legislación panameña, circula libremente y se utiliza sin restricciones en las transacciones comerciales y financieras” (p.5).

Por otro lado, podemos señalar, la concreción y mejoramiento de las políticas públicas, como uno de los principales factores de esa falta de interés por parte de los gobernantes, de adecuar y mejorar las legislaciones entorno a los delitos informáticos, toda vez que en un futuro próximo les resulte insostenible.

El siguiente punto, se trata otro factor relevante, en cuanto a los avances de esta investigación, nos referimos al tratamiento y desarrollo de las operaciones bancarias, específicamente las de banca por Internet, las cuales son consideradas por diferentes autores como comercio electrónico.

Por lo que, Cohen y Asín (2009), advierte que: “el comercio electrónico también es una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como de mejorar la calidad de los bienes y servicios además de mejorar el tiempo de entrega” (p.61).

Mientras tanto, Rayport y Bernal (2007), subraya que

> El comercio electrónico utiliza transacciones con tecnología habilitada. El uso de navegadores de Internet en la World Wide Web para realizar estas operaciones es el ejemplo más conocido de interfaces con los clientes con tecnología habilitada. Sin embargo, otras interfaces como los cajeros automáticos, el intercambio electrónico de datos (EDI; electronic data interchange) entre asociados de negocio a negocio y la banca electrónica y por teléfono también pertenecen a la categoría general de comercio electrónico. Las empresas solían manejar esas transacciones con los clientes y los mercados en persona; en el comercio electrónico es posible realizarlas utilizando la tecnología. (p.5)

Todas estas observaciones se relacionan también, con lo señala Donadío et al (2004), “Cuando se integra un negocio electrónico se requiere una estrategia de negocios completa, que involucra tecnología, información y procesos del negocio para maximizar el valor que se ofrece al cliente en los productos y servicios que adquiere” (p.2).

Amplia, Donadío et al (2004), según lo descrito en el apartado anterior: “Implica que los sistemas computacionales compartan información entre ellos e interactúen con los clientes, proveedores, socios y entidades con los que se relacionan. Las transacciones de comercio electrónico deben estar respaldadas por los sistemas computacionales que integran el negocio electrónico” (p.2).

Por consiguiente, se puede agregar que, a causa del nuevo escenario económico, social y tecnológico, accionado por la crisis financiera de 2008 y otras circunstancias que señala Alkorta (2017), como “los cambios en la vida social a un nuevo entorno de uso de tecnología que facilita la comunicación y atención a clientes a través de las redes, y el aumento en el uso de dispositivos móviles, ha desembocado en la reconversión, reorientación y reducción del número de oficinas bancarias” (p.91).

De ahí que, lo que en otro apartado Alkorta (2017) ha denominado como

> Transformación operativa, multicanalidad e internet y en el cual señala que los avances tecnológicos han cambiado como en muchas otras cosas, la forma de percibir la ejecución de la atención al cliente en cuanto al negocio bancario, enfocando estos sus servicio al desarrollo de nuevos canales como autoservicio, terminales punto de venta, medios de pago electrónicos, banca on-line, banca móvil, etc., e inclusive ha transformado la estructura de las operaciones internas la cual por la tecnología permite una gestión más ágil, eficiente y segura. (p.199)

Ahora bien, cuál es el verdadero trasfondo o la justificación que ha causado dichos cambios en el entorno operativo de los bancos, a parte de los antes señalados; veamos a continuación algunas referencias de costes que señala Alkorta (2017), los cuales nos pueden ayudar a clarificar el panorama en relación con este tema.

> En primer lugar, señala que: “la banca *on line* ha elevado los costes en vez de reducirlos y que las entidades de menor tamaño sufren dificultades para cubrirlos;

sin embargo, se realizan en el conjunto del banco más operaciones a través de estos canales" (p.200).

En segundo lugar, señala que según sus estimaciones el costo por operación por canal utilizado para un banco presentó las siguientes conclusiones:

1. La operación menos costosa es la realizada a través de un autoservicio.

2. La realizada a través de internet supera el coste de la anterior en 25%, por su parte la banca telefónica es 4 veces más costosa.

3. El coste de atención a transacciones en una ventanilla de oficina puede suponerse más de 7 veces superior al de auto servicio o internet (p.200).

En tercer lugar, señala que: dado el alto volumen transaccional de operaciones sin valor añadido que todavía se producen en muchas entidades, con sus consecuencias negativas tanto económicas como de dedicación de tiempo a la gestión comercial personalizada, está justificada la inversión de medios en la transformación operativa en la red y la apuesta por un proyecto que implica no solo al conjunto de la organización, sino a otros clientes y emisores que deben evolucionar hacia el uso de red en tiempo real y la gestión de las domiciliaciones y pagos a través de la banca *on line* (p.200).

En síntesis, aunque difieran las inversiones y los resultados obtenidos por los bancos, todos los antes expuestos, son factores primordiales que evidencia la

importancia y conveniencia que tiene para el sector bancario y los usuarios, la migración y uso de este tipo de modernos canales, ya que la utilización de estos a través de Internet, reduce los costes y las consecuencias negativas producto de la ocupación de tiempo a la atención en ventanilla y el beneficio al consumidor por el uso de estos servicios el cual ahora podrá realizar sus pagos a través de la banca *on line* ahorrando tiempo y dinero en movilización a los sitios físicos para efectuar sus transacciones.

Por lo tanto, se pueden esperar resultados favorables en lo comercial como en la eficiencia, pues esta transformación operativa de los bancos de la mano de la entrada violenta del Internet y la banca móvil trae consigo la posibilidad de aumentar las relaciones con los clientes y de nuevos negocios.

Dicho lo anterior, las organizaciones financieras trabajan en cómo organizarse, ya que como señala Ocaña y Uría (2017), en el Informe de KPMG y Funcas, titulado El nivel de madurez digital, Sector financiero en España, “El nuevo entorno digital obliga a las entidades financieras a reinventarse, transformarse internamente y adoptar un cambio cultural. Para ello deben seguir una estrategia que pivote sobre las personas, los procesos y la tecnología” (p.10).

De manera que, el ofrecimiento al mercado de nuevos productos y servicios, el desarrollo de nuevos modelos de negocios, nuevas propuestas de valor al cliente, entre otras, forman parte de la configuración de oferta digital, que las entidades financieras deben promover, para hacer frente, ante esa incertidumbre que provocan los cambios

continuos del entorno digital, de manera ágil, eficiente y con aprendizaje. (Ocaña & Uría, 2017, p.10)

En cuanto a, las personas, señala Ocaña y Uría (2017) que

> El cliente se convierte en el actor principal de la banca digital, por lo que uno de los retos principales pasa por entender las necesidades de cada individuo (quién es, qué necesita y cómo se comporta) para transformar el modelo de relación después de capturar sus necesidades y expectativas. El cliente es quien marca el ritmo del cambio, y la entidad debe procurarle la mejor experiencia posible en cada interacción de forma que resulte satisfactoria tanto en la vertiente racional como emocional. (p.11)

Igualmente, como señala Ocaña y Uría (2017) citado por Marangunich (2019) en su apartado titulado, Contexto de la transformación del sistema financiero en el siglo XXI, que: “El usuario también ha cambiado a la par de los avances tecnológicos. Este busca estar conectado, autónomo, exigente, participativo, multicanal y multidispositivo. Además, tiene expectativas elevadas en cuanto a la experiencia en los canales digitales y la posibilidad de interactuar con las instituciones financieras 24/7” (p.67).

Ahora bien, cabe señalar que el uso de estos canales a través del Internet cambia las reglas del juego ya que la entrada de este supone la posibilidad de nuevos competidores como los operadores en red, ya que fuerza a la comprensión que estamos frente a un nuevo fenómeno y que la lucha en el mercado ya no es en contra de

competidores establecidos sino respecto a la nueva arquitectura de negocios a la cual se debe estar en capacidad de adaptarse. (Alkorta, 2017, p.200)

Se debe agregar, lo que señala Marangunich (2019), “Estas mejoras han generado un incremento en la oferta de servicios financieros donde ahora no solo participan las instituciones financieras tradicionales sino también actores nuevos que están aprovechando la tecnología para acercarse a los clientes, brindando una mejor experiencia y dándoles la oportunidad de tener un banco en sus manos” (p.67).

En otras palabras, como señala Ocaña y Uría (2017)

> Se dibuja, por tanto, un nuevo entorno competitivo que pone en jaque a la banca tradicional. Estos competidores desarrollan nuevos modelos de negocio sacando partido de la denominada desintermediación de la cadena de valor tradicional y de una regulación laxa, lo que les convierte en una importante amenaza competitiva para bancos tradicionales. (p.14)

De ahí que, según Ocaña y Uría (2017), “aparecen nuevos competidores tecnológicos, que pueden englobarse en dos grupos principales”, los denominados:

> **Fintech:** nueva generación de empresas, generalmente startups, caracterizadas por la agilidad, flexibilidad e innovación, que persiguen los elementos más rentables de la cadena de valor del negocio bancario, ofreciendo productos o servicios

> financieros alternativos. Presentan importantes ventajas competitivas en términos de costes, especialización y uso intensivo de las tecnologías digitales, permitiéndoles crear soluciones innovadoras de la forma más eficiente posible y centrándose en ofrecer la mejor experiencia de usuario y **GAFA (Google, Amazon, Facebook y Apple):** grandes compañías tecnológicas que traspasan las fronteras de su ámbito de actuación tradicional y adquieren relevancia en nichos rentables del negocio bancario, comenzando a ofrecer servicios financieros acompañados por una experiencia de usuario excepcional. Cuentan con prestigio entre sus clientes, una gran capacidad tecnológica y de inversión, así como muchas menos limitaciones, en comparación con las entidades financieras, para usar la ingente cantidad de datos de sus clientes. (p.14)

Consideremos ahora, otro factor de mucha importancia que tiene que ver con el uso de la tecnología e Internet, la inclusión financiera, por lo que subraya Contreras et al (2019), respecto a este tema que

> Es evidente que la disrupción digital en los mercados financieros ha promovido la inclusión financiera, que, actualmente, configura un componente fundamental dentro del propósito de reducción de índices de pobreza y promoción de desarrollo en el hemisferio, pues implica el acceso a servicios y productos financieros beneficiosos, eficientes, y alcanzables que atiendan de manera efectiva las necesidades de las personas. Dichos servicios deben ser prestados de manera responsable y sostenible. La inclusión financiera se ha convertido en una prioridad para los gobiernos, los órganos encargados de las reglamentaciones y los organismos de desarrollo a nivel mundial. (p.17)

De ahí que, Contreras et al (2019), concluyan afirmando que

> Los sistemas financieros revisten de alta importancia; particularmente su acceso y digitalización, pues estos simplifican el diario vivir de los ciudadanos y favorecen la planificación de los agentes económicos. Prueba de ello es que durante los últimos años se ha presenciado una clara expansión de la prestación y de la popularidad de los servicios bancarios móviles y online, pues prácticamente la totalidad de los productos o servicios ofrecidos por las instituciones financieras dependen de la tecnología. Esta colaboración se traduce en una serie de ofertas de productos, proporciona una experiencia de cliente positiva y garantiza que los servicios y las empresas operen de manera eficiente. Incluso los países que han logrado más avances con miras a la inclusión financiera son los que han creado un entorno normativo y reglamentario propicio, y han fomentado la competencia, permitiéndoles a las instituciones bancarias y no bancarias innovar y ampliar el acceso a servicios financieros. (p.17)

Por consiguiente, algunas investigaciones indican que, en Panamá, se dan ciertas barreras para la inclusión financiera, por lo que la SBP (2015), en su Informe de Bancarización 2015, señala que

> Existe una diferencia entre las personas que no utilizan los servicios financieros porque están afectados por algún tipo de barrera y aquellas que no lo hacen simplemente, porque no tienen una demanda para este tipo de servicios. En este sentido, es conveniente mencionar la diferencia entre uso y acceso. El acceso a los servicios financieros se relaciona principalmente con la oferta de dichos servicios

> mientras que el uso viene determinado por la oferta y la demanda. El principal objetivo de la inclusión financiera es mitigar las barreras potenciales que hacen que individuos, cuyo beneficio marginal de estar bancarizados excede a su coste marginal, puedan acceder a este tipo de servicios sin verse afectados por fallos de mercado. (p.17)

Para ilustrar mejor, SBP (2015), señala y explica, algunos de los motivos por los que se da esta barrera

> En esta sección se plantea la identificación de aquellos aspectos individuales que son relevantes para determinar la exclusión del sistema financiero formal de un grupo de individuos. Estos individuos perciben obstáculos en forma de barrera que les impiden satisfacer su demanda de servicios financieros formales. La no tenencia de una cuenta en una institución financiera es la proxy (variable de interés) utilizada para identificar a los individuos excluidos del sistema financiero formal. La estimación de modelos probit que se muestra en la Tabla 6, se centra en las cuatro razones más representativas del total de las catorce que son apuntadas como obstáculos a la bancarización. La estimación de estos modelos permite caracterizar a los individuos afectados por cada una de estas barreras percibidas mediante el análisis de correlaciones significativas entre dichas percepciones y sus características individuales. A través de una encuesta realizada por el CAF en 2010, se realizó una consulta para la identificación de las barreras percibidas que determinan la exclusión de un individuo del sistema financiero formal. Para el caso de Panamá, se identificaron en orden de importancia y con variaciones entre grupos, las siguientes barreras: No tiene trabajo, No tiene dinero, No tiene los requisitos para abrir una cuenta, No confía en las instituciones financieras. (p.1).

Para comprender mejor, los resultados de esta consulta, la SBP (2015), establece que

> la identificación de patrones recurrentes en grupos vulnerables, de los países en desarrollo, podría servir para emprender programas específicos para estos grupos como veremos a continuación. Entre los principales factores, podemos mencionar la falta de confianza, y señala que el hecho de ser mujer, aumentan la falta de confianza en las instituciones financieras, lo cual aumenta la probabilidad de no tener una cuenta, lo que puede explicar, el éxito de programas y proyectos piloto de ahorro y crédito dirigidos a mujeres en diferentes países. (p.18)

Otro factor, que es presentado en esta consulta de SBP (2015) es

> la falta de dinero, el cual entre sus principales características esta, el nivel educativo, en el que señala que grupos con menores niveles educativos, son los que perciben menores ingresos. Comparados estos, con otros grupos que poseen niveles de ingresos similares, presenta como resultados que aquellos que tienen un nivel educativo más alto, tienden a tener una cuenta, lo que indica la posibilidad de ser una variable relevante en el establecimiento de políticas en la materia. (p.18)

A pesar de que, en los últimos años, se ha facilitado la apertura de cuentas, a través de tramites simplificados, la falta de documentación se presenta como otro factor

preponderante, que incide como barrera para que grupos de jóvenes, adultos mayores, así como personas de bajos ingresos, no posean una cuenta bancaria.

Por lo que señala, la SBP (2015) que, “la falta de conocimientos respecto a las alternativas ofrecidas por entidades captadoras de depósitos o simplemente, no tengan la formación necesaria para utilizarlas de forma cómoda, representa una barrera para la apertura de una cuenta bancaria” (p.18).

De la misma forma, señala SBP (2015), que “el principal obstáculo o barrera, en la bancarización, es el desempleo, el cual, para esta consulta, llama a la atención, que las mujeres jóvenes y con menores niveles de educación, son el grupo etario con mayor nivel de desempleo, lo que resalta la puesta en marcha de programas especiales dirigidos a la mujer” (p.19).

En consecuencia, señala SBP (2015), lo siguiente

> ampliar los programas de educación financiera focalizada en elementos como los expuestos, serán positivos en la ampliación efectiva de la educación financiera en el país, además, la bancarización es un factor esencial para garantizar un crecimiento económico sólido y un mayor bienestar social. No obstante, los logros y avances que pueden ser exhibidos en materia de inclusión financiera, evidencian que existen tareas pendientes y desafíos por delante. (p.19, 20)

**Tabla 4**

*Barreras percibidas por los individuos excluidos del sistema financiero formal.*

| | (1) No confía en las instituciones financieras | (2) No tiene suficiente dinero | (3) No tiene los requisitos que se piden para abrir cuenta | (4) No tiene trabajo |
|---|---|---|---|---|
| Mujer | 0.014 | | | 0.35 |
| | (11.20)** | | | (132.59)** |
| Nivel Educativo | | 0.130 | 0.02 | 0.14 |
| | | (33.36)** | (16.62)** | (45.02)** |
| Número de Hijos | | | | 0.02 |
| | | | | (32.76)** |
| Joven | | | 0.07 | 0.26 |
| | | | (21.81)** | (35.45)** |
| Adulto mayor | | 0.034 | 0.04 | 0.02 |
| | | (2.58)** | (6.91)** | (-1.61) |
| Observaciones | 123,46 | 123,476 | 123,476 | 123,476 |

* Nivel de significancia al 5%; ** Nivel de significancia al 1%.

Nota: En esta table se presentan los valores absolutos de estadística z, en paréntesis, con relación a las barreras percibidas por los individuos excluidos del sistema financiero formal.

Según, el Informe Global de Riesgos del Foro Económico Mundial 2019, citado en el Libro Estado de la Ciberseguridad en el Sistema Financiero Mexicano de la Organización de los Estados Americanos & Comisión Nacional Bancaria y de Valores (2019) “los ataques cibernéticos a gran escala y el desglose de las redes y la infraestructura esencial de la información (colapso de la infraestructura de información esencial) son considerados riesgos tecnológicos a escala mundial que, si se producen, pueden tener un impacto negativo significativo en varios países e industrias dentro de los próximos diez años” (p.16).

También, el libro Estado de la Ciberseguridad en el Sistema Financiero Mexicano (2019) amplia afirmando que

> Estos riesgos son actualmente gestionados por sectores altamente digitalizados como el sector financiero que a su vez afronta grandes retos estructurales bajo fuertes procesos de transformación digital. De esta manera, la ciberseguridad es un aspecto crítico actualmente y las entidades e instituciones financieras tienen que estar preparados para recibir ataques sin precedentes que no sólo pretenderán obtener sus recursos económicos y los de sus clientes (socios, asociados o usuarios) sino también y cada vez más información sobre estos últimos. (p.16)

Como resultado, y en concordancia a los factores antes planteados, se hace evidente la gran importancia que tiene la ciberseguridad para el sector financiero, en cuanto a la confiabilidad que estos deben proyectar y garantizar hacia sus clientes en el entorno digital como un espacio confiable para la realización de sus operaciones, toda vez, las inversiones realizadas en procesos de digitalización de servicios al cliente, no generarían el impacto positivo esperado, debido a la desconfianza en el uso de canales digitales. (Contreras et al, 2019, p.18)

Al respecto señala Marangunich (2019), sobre el riesgo cibernético, que

> Si bien es cierto que el riesgo cibernético tiene actualmente mecanismos, pautas, técnicas, procedimientos, teorías y recursos para ser gestionado, todo se refiere a lo que ocurre y tenemos hoy, lo cual se sabe que no será estático. Como parte de

> la gestión de la incertidumbre y el proceso de transformación, los riesgos de seguridad se basan de manera relevante en la participación y deberíamos estar muy atentos a este proceso de evolución. (p.64)

Amplia, Marangunich (2019), sobre la ciberseguridad, que

> Ciertamente, en el ámbito de la ciberseguridad, continuarán existiendo vulnerabilidades dada las condiciones adversas al desarrollo, al citar escenarios de ciberamenazas, ciberataques, ciberfraude, ciberguerras, entre otros. Latinoamérica resalta como una de las regiones con mayor atención en este reto por estar conformada por países en proceso de desarrollo y con potencial de negocio; además de que actualmente presenta incidencias no menores respecto a las amenazas cibernéticas. (p.64)

En definitiva, se presentan dos factores muy importantes para países como Panamá, en aspectos de ciberseguridad, el primero, estos deben estar claros como señaló Marangunich (2019), en lo que ocurre y tenemos hoy, lo que representa una gran amenaza, ya que nuestras autoridades no se ponen ni de acuerdo ni al corriente en la creación de leyes que trabajen en conjunto a los acuerdos adquiridos con anterioridades; También, se hace evidente, la falta de creación de estrategias o planes de contingencia ante incidencias digitales y segundo, estamos situados en una región considerada en vías de desarrollo, y con un alto potencial de nuevos negocios en el ámbito digital, por nuestro sector bancario, como bien habíamos señalado en líneas anteriores de esta investigación, lo que nos ubica en una coyuntura de alto riesgo.

Se hace imprescindible que las autoridades de los países tengan presente la importancia que tiene estar enterado de lo que ocurre a nivel mundial en cuanto a los delitos informáticos y más debido a la característica tan cambiante de estos, los mecanismos, acciones, leyes y convenios que posee para contrarrestar los ataques producidos por estos y con qué estrategias de gestión, respuesta y recuperación cuenta el país ante incidentes de seguridad digital.

Ahora veamos, lo que amplia Morales (2019), en su apartado titulado, El riesgo cibernético como un problema transfronterizo, del Libro, Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, el cual nos introduce a otro factor de gran importancia indicado en el apartado anterior, la ciberseguridad, el riesgo cibernético y el problema transfronterizo, del cual venimos haciendo énfasis desde el inicio del desarrollo de esta investigación, Según Morales

> La naturaleza evolutiva de los riesgos en el sistema financiero es definitivamente una cuestión de interés público, por ello el riesgo cibernético se encuentra en las prioridades más relevantes en la actualidad para las autoridades financieras. El hecho de que el riesgo cibernético sea tan cambiante no es una cuestión imprevista, dado que el sector financiero es una actividad económica que hace un uso intensivo de las tecnologías de información y comunicación, pero la complejidad de este nuevo fenómeno de naturaleza global y amenazante para la economía mundial es el grado de interconexión e interdependencia que existe en el sistema financiero internacional. (p.27).

Además, Morales (2019) amplia

> En el caso del riesgo cibernético, la dinámica del sistema financiero internacional ha mostrado que el potencial de contagio es incalculable y posiblemente de muy alto impacto a nivel doméstico, pero también a nivel transfronterizo. Todo esto exige un seguimiento y una evaluación mucho más coordinada por parte de las distintas autoridades financieras de cada país, y para ello, resulta –en primer lugar– fundamental comprender y reconocer las implicaciones para la estabilidad financiera de un ataque cibernético. Desde luego, esto es una tarea compleja en un contexto de cambio general y de aparición de nuevos patrones y estructuras de mercado en el sector financiero. (p:27)

Ahora se puede decir, que las autoridades financieras, ante la situación de crisis global sufrida, han quedado a prueba, toda vez que la sociedad les hace responsables principales de la preservación y promoción de la estabilidad monetaria y financiera de los países; no obstante, advierte, que, en la actualidad, la principal dificultad que está es encontrar la forma de jugar un papel más efectivo en cuanto a la coordinación y cooperación internacional, y así poder diseñar mecanismos eficaces para la atención de nuevas necesidades (riesgos y amenazas) que surgen a este sistema. (Morales, 2019, p.28)

Es en este sentido que, lo mencionado en el apartado anterior es un factor muy importante, pues si bien la principal función de las autoridades financieras, a aparte de tomar las mejores decisiones y coordinarse entre sí, es la creación de las mejores políticas de gobierno, toda vez, se puedan ir resolviendo dificultades que van surgiendo

en los distintos mercados y el sistema financiero en su conjunto; “esto es de especial relevancia, si se toma en consideración que un objetivo primario de la administración pública es velar por el bienestar social y resolver fallas que los agentes económicos, especialmente del sector privado, no son capaces de resolver” (Morales, 2019, p.28), haciendo esto último contradicción a lo que se viene haciendo en muchos países, o al menos en países como Panamá, que en esta materia, las autoridades encargadas se mantienen al margen, dejando este en un gran vacío legal; además, añade que “Las prioridades, objetivos y compromisos de las autoridades financieras difieren considerablemente entre países, aunque algunos aspectos son comunes a todos ellos. Esto hace que la coordinación y cooperación internacional no resulte una cuestión trivial” (p.28).

Por un lado, y como es señalado en capítulos anteriores, Panamá cuenta con una Superintendencia de Bancos, la cual se encarga de regular a todos aquellos bancos que estén interesados en realizar la actividad bancaria en este país, la cual rige los mismos por acuerdos bancarios y al margen de los acuerdos del Comité de Basilea; es por esta instancia que Panamá cumple considerablemente en aras de tener un marco de políticas y estándares internacionales enfocado en promover que nuestro sistema financiero sea saludable.

Por otro lado, las políticas públicas y leyes de Panamá no guardan concordancia con el Convenio de Budapest, por lo que dejan un gran vacío legal; en otras palabras, el sistema financiero, en esta materia, se encuentra en un limbo jurídico y estaría

desprotegido de no ser por los acuerdos creados por la Súper Intendencia de Bancos, pues la Ley creada para dar protección a este en nuestro país, resulta no ser suficiente.

Como se dijo en líneas anteriores, los delitos informáticos y su estudio no son algo novedoso, diferentes investigaciones se han presentado por muchos estudiosos del tema y diferentes teorías se han aplicado en estos, las cuales en su mayoría han sido investigaciones cualitativas de carácter social, en las que principalmente se ha buscado saber cuáles son las motivaciones para cometer estos ilícitos y sobre el perfil de las personas que cometen los mismos; por lo que a continuación haremos un examen al impacto que tienen estos a los sistemas de información a través de las operaciones de banca por Internet, de forma cuantitativa.

Se inicia por considerar, lo señalado por Carrillo (2013), en su artículo Los delitos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos, el cual afirma que: “entre los mecanismos de pago más utilizados en la actualidad, dentro y fuera de Internet, se encuentran las tarjetas en sus distintas modalidades y las trasferencias electrónicas de fondos, aunque estos no son los únicos dispositivos que permiten realizar pagos en forma electrónica” (p.211).

A su vez, los delitos informáticos, también, operan de manera similar, por lo que podemos encontrar, los cometidos dentro y fuera del Internet, según señala Shick y Toro (2017) en su Libro Cibercriminología, Guía para la investigación del cibercrimen y mejores prácticas en seguridad Digital, el cual presenta en su tabla#1, una categorización para los delitos informáticos dentro y fuera del ciberespacio. Esta describe claramente la

diferenciación de los delitos informáticos y el cibercrimen, los que son objeto de esta investigación y que serán analizados posteriormente en otros apartados.

**Tabla 5**

*Categorización para los delitos informáticos dentro y fuera del ciberespacio.*

| Categoría | | Conductas Criminales |
|---|---|---|
| Cibercrimen | Delitos Informáticos | Ciber pasar los límites en la propiedad de otras personas o causar daños. Por ejemplo, *hacking,* desfiguración, virus, *ransomware.* |
| Cibercrimen fuera del ciberespacio (no Internet) | | Ciber engaños y fraude (dinero, propiedad). Por ejemplo, fraude de tarjetas de crédito, violaciones de la propiedad intelectual (piratería). Clonación de dispositivos inteligentes (*smarts-cards).* |

Nota: esta tabla muestra la categorización para los delitos informáticos y sus diferentes conductas criminales.

Lo presentado hasta aquí supone que, existen tanto operaciones realizadas por cuentahabientes dentro y fuera de Internet, así como delitos Informáticos cometidos (según la clasificación anterior), dentro y fuera de Internet, que tienen que ver con las operaciones investigadas, por lo que este estudio se enfocará solamente a los realizados a través de Internet en la ciudad de Panamá.

Teorías como la TAC (Teoría de las Actividades Cotidianas) de Cohen y Felson, fueron utilizadas por el Dr. Choi en 2008, en su estudio de enfoque cualitativo-experimental, para estimar patrones de victimización por delitos informáticos, así como el

uso de varias categorías para clasificar a los ciberdelincuentes, “incluyendo: sombrero blanco, sombrero negro y ciberpunks o *Script Kiddies”*, las cuales definiremos en apartados posteriores, según Barber 2001, también citado por en su investigación en 2008 (Shick, 2017, p.74).

Además, Shick (2017), señala que, en esta investigación, la encuesta cuantitativa centrada en víctimas, no determino factores motivacionales entre los ofensores, sin embargo: “al utilizar un proceso de entrevista mucho más flexible con los delincuentes informáticos, el estudio proporciono valiosos conocimientos en profundidad al respecto” (p.75).

Otra teoría como la de elección racional (TER) de Cornish y Clarke (2004) fue citada por Shick (2017) en este estudio, para determinar si la comisión de un delito por parte de un delincuente se basa en el principio de utilidad esperada que es parte integral de la teoría económica (TE) (p.80); para Akers & Sellers (2004) también citado por Shick (2017), esta teoría explica que: “las personas tomarán decisiones racionales basadas en la medida en que esperan que la elección maximice sus ganancias o beneficios y minimice costos o perdidas”(p.80); en pocas palabras, lo que se buscaba a través de esta, es demostrar si las motivaciones de los cibercriminales para cometer dichos delitos eran de orden económico.

Más aún, los resultados de la investigación de Shick (2017), indican que son diversos los factores que motivan a los cibercriminales a participar y cometer estos ilícitos, los cuales no solamente obedecen a factores económicos.

A continuación, se mencionan algunos de los resultados de la investigación de Shick (2017), en la que se puede apreciar que

1. “Las personas que participan en actividades de delincuencia informática actúan a partir del refuerzo positivo de la familia y los compañeros” (p.100); este resultado, según el investigador es debido a que participantes de la investigación en determinados momentos actuaron bajo la aprobación o consentimiento de algún familiar o bien fueron animados por amigos o compañeros de trabajo.

2. “Cambios en el curso de la vida” (p.100); al respecto Sampson & Laub (1993), citado por Shick (2017), explican que “los abruptos puntos de inflexión” y los cambios en la vida, como casarse, encontrar trabajo y tener hijos, aumentan los lazos sociales con la sociedad”. (p.101); el investigador señala que este tema despertó su interés en perseguir futuras perspectivas teóricas, y que la evaluación de estas con relación a la delincuencia informática podría ser beneficiosas en la determinación de ciertos acontecimientos que conducen a una discontinuidad en los comportamientos criminales informáticos de un individuo.

3. “Un hallazgo notable en esta investigación encontró que la mayoría de los participantes desconocía o ignoraba las leyes específicas sobre delincuencia informática aplicables a su estado o país de residencia” (p.101); amplia el investigador que, esto se debe en parte la escasa atención dada a la delincuencia informática en el sistema de justicia penal y también a la falta para educar a los ciudadanos sobre las consecuencias y las leyes en materia de delitos informáticos, aspecto que ha sido evaluado en apartados anteriores de esta investigación.

4. La Evidente motivación de los delincuentes informáticos por los incentivos monetarios no puede quedar atrás, además el robo de claves de CD para video juegos, fraude de clic, robos de servicios de Internet, cuestiones de ego, diversión entre otros; en general esta investigación determina que son diversas las motivaciones.

Otras motivaciones, motivaciones señaladas por Echenique (2008), en su apartado, Delitos por Computadora, son:

- Beneficio personal. Obtener un beneficio, ya sea económico, político social o de poder, dentro de la organización.

- Beneficios para la organización. Se considera que al cometer algún delito en otra computadora se ayudará al desempeño de la organización en la cual se trabaja, sin evaluar sus repercusiones.

- Síndrome de Robín Hood (por beneficiar a otras personas). Se están haciendo copias ilegales por considerar que al infectar a alas computadoras, o bien al alterar la información, se ayudará a otras personas.

- Jugar a jugar. Como diversión o pasatiempo.

- Fácil de desfalcar.

- El individuo tiene problemas financieros.

- La computadora no tiene sentimientos. La computadora es una herramienta que es fácil de desfalcar, y es un reto poder hacerlo.

- El departamento es deshonesto.

- Odio a la organización (revancha). Se considera que el departamento o la organización es deshonesta, ya que no ha proporcionado todos los beneficios a los que tiene derecho.

- Equivocación de ego (deseo de sobresalir en alguna forma).

- Mentalidad turbada. Existen individuos con problemas de personalidad que ven en elaborar un virus un reto y una superación, los cuales llegan a ser tan cínicos que ponen su nombre y dirección en el virus, para lograr ese reconocimiento (p.193, 194).

Por otra parte, y para dar seguimiento, otros resultados de investigaciones como la presentada en el libro, Estado de la ciberseguridad en el sistema financiero mexicano (2019), presentado por la Organización de los Estados Americanos y La Comisión Nacional Bancaria y de Valores de México, señala con relación al tipo de eventos y motivaciones, que

> Según las entidades e instituciones financieras en México, el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes con más frecuencia contra los clientes (socios, asociados o usuarios) de servicios financieros son: i) Phishing, ii) Software espía (Malware o troyanos), y iii) Ingeniería social. También resulta importante anotar que dentro de las principales motivaciones para la realización de estos ataques se encuentran las

> económicas (74%), y en una menor medida las políticas, el hacktivismo, la reputación personal como hackers y el robo de información personal. (p.9)

Como resultado, a todo lo anterior inicia su escrito Moreno (2016), Presidente Banco Interamericano de Desarrollo, afirmando en el documento Observatorio de la ciberseguridad en américa latina y el caribe, Informe Ciberseguridad (2016) que está incluido en el libro: Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, lo siguiente:

> Si los lectores han llevado un mensaje de este Informe 2016, del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen. Su análisis es un llamado a la acción para empezar a hacer todo lo necesario por proteger esta infraestructura clave para el siglo XXI. (p.9)

Otro factor, principal de este estudio, son los sistemas de información, al respecto Astudillo (2008), en su artículo titulado, Consideraciones para la selección de sistemas de información contables y administrativos en la pyme colombiana, señala que

> En la operación diaria de un Sistema de Información de misión crítica, en donde la información operada por el mismo, se convierte en vital para el desarrollo del objeto social de la compañía, se deben considerar un conjunto de aspectos importantes para una correcta elección del sistema que permitirá administrar estratégicamente la información (p.53) […], En este momento es cuando se logra identificar, el

> impacto que tiene una correcta elección de la Tecnología Informática a usar al interior de la organización. La relevancia del tema se identifica, en el papel que juega la información que manejan estos sistemas al interior de la organización. El correcto registro de los hechos económicos, el apoyo en el manejo de la información a cada uno de los procesos organizacionales, la consolidación de la información de manera lógica atendiendo las reglas del negocio y por último todo el tema de predicciones con fundamento estadístico basado en la información de eventos económicos de manera histórica, constituyen los principales aspectos necesarios para la correcta dirección de cualquier organización. (p.54)

En otro apartado, titulado, Aspectos funcionales a considerar en la selección de sistemas de información contables y administrativos, Astudillo (2008), señala que

> Los Sistemas de Información Contables y Administrativos deben proporcionar todas las operaciones que el ente económico requiera para poder desarrollar su objeto social de manera conveniente y adecuada a la normatividad legal vigente. Adicional debe proporcionar el concepto de manejo de documentos operativos completamente parametrizables. Además del registro de eventos económicos (movimiento), el manejo apropiado de los datos registrados (consultas por terceros, auxiliares y otros) y las operaciones de interpretación de información (estados financieros), los Sistemas de Información Contables y Administrativos deben cumplir con los siguientes requisitos mínimos:
>
> 1. Sistema de Información Contable debe poder soportar procesos de extracción de información derivada de cualquier forma de consulta y en los formatos portables o populares. 2. El Sistema de Información Administrativo debe poder representar la

> operatividad de la organización mediante la automatización de los procesos y representación de los datos generados por la misma. 3. El Sistema de Información Administrativo, debe poder ser parametrizable mediante el uso de los documentos asociados a la operación. 4. El Sistema de Información Administrativo debe poder ordenar las consultas a la información de tal manera que se constituya en base para la toma de decisiones. 5. El Sistema de Información Contable y Administrativo debe soportar las operaciones de conversión e interpretación de información, necesarios para el análisis financiero del ente económico. (p.54)

Por otro lado, Abrego (2017), en su investigación titulada, Influencia de los sistemas de información en los resultados organizacionales, señala que

> Los sistemas de información (SI) son uno de los componentes más relevantes del entorno actual de negocios, que ofrecen grandes oportunidades de éxito para las empresas, ya que cuentan con la capacidad de reunir, procesar, distribuir y compartir datos de forma oportuna y de manera integrada. Además, ayudan a estrechar las brechas geográficas, permitiendo a los empleados ser más eficientes, lo cual se refleja en una mejora de los procesos, de la gestión, y del manejo de la información, dando como resultado un impacto positivo en la productividad y competitividad de las empresas. (p.304)

Algunos resultados de la investigación de Abrego (2017) que consideramos acorde a esta investigación, son los que tienen que ver con la satisfacción de los usuarios por el uso de sistemas de información, los que se presentan a continuación:

> Se concluye que los usuarios que alcanzan una mayor satisfacción se ven motivados a un uso mayor de los SI, donde una mayor satisfacción y uso conducen a mejores resultados a nivel organizacional, lo que podría apoyar a las empresas en sus decisiones de inversión en tecnología, puesto que permitirían acrecentar la calidad del sistema y la calidad de los servicios, contribuyendo al rendimiento organizacional. En otras palabras, las organizaciones con mayor infraestructura tecnológica, metodologías de desarrollo y competencia de sus programadores mejoran los resultados en la calidad del sistema contribuyendo al rendimiento individual y organizacional de la empresa. (p.316)

Podemos decir, que lo anterior es lo que ha sucedido con las entidades bancarias, han apostado a la búsqueda de ventajas competitivas y han visto en las nuevas Tecnologías de información y comunicación (TIC), la forma de hacer que los usuarios encuentren, con el uso de estas, una mayor satisfacción y así aumentar sus ingresos.

## Descripción del contexto o de las unidades de análisis

### Unidad de análisis

En cuanto a, la unidad de análisis de esta investigación, hace referencia al Sistema Financiero de la ciudad de Panamá, específicamente Bancos de la ciudad de Panamá, y principalmente, sus cuentahabientes y tarjetahabientes que manejan los sistemas de información para realizar operaciones a través de medios o canales de banca por Internet.

## Contexto

La investigación se realizará en un contexto de campo, por lo que se ha planificado entrevistar gerentes que tengan bajo su responsabilidad lo referente a los riesgos que tienen afectaciones por los delitos informáticos en las operaciones del sistema financiero, además de encuestar a cuentahabientes y tarjetahabientes de bancos de la ciudad de Panamá que realicen transacciones a través de medios o canales electrónicos en este caso, los sistemas de información, con la finalidad de recaudar datos que den respuesta a los objetivos de la investigación e hipótesis.

## Normativa bases legales

Entre las leyes y los acuerdos mencionados con antelación y relacionados con la ciberdelincuencia que se han emitido en Panamá, para controlar y regular los delitos financieros, informáticos y las operaciones de Banca electrónica, podemos señalar:

- Ley que da protección al sistema financiero, la cual está contenida en el Capítulo III, titulado Delitos Financieros, Artículo 243, Texto Único del Código Penal de la República de Panamá.

- La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013, que fue publicada en la Gaceta Oficial No. 27403-A del 25 de octubre 2013.

- El Código Penal de Panamá, adoptado por la Ley 14 de 2007, con las modificaciones y adiciones introducidas por las leyes 26 de 2008, 5ª de 2009, 68 de 2009 y 14 de 2010, tipifica principalmente los delitos informáticos en su título VIII, “Delitos contra la seguridad jurídica de los medios electrónicos”, regula los delitos contra la seguridad informática. Del artículo 289 al 292

- SBP-Acuerdo No.002-2005 (de 26 de enero de 2005), en el que se regulan las transferencias bancarias realizadas por medio de tarjetas de crédito y débito y también por medio de ACH, con el fin de controlar el Blanqueo de Capitales por este medio electrónico.

- SBP-Acuerdo N°.006-2011 (Por medio del cual se establecen lineamientos sobre banca electrónica y la gestión de riesgos relacionados): Este regula y permite el acceso a los servicios bancarios a través de los servicios de banca por internet, banca móvil, banca por teléfono, terminales de puntos de venta (POS), mensajería instantánea (chat), redes sociales, correo electrónico, firma electrónica, dinero electrónico, red ACH, redes especializadas, cajeros automáticos, monedero o pago móvil, tarjeta bancaria con circuito integrado, medios de pago electrónico o cualquier otro medio o canal electrónico.

- SBP-Acuerdo No.007-2011 de 20 de diciembre de 2011, en el que se establecen las normas sobre riesgo operativo. G.O. 26944 y sus modificaciones, Acuerdo No. 002-2013, el cual modifica el artículo 28 del Acuerdo No. 007-2011 sobre Riesgo Operativo. G.O. No 27223-A de 8 de febrero de 2013. Derogado por el Acuerdo 11-2014 de 14 de octubre de 2014. Ver Resolución SBP-RG-0001-2013.

- SBP-Acuerdo 002-2012 (Por medio del cual se regula la contratación de corresponsales no bancarios para la prestación de determinados servicios en nombre de los bancos): Permite a los bancos oficiales y de licencia general, que llevan a cabo el negocio de banca en la República de Panamá, ofrecer sus servicios mediante la contratación de terceros donde no existen sucursales o cajeros automáticos. Entre las modalidades de servicio que ofrecerán los corresponsales no bancarios se destacan depósitos y retiros en efectivo en cuentas corrientes y cuentas de ahorros, así como transferencias de fondos que afecten dichas cuentas, consultas de saldos, movimientos en cuentas de ahorro y corrientes, consulta de saldos de préstamos u otras facilidades crediticias, desembolsos por concepto de operaciones de crédito.

- SBP-Acuerdo No.003-2012, de 22 de mayo de 2012 en el que se establecen lineamientos para la gestión del riesgo de la tecnología de la información. G.O. 27047-A de 1 de junio de 2012. Véase la Circular 22-2008.

- SBP-Acuerdo No.004-2013, de 28 de mayo de 2013 en el que se dictan disposiciones sobre la gestión y administración del riesgo de crédito. Derogó el Acuerdo No. 6-2000, el Acuerdo No. 6-2002 y el artículo 7 del Acuerdo No. 2-2003. G.O. 27305 de 10 de junio de 2013. Modificado por el Acuerdo No.8-2014. "Documento compilado". Véase las Circulares (30-2001, 92-2014, 165-2014, 166-2014 y 51-2017).

- SBP-Acuerdo No.001-2016 (de 26 de enero de 2016), en el que se establecer parámetros y lineamientos generales con relación a la compensación de las transacciones realizadas a través de la red ACH y la disponibilidad de sus fondos.

# CAPÍTULO III

# ASPECTO METODOLÓGICO

En este apartado se presentan los aspectos metodológicos, las técnicas y el diseño de los instrumentos que serán aplicados posteriormente a los sujetos dentro del contexto de la investigación, así como la validez y confiabilidad de estos, los procedimientos a utilizar para la recolección de la información, y el procesamiento y análisis de sus resultados, los que proporcionarán al lector una imagen más clara y precisa.

En cuanto al método de investigación a seleccionar, menciona Bernal (2010) “La elección o selección del tipo de investigación va a depender, en un alto grado, del objetivo del estudio del problema de investigación y de las hipótesis formuladas en el trabajo a realizar, así como la concepción epistemológica y filosófica del investigador” (p.110).

## Tipo y diseño de la investigación

Se emprende esta investigación con el enfoque en el que se desarrolla, el cual se puede ubicar como cuantitativo, ya que se hará uso de cifras y datos estadísticos de libros y documentos de diferentes expertos, que tratan de la temática tanto de delitos informáticos como de los sistemas de información de operaciones bancarias, utilizando técnicas de campo para obtener los resultados producto de encuestas y entrevistas a la unidad de análisis denominada sector financiero, llámese cuentahabientes y bancos de

la ciudad de Panamá, los cuales, posteriormente, serán verificados, procesados y analizados para ver si se cumple la hipótesis planteada.

Con respecto a su uso, se puede identificar su tipo como aplicada, puesto que con los resultados obtenidos se pretende presentar las recomendaciones que, en futuras investigaciones, sirvan al reforzamiento de los sistemas de información utilizados en dichas operaciones y también, para la creación de un modelo conceptual de sistema de información contable, cuya respuesta ayude a mitigar este flagelo.

En cuanto a, el diseño de la investigación, que se realizó es de tipo no experimental, ya que este modelo no utiliza manipulación de sus variables, es decir, se trata de investigaciones donde no se producen cambios intencionales en las variables independientes, ni se puede asignar aleatoriamente a los sujetos de la muestra, en este tipo de investigación lo que se hace “Se observan los hechos tal y como se presentan en su contexto real y en un tiempo determinado o no, para luego analizarlos. Por lo tanto, en este diseño no se construye una situación específica si no que se observan las que existen” (Stracuzzi, Pestana, 2012, p.87) como bien ha sucedido en este estudio.

Este estudio se realizó, con un método descriptivo y correlacional, puesto que se describirán hechos como el señalado por la Encuesta de victimización y percepción social de la seguridad (ENVI) en el que se estimó que en 2016, 11,458 personas de 18 años de edad o más, fueron víctimas del delito de fraude bancario, con un estimado en pérdidas de USD 9.2 millones, lo que según ellos, hace obligante analizar y estudiar los actuales procedimientos internos de los cuenta habientes con el objetivo de robustecer aún más

la tecnología inherente y así reducir las incidencias en estos delitos (p.116), por lo que con estos se pretende comprobar a través de la correlación y medición de sus variables, ¿Cómo impactan, la recurrencia, porcentajes, afectaciones contables y tipos de delitos informáticos a los sistemas de información a través de las operaciones de banca por Internet de cuentahabientes que manejan este tipo de medios o canales en la ciudad de Panamá? hasta el 2020, con el fin de especificar las propiedades más importantes de dicho fenómeno.

También, en cuanto a los logros que se pretenden con esta investigación, será de gran novedad, ya que al medir y evaluar el grado de relación y la forma en que interactúan sus variables entre sí, la causa de estos eventos, sucesos o fenómenos (robos, hurtos, hackeos, intrusiones, clonaciones) que están ocurriendo, servirá para diagnosticar las necesidades y problemas de nuestra sociedad, en cuanto a los delitos informáticos ocurridos a los sistemas de información de cuentahabientes y bancos de la ciudad de Panamá, a los efectos de aplicar estos conocimientos con finalidades prácticas (investigación aplicada) ya que en este país no se ha realizado estudio previo en esta área.

## Alcance y dimensión temporal

Así mismo, según el periodo de tiempo en que se desarrolla, la podremos considerar de corte transversal, ya que en este tipo de investigación se “recolectan datos en un solo momento, en un único tiempo, su propósito es describir variables, y analizar su incidencia e interrelación en un momento dado” (Hernández, et al 2014).

## Universo población y muestra

### El Universo

Para el desarrollo de este estudio se identifican dos tipos de universo a estudiar:

Documental: este universo es representado o constituido por datos estadísticos de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC 2013), Tasas de Victimización de la (UNODC 2013), Informe de Seguridad Ciudadana (CCIAP-PNUD 2017), Informe de Criminalidad año 2016, del Ministerio de Seguridad Pública a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC), de los cuales se obtuvo cifras y estadísticas de uso de redes sociales e Internet, de victimización y recurrencia de algunos delitos informáticos, entre otros.

Para el tratamiento del universo documental no se calculará una muestra ya que se puede considerar que los datos obtenidos son fáciles de manejar. Estos datos posteriormente, serán comparados con los resultados obtenidos de los dos instrumentos utilizados (entrevista y encuesta).

De campo: El otro universo, denominado de campo, es conformado por cuenta habientes y tarjetahabientes que utilizan el servicio de banca por Internet a través de los medios o canales ofrecidos por las entidades bancarias de su elección, además, los gerentes de riesgo de las entidades bancarias que tienen que ver con las áreas de Tecnología de la información (TI) y Riesgo tecnológico de Bancos que manejan banca electrónica en la ciudad de Panamá.

Para el tratamiento del universo de campo si es necesario obtener una muestra representativa de este, ya que para la consecución de los resultados se va a utilizar dos tipos de instrumentos de recolección de datos diferentes. Los cálculos para la consecución de las muestras se podrán observar en el apartado siguiente.

## Población

En este estudio se consideró como población la unidad de análisis que se refiere al sector financiero, específicamente los cuentahabientes y bancos que manejan la banca por Internet, dándole seguimiento a lo que señala Ñaupas et al (2013), “En las ciencias sociales la población es el conjunto de individuos o personas o instituciones que son motivo de investigación y que la muestra es el subconjunto, o parte del universo o población, seleccionado por métodos diversos, pero siempre teniendo en cuenta la representatividad del universo” (p.246).

## La Muestra

Siguiendo este sentido y poder verificar la hipótesis de investigación, se puede señalar que: para la determinación del tamaño óptimo de la muestra “al lector le será muy útil comparar qué tamaño de muestra han empleado o sugieren diversos metodólogos e investigadores” (Hernández et al, 2014, 187).

Es por este motivo que, para la determinación de la muestra en este estudio, ya que está delimitado a la ciudad de Panamá, se utilizará los tamaños de muestra más

sugeridos o propuestos por diversos autores, según sus poblaciones (nacionales o regionales) y los subgrupos que quieren estudiarse, así como de acuerdo con los análisis que se lleven a cabo.

Siendo este estudio de tipo económico y en el plano regional con una población de más de 1000, se tomará la muestra de 100 sugerida para este tipo de estudios.

En la Tabla 8.4, denominada, Muestras utilizadas con frecuencia en investigaciones nacionales y regionales según área de estudio Hernández et al (2014), “podemos encontrar los tamaños de las muestras sugeridos para los diferentes tipos de estudios y sus respectivas muestras tanto para nacionales como para regionales” (p.188).

**Tabla 6**

*Muestras utilizadas con frecuencia en investigaciones nacionales y regionales según área de estudio.*

| Tipos de estudio | Nacionales | Regionales |
|---|---|---|
| Económicos | 1000+ | 100 |
| Médicos | 1000+ | 500 |
| Conductas | 1000+ | 700-300 |
| Actitudes | 1000+ | 700-400 |
| Experimentos de laboratorio | – – – | 100 |

Nota: en esta tabla se pueden apreciar los tipos de muestras utilizadas para investigaciones nacionales y regionales según área de estudio.

## Variables

A continuación, se presentan las variables las cuales “son elementos o factores que pueden ser clasificados en una o más categorías. Es posible medirlas o cuantificarlas, según sus propiedades o características (Stracuzzi, Pestana, 2012, p.67).

**Variable independiente:** La variable independiente para este estudio es: Delitos informáticos.

**Variable dependiente:** La variable dependiente para este estudio es: Operaciones bancarias.

### Conceptualización de las variables

Como señalamos con anterioridad la variable independiente objeto de estudio se denomina ***delitos informáticos***, para conceptualizarla se presentan los siguientes conceptos o definiciones de esta.

Según Morales et al (2017) “Es aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto en ellos, así como el mal uso de estos” (p.96).

Para Gabriel Andrés Campoli, citado por Morales et al. (2017), “Son aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la

legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos" (p.97).

Por lo que para esta investigación los delitos informáticos son comportamientos o conductas ilícitas, entre las que se pueden mencionar robo, fraudes, intrusión, etc. en las que ha estado involucrada la computadora, software o cualquier otro medio tecnológico con la finalidad de afectar a estos teniendo como consecuencia daños o lesiones a bienes ajenos.

En cuanto a nuestra variable dependiente, ***Operaciones bancarias***, presentamos algunos conceptos y definiciones de esta.

Maldonado (2006) "Las operaciones de los bancos son aquellas transacciones que las personas emplean para un determinado bien económico puede ser a través de cuentas bancarias" (párr.1).

La Superintendencia de Bancos de la República de Panamá define en su glosario (BAN_08 Glosario) como la prestación de servicios bancarios a través de medios o canales electrónicos, la cual involucra los servicios ofrecidos por: banca por internet banca móvil, banca por teléfono, terminales de puntos de venta (POS), mensajería instantánea (Chat), redes sociales, correo electrónico, firma electrónica, dinero electrónico, red ACH, redes especializadas, cajeros automáticos, monedero o pago móvil, tarjeta bancaria con circuito integrado, medios de pago electrónico o cualquier otro medio o canal electrónico.

Por lo que para esta investigación, las operaciones de banca por Internet representan todas aquellas transacciones realizadas por los cuentahabientes de un banco a través de servicios ofrecidos por el sistema financiero, utilizando medios o canales electrónicos.

## Operacionalización de las variables

En cuanto a la variable independiente, delitos informáticos: Todos los tipos de delitos o conductas ilícitas más comunes que afectan los sistemas de información y las operaciones de banca por Internet, así como el conocimiento que poseen las personas acerca de estos, su problemática, riesgos por el mal uso, magnitud de los daños, regulaciones y mecanismos que den protección, así como también, el conocimiento que tengan los usuarios de redes o cualquier medio tecnológico; por lo que para esta investigación se realizarán encuestas a cuentahabientes y tarjetahabientes de bancos de la ciudad de Panamá que realicen transacciones a través de medios o canales electrónicos con la finalidad de recaudar las cifras que den respuesta a los objetivos de la investigación e hipótesis.

En cuanto a la variable dependiente, operaciones bancarias: Características de sector financiero, como que tipos de servicios ofrecen, cuáles son las más utilizados a través de medios o canales electrónicos, a través de banca por Internet y niveles de afectación para poder ejercer mejor control; por lo que para esta investigación se realizarán entrevistas a profesionales y/o gerentes que tengan bajo su responsabilidad lo referente a los riesgos que tienen afectaciones por los delitos informáticos en las operaciones del sistema financiero.

A continuación, se presentan algunas dimensiones o características los cuales son elementos integrales producto del análisis o descomposición de una variable.

**Tabla 7**

*Operacionalización de las variables.*

| VARIABLES | DIMENSIONES | INDICADORES | PREGUNTAS |
|---|---|---|---|
| **Delitos informáticos.** | Tipos de delitos que afectan los sistemas de información y las operaciones de banca por Internet. | Fraude informático. | #10 |
| | | | #11 |
| | | Falsificación informática. | #8 |
| | Conductas ilícitas más comunes a la banca por Internet. | Magnitud de daños a bien privado. | #14 |
| | | | #9 |
| | Proporción de personas que están enteradas o poseen conocimientos sobre la problemática social que representan estas malas prácticas. | Tecnológicas. | #5 |
| | | | #4 |
| | Proporción de personas que están informadas sobre los riesgos producto del mal uso de la banca por Internet. | | #6 |
| | Proporción de personas que tienen conocimiento de regulaciones o leyes que le protejan de los delitos informáticos | | #7 |
| | Proporción de personas que poseen conocimiento en el uso de la tecnología (hardware/software). | | #15, 16, 17 |
| | Proporción de personas que poseen mecanismos de protección en sus computadores o medios electrónicos. | | #18 |
| **VARIABLES** | **DIMENSIONES** | **INDICADORES** | **PREGUNTAS** |
| **Operaciones de banca por Internet.** | Servicios financieros más utilizados por cuentahabientes de banca por Internet. | Servicios financieros. | #1 |
| | | | #2 |
| | Afectaciones a operaciones banca por Internet producto de delitos informáticos. | Operacional. | #3 |
| | Niveles de control ejercidos por las entidades bancarias. | Controles. | #12 |
| | | | #13 |

Nota: en este cuadro se puede apreciar la operacionalización de las variables de estudio.

## Selección de técnicas e instrumentos

Diseñado el plan para esta investigación y solucionados los aspectos que corresponde a la muestra, “Es entonces cuando se hace uso de las técnicas de recolección de datos, que son las distintas formas o maneras de obtener la información. Para el acopio de los datos se utilizan técnicas como observación, entrevista, encuesta, pruebas, entre otras” (Stracuzzi, Pestana, 2012, p.115).

## Técnicas para la recolección de datos

Para seleccionar los datos que servirán en la verificación de la hipótesis se utilizarán las siguientes técnicas: el análisis de documentos, la entrevista, el cuestionario y como instrumentos: la matriz o ficha de investigación, la guía de entrevista y la cédula de cuestionario.

## Instrumentos

Como se menciona con antelación, para verificar la hipótesis de investigación se utilizarán instrumentos para desarrollar los dos tipos de universo a estudiar como lo son:

## Instrumento de análisis de documentos:

Matriz o ficha de investigación

## Instrumento de observación de campo:

Cédula de cuestionario para encuesta a cuentahabientes y tarjetahabientes de medios o canales electrónicos de bancos de la ciudad de Panamá.

Guía de entrevista para entrevista a Gerentes relacionados a las áreas de riesgo de bancos de la ciudad de Panamá.

## Elaboración y descripción de los instrumentos

### La Matriz, ficha-fichaje

La ficha es una hoja de cartulina, rayada o sin rayar que sirve para registrar los datos e informaciones de los planes constituidos por datos estadísticos de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC 2013), Tasas de Victimización de la (UNODC 2013), Informe de Seguridad Ciudadana (CCIAP-PNUD 2017), Informe de Criminalidad año 2016 del Ministerio de Seguridad Pública a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). El instrumento es la ficha, pero el proceso de recopilar los datos de libros o documentos se denomina fichaje. Se utilizarán, fichas de contenido o investigación (textual) de acuerdo con las normativas APA, **ver cuadro Nª17**.

## Cédula del cuestionario

Es un sistema de preguntas referidas al desarrollo de la hipótesis formulada. Se elaborará el cuestionario, dirigido al público usuario de servicios ofrecidos a través de medios o canales electrónicos llámese cuentahabientes o tarjetahabientes del sistema financiero de la ciudad de Panamá.

En cuanto a, la construcción del instrumento, se consideraron las diferentes fuentes de información documental explotadas hasta el momento, entre las que se pueden mencionar: investigaciones doctorales, libros, artículos científicos de autores como González (2013), Alkorta (2017), Maldonado (2006) y Carrillo (2013), los cuales aportaron al análisis e identificación de dos variables: los delitos informáticos y las operaciones de banca electrónica.

Con la información obtenida, se realiza una revisión y se crean una serie de indicadores que ayudarán a construir un instrumento el cual cuenta con 18 ítems distribuidos entre las variables antes mencionadas; se diseñó a través de diferentes tipos de escalas, entre las que se puede mencionar las nominales, ordinales y de intervalo (Likert), que varían por pregunta y entre las que podemos encontrar desde 1-siempre, 2-Casi siempre, 3-Algunas veces, 4-Casi nunca, 5-nunca, además de 1-Totalmente de acuerdo, 2-Parcialmente de acuerdo, 3-Ni de acuerdo ni en desacuerdo, 4-Parcialmente en desacuerdo, 5-Totalmente en desacuerdo, y otras como, 1-Nada, 2-Poco, 3-Mucho, por lo que podemos concluir que las variables de medición en este estudio son de orden policotómicas. Una vez terminado el instrumento fue sometido a una prueba piloto, en la cual participaron 10 cuentahabientes que manejan sus operaciones a través de la banca

por Internet y posteriormente validado por el juicio de una serie de profesionales en el área, validación que se detalla en apartados siguientes.

El diseño original de la investigación señala que se realizaría una encuesta (de campo) a cuentahabientes de bancos que manejan banca por Internet y una entrevista a Gerentes de Tecnología de la información, así como a Gerentes de riesgo Tecnológico. Cabe señalar que, este diseño, por motivos de la afectación mundial denominada Pandemia Covid-19, se modificó, ya que las condiciones de cuarentena y restricciones de movilidad y trabajo en el país, impidieron la realización de la aplicación del cuestionario y la entrevista de la forma descrita en este.

En cuanto a, el cuestionario, al permanecer los bancos cerrados y sus operaciones físicas cesadas en los distintos departamentos y la movilidad de las personas restringidas, se procedió a suplantar el documento escrito por un formulario digital.

Para la creación de este formulario se utilizó un formato electrónico de Google, denominado Google Forms, en el cual se vaciaron todas las preguntas de la encuesta escita, con sus respectivas escalas de medición.

Este formulario fue enviado a través de correos electrónicos y enlaces directos a este, a través de la plataforma de Wasap, en una cantidad mayor a la muestra requerida, de los cuales se obtuvo 113 resultados, superando la cifra requerida de 100 encuestados.

## La Guía de entrevista

Por otro lado, se elabora el cuestionario, dirigido a Gerentes de riesgo relacionados al área de Tecnologías de la información y riesgos de entidades bancarias de la ciudad de Panamá, basando este en el criterio anterior, la explotación de información documental planteada por diferentes expertos, la cual nos conduce al análisis de las dos variables antes mencionadas.

Con relación a, la entrevista, no se obtuvo los resultados esperados, por los motivos antes indicados de restricciones de movilidad, ya que, en la mayoría de los bancos, los departamentos de Tecnología de la información y Riesgo tecnológico se encontraban cerrados, limitando el acceso a la realización de esta.

Más aún, se logró contactar al vicepresidente ejecutivo de una prestigiosa compañía consultora de Riesgos, que realiza este tipo de operaciones a gran cantidad de empresas y bancos de la localidad, el cual respondió la entrevista a través de la plataforma de Zoom, en la mañana del día jueves 25 de septiembre del presente. Los datos de esta entrevista serán analizados y utilizados como referencia en la descripción de los resultados de la investigación, toda vez por efectos de la situación mencionada con anterioridad, no se pudo cumplir con el diseño planteado.

## Validez y confiabilidad de los instrumentos

En cuanto a, la validez del instrumento, como señala Espinosa y Lloréns (2015), en su artículo, Exploración de la capacidad de liderazgo para la incorporación de TICC

en educación: Validación de un instrumento, lo que se busca es “asegurar que el instrumento mide la variable que se quiere medir” (p.40).

Por otro lado, en cuanto a la confiabilidad, Espinosa y Llorénz (2015) cita a Arribas (2006), el cual señala que la capacidad del instrumento para “ofrecer en su empleo, repetido, resultados veraces y constantes en condiciones similares de medición” (p.40).

Para validar el contenido de los instrumentos utilizados en esta investigación (cuestionario y entrevista), se utilizará un método muy aplicado y desarrollado en muchas investigaciones, denominado valoración por juicio de expertos, de acuerdo al modelo de Lawshe (1975), modificado por Tristán (2015), el cual se cita a continuación por Espinosa & Llorénz (2015);

> Se extrae un indicador de acuerdo, entre un número determinado de jueces con el que se puede establecer la Razón de Validez de Contenido (*Content Validity Ratio, CVR*), con lo que se obtiene el Índice de Validez de Contenido (*Content Validity Index, CVI*), de todo el instrumento. La validación se lleva a cabo por cada ítem que se está validando. En relación con lo anterior, a fin de dictaminar que un ítem es aceptable, se espera que el CVI, sea superior a 0.5823. En consecuencia, para cuidar la calidad del instrumento, todos aquellos ítems o banco de ítems con valores inferiores debe considerarse su eliminación. (p.41)

Dicho lo anterior, y considerando la experiencia en las áreas de informática y sistemas de información, se invitó a seis académicos expertos, doctores, de la Universidad Autónoma de Baja California para que participaran como jueces, a los cuales se le entregaron dos instrumentos a cada uno.

Para ser más específicos, los instrumentos entregados a los expertos son: el cuestionario, el cual consta de 18 ítems, de los cuales 1 ítem corresponde a identificación del informante, 12 ítems corresponden a la variable delitos informáticos, 5 ítems a la variable operaciones de banca electrónica. El segundo instrumento, la entrevista, consta de 10 ítems, de los cuales 1 ítem corresponde a la variable delitos informáticos y 9 ítems a la variable operaciones de banca electrónica.

Para comprender mejor, se anexó la matriz de consistencia; en esta se presentan las definiciones operacionales para las variables estudiadas, toda vez fuesen de fácil interpretación los conceptos, así como también se ha fijado proporcionar al declarante, toda la información que le ayude o facilite la comprensión de ideas y conceptos que encuadran las preguntas del instrumento, para que este sea de su entero consentimiento.

Para ilustrar mejor, la tarea de los expertos consiste en valorar la relevancia de cata ítem, a través del uso de una escala que va de esencial, útil pero no esencial hasta no esencial; además se le anexo un espacio a un costado de cada pregunta, toda vez, los jueces puedan hacer sus observaciones de cada ítem.

Luego, el siguiente paso del método es, la contabilización de cada uno de los ítems señalados como esenciales por cada uno de los jueces, toda vez se logre determinar la Razón de Validez de Contenido, utilizando el siguiente enunciado y apoyados por el software Microsoft Excel Office 365.

$$CVR' = \frac{n_e}{N}$$

En resumen, el enunciado anterior, indica la proporción de acuerdo entre los jueces de la categoría “esencial”, respecto del número de participantes de la valoración, donde ***ne***= al número de jueces que tiene acuerdo en la categoría “esencial” y N= al número total de jueces; según el método, se deben considerar todos aquellos ítems que resultaron con CVR´ igual o superior a 0.58 y todos aquellos que no cumplen este criterio deben ser descartados.

Para finalizar, se calcula el CVI, relativo al conjunto del instrumento, como promedio de los CVR’ de todos los ítems del instrumento, con el enunciado; en este cálculo se incluyen los aceptables y no aceptables.

$$CVI = \frac{\Sigma_{i-1}^{m} CVRi}{M}$$

Luego, al obtener los resultados, producto del análisis de juicio de expertos, inicia el proceso de descarte de aquellos ítems que no cumplen con el criterio de este modelo, iniciando con el instrumento cuestionario, por lo que para este instrumento se presenta lo siguiente:

1. Se descarta el uso de ítem número 1, de identificación del informante, “Edad”, debido a que obtuvo un puntaje de 0.50, y eliminarlo no compromete los resultados.

2. El ítem número 11, de la variable delitos informáticos, ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias?, fue considerada no esencial por los jueces, también se descarta por que obtuvo un puntaje de 0.5, su eliminación tampoco compromete los resultados.

3. El ítem número 17, correspondiente a la variable delitos informáticos, ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico?, por sugerencia de los expertos se extiende a tres preguntas. Con el instrumento anterior se buscaba saber el grado de experiencia del cuentahabiente en aspectos tecnológicos específicos. Se sugiere separar este ítem en varias preguntas, toda vez que se puedan obtener resultados separados, por lo que se realiza el ajuste en base a estas observaciones.

Realizados los ajustes, de acuerdo con las observaciones hechas por los expertos, se procede al tiraje de un nuevo instrumento cuestionario de 18 ítems, el cual queda de la siguiente manera: 13 ítems a la variable delitos informáticos y 5 ítems a la variable operaciones de banca electrónica; Posteriormente, a este instrumento se le realizó una nueva prueba piloto a un grupo de 10 cuentahabientes.

Por otra parte, en cuanto al instrumento entrevista, se procede con el descarte de aquellos ítems que no cumplen con el criterio del modelo y se realizan los ajustes sugeridos por los expertos a los siguientes:

1. Se descarta el uso del ítem número 4, ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet?, ya que obtuvo un puntaje de 0.50 y su eliminación no compromete los resultados.

2. Se modifica el ítem número 6, quedando así, ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet?, por sugerencia de los expertos, con esta modificación lo que se busca es que el entrevistado indique los tipos de delitos informáticos identificados por los bancos.

3. Se extiende el ítem número 9, ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?, a tres preguntas, por sugerencia de los expertos, con la finalidad que se obtengan resultados separados con cada una de estas.

Realizados los ajustes, de acuerdo con las observaciones hechas por los expertos, se procede al tiraje de un nuevo instrumento entrevista de 11 ítems, quedando de la siguiente manera: 1 ítems a la variable delitos informáticos y 10 ítems a la variable operaciones de banca electrónica.

## Resultados de la validación

En cuanto a la validez del contenido de los ítems correspondientes al instrumento cuestionario, los resultados obtenidos destacan, un CVI global de 0.82, superior a 0.58 y por lo tanto aceptable en cuanto a la propuesta de Tristán (2008). De manera general, se puede apreciar que 5 de los 18 ítems tienen un puntaje máximo de 1, luego, 6 ítems un puntaje de 0.88, 4 ítems un puntaje de 0.75 y 3 ítems estuvieron por debajo del mínimo aceptable con un puntaje de 0.50.

Desde una perspectiva más particular, de los 3 ítems que estuvieron por debajo del mínimo aceptable 0.50, el ítem número 1, corresponde a identificación del informante “Edad”, por lo que no compromete los resultados de la investigación, al igual que el ítem número 11 de la variable delitos informáticos; En cuanto al ítem número 17, este a sugerencia de los expertos debe ser desglosado en tres preguntas separadas, por lo que se procedió a su debido ajuste.

Por otro lado, en cuanto al instrumento entrevista, los resultados obtenidos destacan un CVI global de 0.81, superior a 0.58 y por lo tanto aceptable en cuanto a la propuesta de Tristán (2008). De manera general, se puede apreciar que 2 de los 10 ítems tienen un puntaje máximo de 1, luego, 4 ítems un puntaje de 0.88, 2 ítems un puntaje de 0.75, 1 ítem un puntaje de 0.62 y 1 ítem estuvo por debajo del mínimo aceptable con un puntaje de 0.50.

Desde una perspectiva más particular, el ítem que estuvo por debajo del mínimo aceptable 0.50, el número 1, corresponde a la variable operaciones de banca electrónica, se descarta y no compromete los resultados de la investigación, al igual que el ítem número 6 de esta misma variable se modifica a sugerencia de los expertos, y cambia su sentido para obtener los tipos de delitos informáticos identificados por los bancos, al igual que el ítem número 9, el cual se desglosa en tres preguntas específicas, las cuales deben identificar las frecuencias en las que se realizan las evaluaciones de los riesgos tecnológicos, operacionales y legales.

En cuanto a la confiabilidad del instrumento, en este caso del cuestionario, se utilizará la herramienta conocida como el ***Alpha de Cronbach,*** apoyados de la herramienta denominada Software IBM SPSS Statistics, versión 23 el cual será aplicado

a las preguntas del cuestionario que contengan escala de ***Lykert***. A continuación, se muestra el cuadro con los resultados:

**Tabla 8**

*Estadísticas de fiabilidad.*

| Alfa de Cronbach | Alfa de Cronbach basada en elementos estandarizados | N de elementos |
|---|---|---|
| .625 | .627 | 2 |

Nota: esta tabla muestra la estadística de fiabilidad del estudio.

Señala Corral (2009) que

> El coeficiente de confiabilidad permite medir la consistencia interna de instrumentos de medición, en este caso del cuestionario, estadísticamente es un coeficiente de correlación y teóricamente significa la correlación del cuestionario consigo mismo; sus valores oscilan entre 0 y 1. También, presenta en este artículo una escala de interpretación que indica que el cuestionario será aplicable para la recolección de datos si la magnitud del Coeficiente de Confiabilidad es igual o mayor a 0,625, es decir, magnitud alta; según la escala recomendada, por lo que consideramos utilizar la prueba ya que el resultado obtenido de la misma es .625. (p.166)

Como se puede observar, la herramienta utilizada para verificar la confiabilidad del instrumento en este caso la encuesta, arroja un valor de 0.625 el cual es considerado como bueno para este.

Por consiguiente, los resultados de validez de contenido a través de juicio de experto y de confiabilidad a través del coeficiente de Alfa de Cronbach, se puede concluir que los instrumentos objeto de este estudio, cumplen con los requisitos suficientes para ser aceptable.

## Técnicas de procesamiento y análisis de datos

Los datos proporcionados por los cuestionarios y entrevistas serán procesados y analizados entre los meses de agosto y septiembre de 2020. Este análisis se hará mediante la clasificación de datos y el análisis estadístico. La clasificación de datos comprende: la codificación, la tabulación; por otro lado, el análisis estadístico permitirá determinar medidas o parámetros de tendencia central (Moda), correlaciones de las variables entre otras, las que se explicarán en los siguientes apartados.

Una vez obtenido los resultados de la encuesta, se procede a exportar los datos en una hoja de Microsoft Office Excel versión 2016 y estos posteriormente al programa estadístico IBM SPSS versión 23, es así como “en la etapa de recuento, se organizan y ordenan los datos obtenidos de la muestra. Esta será descrita en la siguiente etapa utilizando la estadística descriptiva, todas las investigaciones utilizan estadística descriptiva, para conocer de manera organizada y resumida las características de la muestra” (Juárez et al., 2002).

Por otro lado, cabe resaltar lo que señala Juárez et al. (2002), que

> La estadística, también, se puede clasificar como: paramétrica y no paramétrica. La estadística paramétrica: Está basada en dos supuestos: estimadores que son medidas referentes a la muestra como la media o la varianza y parámetros que son los equivalentes poblacionales de los estimadores, como la media y la varianza poblacionales.
>
> La estadística paramétrica necesita cumplir con cuatro requisitos para poderse aplicar:
>
> 1. La variable dependiente debe distribuirse normalmente (campana de Gauss) o muy similar.
> 2. Homocedasticidad u homogeneidad de varianzas o varianzas iguales: que cuando se comparan grupos estos tengan la misma dispersión con respecto a la media de la variable dependiente.
> 3. Asignación y selección aleatoria de los grupos (muestreo completamente al azar).
> 4. Que la variable dependiente esté medida a nivel intervalar o de razón.
>
> Estos requisitos deben ser cubiertos para poder generalizar con base en los estimadores y hacer conclusiones de una muestra a la población.
>
> Por otro lado, la estadística no paramétrica:
>
> 1. Está libre de curva, no necesita distribuirse como la curva normal.
> 2. Se basa en frecuencias, porcentajes, modas y rangos.
> 3. Su nivel de medición es ordinal o nominal. (p10)

De acuerdo con, lo anterior, para esta investigación se cumple el requisito que la clasifica como no paramétrica, ya que los niveles de medición en esta son ordinales y nominales; inmediatamente se procede a verificar si los niveles de distribución son normales o no normales, a través de la prueba Kolmogorov/Smirnof, obteniendo como resultado que la distribución en los niveles de medición es no normal.

**Tabla 9**

*Pruebas de normalidad Kolmogorov-Smirnov para muestras mayores de 50*

**Pruebas de normalidad**

| | Kolmogorov-Smirnov[a] (muestras mayores de 50) | | |
|---|---|---|---|
| | Estadístico | gl | **Sig.** |
| P1 ¿Qué tipo de servicios de banca por electrónica utiliza? | ,360 | 113 | ,000 |
| P2 ¿Qué tipo de servicios de banca por Internet utiliza con mayor frecuencia? | ,290 | 113 | ,000 |
| P3 ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | ,237 | 113 | ,000 |
| P12 De los tipos delitos enunciados señale ¿cúal considera causa mayores afectaciones a las operaciones de banca por Internet? | ,283 | 113 | ,000 |
| P13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | ,324 | 113 | ,000 |
| P10 De los delitos enunciados señale ¿Cuál considera el tipo más común que afecta a los servicios de banca por Internet | ,317 | 113 | ,000 |
| P11 De los delitos enunciados señale ¿cuál considera el tipo más común que afecta a los sistemas informáticos? | ,401 | 113 | ,000 |
| P8 ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | ,316 | 113 | ,000 |
| P5 ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? | ,318 | 113 | ,000 |
| P9 ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | ,284 | 113 | ,000 |
| P14 ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a usuarios de banca por Internet? | ,382 | 113 | ,000 |
| P6 ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet? | ,175 | 113 | ,000 |

| | | | |
|---|---|---|---|
| P7 ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | ,289 | 113 | ,000 |
| P4 ¿Consideras las compras por Internet seguras? | ,355 | 113 | ,000 |
| P15 ¿Posee alguna experiencia en el uso de redes de comunicación? | ,292 | 113 | ,000 |
| P16 ¿Posee alguna experiencia en el uso de sistemas de información? | ,309 | 113 | ,000 |
| P17 ¿Posee alguna experiencia en el uso de cualquier medio electrónico? | ,341 | 113 | ,000 |
| P18 ¿Posee algún mecanismo de protección en su computador o medio electrónico para evitar delitos informáticos? | ,226 | 113 | ,000 |

Nota: a. esta tabla nos muestra la Corrección de significación de Lilliefors

A continuación, se procedió a correr un Alfa de Cronbach para verificar la confiabilidad del instrumento el cual en esta ocasión arrojó un valor global de 0.680, lo cual es considerado bueno para esta investigación.

**Tabla 10**

*Estadísticas de fiabilidad.*

**Estadísticas de fiabilidad**

| Alfa de Cronbach | N de elementos |
|---|---|
| .680 | 18 |

Nota: esta tabla nos muestra la estadística de fiabilidad del estudio.

Adicional a esto, con los datos ordenados se procede a correr las tablas de frecuencias, al cual se realizó por ítem y por variables dimensiones, obteniendo con esta, resultados de las frecuencias y porcentajes que nos ayudará a calcular la medida de tendencia central denominada moda o frecuencia más alta.

**Tabla 11**

*Tabla de frecuencias*

**P10 De los delitos enunciados señale ¿Cuál considera el tipo más común que afecta a los servicios de banca por Internet**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Hackeo | 2 | 1,8 |
| | Robo de identidad (Phishing o Pharming) | 3 | 2,7 |
| | Malware | 50 | 44,2 |
| | Ataques dirigidos (Sniffing o Spoofing, Desfiguración de sitios web) | 58 | 51,3 |
| | Total | 113 | 100,0 |

Nota: esta tabla muestra la tabla de frecuencia para la pregunta 10.

Posterior a este, se realizó un análisis factorial exploratorio mediante el método de componentes principales para identificar los factores en los que tendían a agruparse los ítems que conformaron los constructos que se querían medir (Morales, 2011). De acuerdo con este cálculo se obtuvieron los factores, la carga factorial o correlación de cada ítem con cada factor (matriz factorial) y la proporción de la varianza que explica cada factor. También se aplicó el Método de rotación Varimax con normalización Kaiser, con el fin de obtener una estructura más simple e interpretable de los constructos al maximizar las correlaciones entre los ítems y los factores, y se procediera con la creación de las variables sumativas para realizar el análisis de relaciones.

**Tabla 12**

*Análisis factorial exploratorio mediante el método de componentes principales, método de rotación Varimax con normalización de Kaiser.*

**Matriz de componente rotado[a]**

| | Componente | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| P15 ¿Posee alguna experiencia en el uso de redes de comunicación? | .892 | | | | | | |
| P16 ¿Posee alguna experiencia en el uso de sistemas de información? | .865 | | | | | | |
| P17 ¿Posee alguna experiencia en el uso de cualquier medio electrónico? | .803 | | | | | | |
| P8 ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | | .845 | | | | | |
| P7 ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | | .790 | | | | | |
| P9 ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | | .642 | | | | | |
| P5 ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? | .330 | .567 | | | | | |
| P12 De los tipos delitos enunciados señale ¿cúal considera causa mayores afectaciones a las operaciones de banca por Internet? | | | .817 | | | | |
| P10 De los delitos enunciados señale ¿Cuál considera el tipo más común que afecta a los servicios de banca por Internet | | | .631 | | | | |
| P11 De los delitos enunciados señale ¿cuál considera el tipo más común que afecta a los sistemas informáticos? | | -.342 | .555 | | | | |
| P1 ¿Qué tipo de servicios de banca por electrónica utiliza? | | | | .756 | | | |
| P2 ¿Qué tipo de servicios de banca por Internet utiliza con mayor frecuencia? | | | | -.649 | | | |
| P13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | | | | | .760 | | |
| P18 ¿Posee algún mecanismo de protección en su computador o medio electrónico para evitar delitos informáticos? | | | | | .744 | | |
| P4 ¿Consideras las compras por Internet seguras? | | | | | | .892 | |
| P3 ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | .334 | | | .391 | | .439 | .365 |
| P14 ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a usuarios de banca por Internet? | | | | | | | .796 |
| P6 ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet? | | .306 | | .390 | | | .543 |

Nota: esta tabla muestra el método de extracción: análisis de componentes principales.
Método de rotación: Varimax con normalización Kaiser.

Una vez, ajustadas las variables se procede a correr la prueba de Chi cuadrado para una tabla 2x2, con la intención de establecer la asociación entre las variables de estudio. En la tabla 13 se presenta uno de los casos con mayor significancia.

**Tabla 13**

*Tabla cruzada/Chi cuadrado*

*Uso de los servicios financieros por Internet * Conocimiento informado*

**Tabla cruzada**

| | | | Conocimiento informado | | Total |
|---|---|---|---|---|---|
| | | | Con conocimiento informado | Sin conocimiento informado | |
| Uso de los servicios financieros por Internet | Mayor uso de servicios financieros | No, % | 44<br>68,8% | 30<br>61,2% | 74<br>65,5% |
| | Menor uso de servicios financieros | No, % | 20<br>31,3% | 19<br>38,8% | 39<br>34,5% |
| Total | | No, % | 64<br>100,0% | 49<br>100,0% | 113<br>100,0% |

**Pruebas de chi-cuadrado**

| | Valor | gl | Significación asintótica (bilateral) | Significación exacta (bilateral) | Significación exacta (unilateral) |
|---|---|---|---|---|---|
| Chi-cuadrado de Pearson | .695[a] | 1 | ,404 | | |
| Corrección de continuidad[b] | ,402 | 1 | ,526 | | |
| Razón de verosimilitud | ,693 | 1 | ,405 | | |
| Prueba exacta de Fisher | | | | ,430 | ,263 |
| Asociación lineal por lineal | ,689 | 1 | ,406 | | |
| N de casos válidos | 113 | | | | |

Nota: esta tabla muestra los resultados del cruce de variables, Uso de los servicios financieros por Internet * Conocimiento informado y su prueba de chi-cuadrado.

El cruce de las variables nos indicó cuales son las que poseen mayor significancia o relación entre sí, por lo que a continuación se presentan en la Tabla 15 el Extracto de correlaciones con mayor significancia, el cual nos servirá de apoyo en el capítulo IV, Discusión y Presentación de los resultados, para armar las hipótesis que darán respuesta a las variables de estudio.

**Tabla 14**

*Extracto de correlaciones con mayor significancia.*

| **Dimensiones / Variable dependiente** | **Variable independiente** | | | | |
|---|---|---|---|---|---|
| | Fraude informático | Falsificación informática | Magnitud de los daños | Conocimiento informado | Competencia tecnológica |
| **Tipo de los servicios financieros que utiliza** | 0.301 | 0.599 | 0.218 | 0.404 | 0.637 |
| **Frecuencia de uso de la banca por medio electrónicos** | 0.701 | 0.681 | ***0.095*** | 0.229 | ***0.050*** |
| **Afectaciones por delitos informáticos** | 0.081 | 0.970 | 0.973 | 0.262 | 0.288 |
| **Niveles de seguridad ofrecidos por los bancos** | 0.579 | ***0.012*** | ***0.000*** | ***0.001*** | ***0.012*** |
| **Variable dependiente** | **0.096** | **0.788** | **0.176** | **0.033** | **0.401** |

Nota: esta tabla muestra un extracto de las correlaciones con mayor significancia analizadas en la investigación.

Las discusiones de los resultados producto del análisis de la aplicación de las pruebas y el contraste de estos con las fichas de investigación y con las aportaciones de otros investigadores, se podrán apreciar en el capítulo siguiente.

# CAPÍTULO IV

# DISCUSIÓN Y PRESENTACIÓN DE RESULTADOS

“No existe la investigación perfecta, pero debemos tratar de demostrar que hicimos nuestro mejor esfuerzo. El reporte de investigación es la oportunidad para ello”, Hernández et al. (2014). Por lo que, con esta cita, damos inicio a la presentación de los resultados de la investigación y con ello, dar respuesta al planteamiento de la situación problemática presentada en esta.

En este apartado se introducirán los resultados, de las técnicas e instrumentos que fueron aplicados a los sujetos dentro del contexto de la investigación, los que serán comentados a partir de las respuestas a las dimensiones de las variables que tuvieron mayor contraste o alto grado de significancia y que lograron demostrar de esta forma, que se rechazara la hipótesis nula, dando respuesta tanto a la situación problemática planteada, como a los objetivos específicos para este estudio.

Además, se expondrán los resultados por objetivos de investigación, así como también frecuencias, porcentajes y tipos de delitos informáticos, considerados más comunes por los cuentahabientes, resultados que, también, serán contrastados con los de las entrevistas que se lograron obtener de profesionales del sector bancario y por las investigaciones y datos estadísticos recopilados a lo largo de esta investigación sobre esta temática.

## Resultados por dimensiones de variables de investigación

“El tratamiento de los datos de la investigación científica tiene varias etapas: En la etapa de recolección de datos del método científico, se define a la población de interés y se selecciona una muestra o conjunto de personas representativas de la misma”, (Juárez et al. 2002). Como mencionamos en el capítulo anterior, se emprende esta investigación con el enfoque en el que se desarrolla, el cual se puede ubicar como cuantitativo. En su tratamiento, se utilizaron técnicas de campo como encuestas y entrevistas para así obtener resultados que pudiésemos medir, comparar o hacer inferencias; cifras como porcentajes o proporciones, producto de aplicación a la unidad de análisis denominada sector financiero, el cual es representado por cuentahabientes y bancos de la ciudad de Panamá.

“En la etapa de recuento, se organizan y ordenan los datos obtenidos de la muestra. Esta será descrita en la siguiente etapa utilizando la estadística descriptiva, todas las investigaciones utilizan estadística descriptiva, para conocer de manera organizada y resumida las características de la muestra” […] “En la etapa de análisis se utilizan las pruebas estadísticas (estadística inferencial) y en la interpretación se acepta o rechaza la hipótesis nula”, Juárez et al. (2002).

En este sentido, los resultados obtenidos, de una muestra de 113 encuestados, fueron verificados, procesados y analizados para ver si se acepta o rechaza la hipótesis nula planteada, “La recurrencia, porcentaje, afectaciones contables y tipos de delitos,

impactan a los sistemas de información a través de las operaciones de banca por Internet de cuentahabientes de la ciudad de Panamá hasta 2020”

En lo que respecta a, las pruebas estadísticas utilizadas para la obtención de los resultados, se puede mencionar que, con la finalidad de identificar la adecuada, se aplicó el análisis de normalidad de los datos, denominado Kolmogorov-Smirnov, para muestras mayores de 50. Los resultados obtenidos, evidenciaron la necesidad de aplicar pruebas no paramétricas debido a que se obtuvo una distribución no normal de datos.

En cuanto a la parte de estadística inferencial de este estudio, “su propósito principal es estimar los atributos de la población a partir de una muestra de casos. Se pueden probar relaciones entre variables, comparar grupos con respecto a cierta característica y hacer inferencias”, Juárez et al. (2002), por lo que se procedió con la prueba de Chi cuadrado para una tabla 2x2, con la intención de establecer la asociación entre las variables de estudio y posteriormente la correlación de Pearson.

Como se menciona en el capítulo anterior, el cruce de las variables indicó cuáles son las que poseen mayor significancia o relación entre sí, datos presentados en la Tabla 15, denominada, Extracto de correlaciones con mayor significancia, del capítulo anterior, por lo que en este apartado, se procederá a la construcción de las hipótesis que dan respuesta a cada una de las dimensiones de las variables de estudio, hipótesis que se presentan a continuación en la Tabla 16, Construcción de Hipótesis por variable o Dimensión.

**Tabla 15**

*Construcción de hipótesis por variable o dimensión.*

| HIPÓTESIS NULA | | (Vp) | HIPÓTESIS ALTERNATIVA | |
|---|---|---|---|---|
| **$H_0$:** | No existe afectación entre la frecuencia de uso de la banca por medios electrónicos y el nivel de competencia tecnológica que tienen los cuentahabientes. | ***0.050*** | | Existe afectación entre la frecuencia de uso de la banca por medios electrónicos y el nivel de competencia tecnológica que tienen los cuentahabientes. |
| **$H_0$:** | No existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de competencia tecnológica que tienen los cuentahabientes. | ***0.637*** | **$H_1$:** | Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de competencia tecnológica que tienen los cuentahabientes. |
| **$H_0$:** | No existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento básico sobre la falsificación informática de los cuentahabientes. | ***0.012*** | **$H_1$:** | Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento básico sobre la falsificación informática de los cuentahabientes. |
| **$H_0$:** | No existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de afectación o magnitud de los daños a los cuentahabientes. | ***0.000*** | **$H_1$:** | Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de afectación o magnitud de los daños a los cuentahabientes. |
| **$H_0$:** | No existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento informado que tienen los cuentahabientes. | ***0.001*** | **$H_1$:** | Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento informado que tienen los cuentahabientes. |
| **$H_0$:** | No existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de competencia tecnológica que tienen los cuentahabientes. | ***0.012*** | **$H_1$:** | Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de competencia tecnológica que tienen los cuentahabientes. |

Nota: esta tabla muestra el constructo de hipótesis realizado por variable y dimensión el cual comprueba en cuales se rechazó de la hipótesis nula.

En cuanto a, los resultados por dimensión de las variables, se inicia con los de la dimensión de la variable dependiente, denominada: Frecuencia de uso de la banca por medio electrónicos, que se encuentra la pregunta #3 ¿Con que frecuencia utiliza los

servicios de banca a través de medios o canales electrónicos?, la cual se cruzó con la dimensión de la variable independiente, denominada Competencia Tecnológica, que encierra experiencias de compras por Internet seguras, en el uso de redes de comunicación, sistemas de información y cualquier medio o mecanismo electrónico por su alto grado de asociación, la cual mostro un Valor p (Vp) o significancia menor o igual a 0.05.

"Como regla de decisión, observando los resultados del paquete estadístico, a un nivel de significancia establecido en 0.05: Si la probabilidad o nivel de significancia es menor o igual a 0.05 se rechaza la hipótesis nula" (Juárez, Villatoro &López, 2002, p.15). Por lo que, con el desarrollo de esta dimensión de las variables de estudio podemos afirmar que se rechaza la hipótesis nula y se acepta de hipótesis de trabajo.

**Análisis del resultado:** podemos señalar que si existe afectación entre la frecuencia de uso de la banca por medios electrónicos y el nivel de competencia tecnológica que tienen los cuentahabientes.

**Interpretación del resultado:** por lo que se puede interpretar que sin importar el nivel de conocimientos que tengan los cuentahabientes sobre el uso de redes de comunicación, sistemas de información o cualquier mecanismo o medio electrónico, estos seguirán utilizándolos con mucha frecuencia y los cibercriminales se aprovecharán de estos usuarios inexpertos que realizan transacciones u operaciones por estos medios o canales electrónicos.

Sin embargo, llama a la atención que en cuanto a la dimensión denominada: Tipo de los servicios financieros que utiliza, la cual encierra la pregunta # 1 y 2, ¿Qué tipo de

servicios de banca por electrónica utiliza?, ¿Qué tipo de servicios de banca por Internet utiliza con mayor frecuencia?, cruzada con la dimensión de la variable independiente, Competencia Tecnológica, que agrupa experiencias de compras por Internet seguras, en el uso de redes de comunicación, sistemas de información y cualquier medio o mecanismo electrónico, que mostró un Valor p (Vp) o significancia mayor a 0.05.

**Análisis del resultado:** no arrojó un valor de significancia bajo por lo que el resultado nos indica que, no existe afectación entre los tipos de servicios financieros ofrecidos por los bancos y nivel de conocimientos que tengan o no los cuentahabientes sobre el uso de redes de comunicación, sistemas de información o cualquier mecanismo o medio electrónico.

**Interpretación del resultado:** lo que se puede interpretar como: sin importar los tipos de servicios ofrecidos por los bancos, llámese banca electrónica o por internet, no se ven afectados por el conocimiento o desconocimiento del cuentahabiente, en lo que se refiere a experiencias de compras por Internet seguras, en el uso de redes de comunicación, sistemas de información y cualquier medio o mecanismo electrónico.

En el siguiente análisis se presenta, la dimensión de la variable dependiente denominada: Niveles de seguridad ofrecidos por los bancos, la cual encierra la pregunta #13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, cruzada con la dimensión de la variable independiente, Falsificación informática, Magnitud de los daños, conocimiento informado, competencia tecnológica. En este cruce se puede apreciar los valores de significancia (Vp) más bajos obtenidos. Por lo que procede a realizar el análisis de cada una de ellas, iniciando con la falsificación informática.

En cuanto al cruce de la pregunta #13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, con la variable independiente Falsificación informática, que encierra la pregunta #8 ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá?, mostro un Valor p (Vp) o significancia menor o igual a 0.05, en este caso el (Vp) fue de 0.012.

**Análisis de los resultados:** el cruce de estas variables arrojó un Vp por debajo del valor aceptable según las reglas de decisión, por lo que podemos decir que: Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento básico sobre la falsificación informática de los cuentahabientes.

**Interpretación del resultado:** Lo que se puede interpretar como: No existe una adecuada información o divulgación, en cuanto a los pasos a seguir para presentar las denuncias por los delitos informáticos, de parte de los bancos panameños.

En el cruce de la pregunta #13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, con la variable independiente denominada: Magnitud de los daños, en la que encierra preguntas como ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? y ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? mostró un Valor p (Vp) o significancia menor o igual a 0.05, en este caso el (Vp) fue de 0.000, siendo esta la de más alta significancia, de acuerdo a las reglas de decisión.

**Análisis de los resultados:** para el cruce de estas variables su resultado indica que: Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de afectación o magnitud de los daños a los cuentahabientes.

**Interpretación de los resultados:** Lo que se puede interpretar como: No existe una adecuada información o divulgación por parte de las entidades bancarias, que permitan darle seguimiento a las denuncias por los delitos informáticos, de parte de los bancos panameños, así como se confirma que no existe algún conocimiento por el cuentahabiente, sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet.

En el cruce de la pregunta #13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, con la variable independiente denominada: Conocimiento informado, mostró un Valor p (Vp) o significancia menor o igual a 0.05, en este caso el (Vp) fue de 0.001, siendo esta la segunda de más alta significancia, de acuerdo con las reglas de decisión.

**Análisis de los resultados:** para el cruce de estas variables su resultado indica que: Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de conocimiento informado que tienen los cuentahabientes.

**Interpretación de los resultados:** Lo que se puede interpretar como: No existe una adecuada información o divulgación por parte de las entidades bancarias, que permitan dar conocimiento al cuentahabiente, sobre los riesgos producto del mal uso del Internet y sobre las regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos.

En el cruce de la pregunta #13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, con la variable independiente denominada: Competencia tecnológica, prfesentó un Valor p (Vp) o significancia menor o igual a 0.05, en este caso el (Vp) fue de 0.012, de acuerdo a las reglas de decisión.

**Análisis de los resultados:** para el cruce de estas variables su resultado indica que: Existe afectación entre los niveles de seguridad ofrecidos por los bancos y el nivel de competencia tecnológica que tienen los cuentahabientes.

**Interpretación de los resultados:** Lo que se puede interpretar como: No existe una adecuada información o divulgación por parte de las entidades bancarias, que permitan al cuentahabiente, ampliar sus conocimientos sobre el uso de sistemas de información, de cualquier mecanismo o medio electrónico ya sea de protección en su computador o dispositivo electrónico que contribuya a evitar delitos informáticos.

De esta forma, culminamos la discusión de los resultados por dimensiones de cada variable y proseguimos con el análisis de los objetivos planteados en esta investigación.

## Resultado por objetivos de la investigación

En este apartado se expondrán, los resultados de acuerdo con los objetivos planteados para esta investigación, por lo cual a continuación presentaremos y desarrollaremos estos.

El objetivo general de esta investigación es: Valorar el impacto que generan en los sistemas de información contables, los delitos informáticos a través de las operaciones de banca por Internet en la ciudad de Panamá para lograr ejercer un mayor control de estos. Para la consecución del objetivo planteado en la investigación, se diseñaron una serie de objetivos específicos, que, en el desarrollo de esta, nos sirvieron de guía para la consecución de este, los cuales en su orden son:

Identificar cuáles son los tipos de delitos informáticos que impactan a los sistemas de información a través de las operaciones de banca por Internet y los sistemas informáticos en la ciudad de Panamá hasta 2020.

Analizar, cuál de los tipos de delitos informáticos identificados, causa mayores afectaciones a las operaciones de Banca por Internet hasta 2020.

Determinar la forma de mitigar los riesgos producto de los delitos informáticos.

Partiendo por, el análisis del primer objetivo específico, lo que se buscó fue, identificar cuáles son los tipos de delitos informáticos que impactan a los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá y sus repercusiones, por lo que en esta ocasión haremos uso de la estadística descriptiva.

En este sentido, señala Juárez et al. (2002), que la Estadística Descriptiva, “permite la organización de datos desestructurados de tal manera que sean más fáciles de interpretar y de conocer las características de una muestra de forma rápida y resumida” […] “Incluye: Tablas de frecuencias y porcentajes, Métodos de resumen o numéricos que se dividen en: Medidas de tendencia central y Medidas de dispersión, y Gráficos” (p.4,5).

Para lograr identificar, cuáles son los tipos de delitos informáticos que impactan a los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá, se utilizó la prueba estadística denominada tabla de frecuencias, aplicada a la muestra de 113 cuentahabientes encuestados. En este instrumento se diseñó dos preguntas para captar la precepción del encuestado de acuerdo con su experiencia en el uso de medios o canales electrónicos. La pregunta #10, que va dirigida a las afectaciones a los servicios de banca por Internet y que en el instrumento se describe así: De los delitos enunciados señale ¿Cuál considera el tipo más común que afecta a los servicios de banca por Internet? Y la #11, que va dirigida a las afectaciones a los sistemas informáticos, la cual en el instrumento se describe así: De los delitos enunciados señale ¿cuál considera el tipo más común que afecta a los sistemas informáticos?

El resultado se presenta continuación en la Tabla 17 Frecuencia de los tipos de delitos que afectan las operaciones de banca por Internet en la ciudad de Panamá hasta 2020.

**Tabla 16**

*Frecuencia de los tipos de delitos que afectan las operaciones de banca por Internet en la ciudad de Panamá hasta 2020.*

**P#10 De los delitos enunciados señale ¿Cuál considera el tipo más común que afecta a los servicios de banca por Internet**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Hackeo | 2 | 1,8 |
| | Robo de identidad (Phishing o Pharming) | 3 | 2,7 |
| | Malware | 50 | 44,2 |
| | Ataques dirigidos (Sniffing o Spoofing, Desfiguración de sitios web) | 58 | 51,3 |
| | Total | 113 | 100,0 |

**P#11 De los delitos enunciados señale ¿cuál considera el tipo más común que afecta a los sistemas informáticos?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Piratería informática | 8 | 7,1 |
| | Malware | 7 | 6,2 |
| | Ransomware | 21 | 18,6 |
| | Ataques dirigidos (Sniffing o Spoofing, Desfiguración de sitios web) | 77 | 68,1 |
| | Total | 113 | 100,0 |

Nota: esta tabla muestra con qué frecuencia y que tipo de delito son más comunes al servicio de banca por internet y a los sistemas informáticos.

**Análisis del resultado:** En cuanto a la pregunta #10, se puede observar que, en la frecuencia de encuestados, 58 de 113, que representa el 51,3%, de estos, opinó que los Ataques dirigidos es el tipo de delito más común que afectan a los servicios de banca por Internet, seguido de Malware con una frecuencia de 50 de 113 encuestados, que representa el 44,2%, el resto de los delitos enunciados no es representativo.

En cuanto a la pregunta #11, se puede observar que, en la frecuencia de encuestados, 77 de 113, el cual representa el 68,1% de estos, opinó que los Ataques dirigidos son el tipo más común que más afectan a los Sistemas informáticos, seguido del Ransomware con una frecuencia de 21 de 113 encuestado, que representa el 18,6%, el resto de los delitos enunciados no es representativo.

**Interpretación de los resultados:** Por lo que, para el desarrollo del primer objetivo específico, el cual busca identificar de los tipos de delitos más comunes, ¿Cuáles impactan los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá hasta 2020?, podemos afirmar que son: los Ataques dirigidos, el Malware y el Ransomware respectivamente, según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos.

En cuanto a, el desarrollo del segundo objetivo específico, este va ligado al anterior, toda vez que para saber ¿Cuál es el delito informático que causa mayor impacto?, debemos primero saber ¿Cuáles de estos son los tipos más comunes que afectan los sistemas de información a través de las operaciones de banca electrónica?

Teniendo una respuesta despejada para la primera incógnita, presentamos la Tabla 18, denominada frecuencia de los tipos de delitos que causan mayores afectaciones a las operaciones de banca por Internet, que nos ayudara a presentar el resultado de la siguiente incógnita, la cual con el análisis de pregunta #12, De los tipos delitos enunciados señale ¿Cuál considera causa mayores afectaciones a las operaciones de banca por Internet? Podremos describir.

**Tabla 17**

*Frecuencia de los tipos de delitos que causan mayores afectaciones a las operaciones de banca por Internet.*

**P#12 De los tipos delitos enunciados señale ¿cuál considera causa mayores afectaciones a las operaciones de banca por Internet?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Hackeo | 12 | 10,6 |
| | Robo de identidad (Phishing o Pharming) | 4 | 3,5 |
| | Malware | 49 | 43,4 |
| | Ataques dirigidos (Sniffing o Spoofing, Desfiguración de sitios web) | 48 | 42,5 |
| | Total | 113 | 100,0 |

Nota: esta tabla nos muestra la frecuencia de los tipos de delitos informáticos que causan mayores afectaciones a las operaciones de banca por internet.

**Análisis de los resultados:** En cuanto a la pregunta #12, De los tipos delitos enunciados señale ¿cuál considera causa mayores afectaciones a las operaciones de banca por Internet?, podemos observar que existe una frecuencia de 49 de 113, el cual representa el 43,4% de los encuestados, que afirman según su experiencia y conocimientos en cuanto al uso de medios o canales electrónicos, el delito informático que causa mayor afectación a las operaciones de banca por Internet es el Malware, seguido muy de cerca por los Ataques dirigidos con una frecuencia de 48 de 113 encestados, lo que representa el 42,5% de los encuestados.

**Interpretación de los resultados:** Por lo que, para el desarrollo del segundo objetivo específico, el cual busca, de los tipos de delitos identificados, ¿cual afecta mayormente

las operaciones de banca por Internet en la ciudad de Panamá hasta 2020?, podemos afirmar que son: el Malware seguido muy de cerca por los Ataques dirigidos, según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos.

En cuanto al desarrollo del último objetivo específico, Determinar la forma de mitigar los riesgos producto de los delitos informáticos, se pretende hacer varias observaciones en cuanto al análisis de este.

Vamos a iniciar por presentar el análisis e interpretación de los resultados de las preguntas que nos ayudarán a realizar sugerencias en apartados posteriores, en cuanto a la forma de mitigar los riesgos producto de los delitos informáticos; estas frecuencias y porcentajes se muestran en la Tabla 19, denominada, Frecuencias y porcentajes por preguntas.

**Tabla 18**

*Frecuencias y porcentajes por preguntas.*

**P1 ¿Qué tipo de servicios de banca por electrónica utiliza?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Tarjeta Bancaria (Visa/Clave) | 15 | 13,3 |
| | Terminales de punto de venta (POS) | 3 | 2,7 |
| | Banca por teléfono | 5 | 4,4 |
| | Banca Móvil | 19 | 16,8 |
| | Banca en línea | 71 | 62,8 |
| | Total | 113 | 100,0 |

**P2 ¿Qué tipo de servicios de banca por Internet utiliza con mayor frecuencia?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Transferencias | 37 | 32,7 |
| | Pagos a terceros | 61 | 54,0 |
| | Compras por Internet | 15 | 13,3 |
| | Total | 113 | 100,0 |

**P3 ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nunca | 1 | ,9 |
| | Casi nunca | 1 | ,9 |
| | Algunas veces | 22 | 19,5 |
| | Casi siempre | 45 | 39,8 |
| | Siempre | 44 | 38,9 |
| | Total | 113 | 100,0 |

**P4 ¿Consideras las compras por Internet seguras?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nada | 14 | 12,4 |
| | Poco | 77 | 68,1 |
| | Mucho | 22 | 19,5 |
| | Total | 113 | 100,0 |

**P5 ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nada | 14 | 12,4 |
| | Poco | 67 | 59,3 |
| | Mucho | 32 | 28,3 |
| | Total | 113 | 100,0 |

**P6 ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nunca | 10 | 8,8 |
| | Casi nunca | 14 | 12,4 |
| | Algunas veces | 29 | 25,7 |
| | Casi siempre | 26 | 23,0 |
| | Siempre | 34 | 30,1 |
| | Total | 113 | 100,0 |

**P7 ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nada | 49 | 43,4 |
| | Poco | 56 | 49,6 |
| | Mucho | 8 | 7,1 |
| | Total | 113 | 100,0 |

**P8 ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nada | 56 | 49,6 |
| | Poco | 48 | 42,5 |
| | Mucho | 9 | 8,0 |
| | Total | 113 | 100,0 |

**P9 ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nunca | 17 | 15,0 |
| | Casi nunca | 35 | 31,0 |
| | Algunas veces | 55 | 48,7 |
| | Casi siempre | 5 | 4,4 |
| | Siempre | 1 | ,9 |
| | Total | 113 | 100,0 |

**P13 ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Totalmente en desacuerdo | 2 | 1,8 |
| | Parcialmente en desacuerdo | 14 | 12,4 |
| | Ni de acuerdo ni en desacuerdo | 18 | 15,9 |
| | Parcialmente de acuerdo | 61 | 54,0 |
| | Totalmente de acuerdo | 18 | 15,9 |
| | Total | 113 | 100,0 |

**P14 ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a usuarios de banca por Internet?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Totalmente en desacuerdo | 2 | 1,8 |
| | Parcialmente en desacuerdo | 3 | 2,7 |
| | Ni de acuerdo ni en desacuerdo | 6 | 5,3 |
| | Parcialmente de acuerdo | 27 | 23,9 |
| | Totalmente de acuerdo | 75 | 66,4 |

| | | | |
|---|---|---|---|
| | Total | 113 | 100,0 |

**P18 ¿Posee algún mecanismo de protección en su computador o medio electrónico para evitar delitos informáticos?**

| | | Frecuencia | Porcentaje |
|---|---|---|---|
| Válido | Nunca | 13 | 11,5 |
| | Casi nunca | 10 | 8,8 |
| | Algunas veces | 20 | 17,7 |
| | Casi siempre | 32 | 28,3 |
| | Siempre | 38 | 33,6 |
| | Total | 113 | 100,0 |

Nota: esta tabla muestra las frecuencias y porcentajes de todas las preguntas formuladas para la investigación.

**Análisis de los resultados:** Iniciamos el análisis de los resultados, respetando el orden en que están planteadas las preguntas, siendo así, las preguntas #1, 2 y 3, guardan mucha relación, y tienen que ver con las preferencias de los cuentahabientes, en cuanto a los tipos de servicios de banca electrónica, y banca por Internet y su frecuencia de uso.

Es así, como en la pregunta #1, ¿Qué tipo de servicios de banca electrónica utiliza?, se puede notar que hay tres escalas con niveles significativos para esta, entre los que se puede mencionar que la Banca en línea, o por Internet es la de mayor preferencia en uso por los cuentahabientes que manejan este tipo de medios electrónicos; 71 de 113 encuestados, con un porcentaje de 62,8% manifestó utilizar esta, seguido por la Banca móvil, en la que 19 de 113 encuestados, representando un 16,8%, manifestó usarla y la Tarjeta Bancaria (Visa/Clave), con 15 de 113 encuetados, representando un 13,3%, manifestó su preferencia.

Ya que, la Banca en línea o por Internet, es la que obtuvo mayor preferencia por los encuestados, dirigimos el estudio a la pregunta #2, ¿Qué tipo de servicios de banca por Internet utiliza con mayor frecuencia?, toda vez se pueda observar las frecuencias de uso de esta; es así como vemos que los cuentahabientes 61 de 113, que representa un 54,0%, manifestaron que con frecuencia realizan pagos a terceros, 37 de 113, indicaron que prefieren realizar transferencias, el cual representa un 32,7% y las compras por Internet no se quedan atrás con una preferencia de 15 de 113, el 13,3% de preferencia, este resultado va de la mano o confirma el resultado de la pregunta #4, ¿Consideras las compras por Internet seguras?, que analizaremos a continuación.

En cuanto a, la frecuencia de uso de la banca a través de medio o canales electrónicos, estudiada en la pregunta #3, ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos?, podemos observar que 39,8 de 113 encuestados, manifestó que Casi siempre utiliza los servicios de banca electrónica, el cual representa un 39,8% de preferencia.

**Interpretación de los resultados:** se puede interpretar los resultados para las preferencias de los cuentahabientes de la siguiente manera; Ya que, el 63% de los encuestados manifestó su preferencia por la Banca en línea o por Internet; de los servicios que se prestan por esta, 54% de los encuestados, manifestaron que con frecuencia realizan transferencias a través de la banca en línea o por Internet, y el 40%, manifestó usar casi siempre la banca electrónica o por Internet, podemos afirmar que existe una alta preferencia por parte de los usuarios de medios o canales electrónicos por el uso de la Banca en línea o por Internet.

En cuanto a, las preguntas #4, 5, 6, 7, 8, y 9, se basan en obtener del encuestado, que ya manifestó su preferencia por el uso de medio o canales digitales, si este tiene algún grado de conocimiento en cuanto a algunos aspectos de seguridad; Aspectos como, si las compras por Internet son seguras, si conocen o saben que son delitos informáticos, si los bancos le informan de los riesgos que corren por el mal uso de los servicios de banca a través de medios o canales electrónicos, si conocen las Leyes y pasos a seguir para realizar las denuncias y si se les da seguimiento a estas.

**Análisis de los resultados:** En cuanto a, la pregunta #4, ¿Consideras las compras por Internet seguras?, y para dar seguimiento, se puede apreciar que de los 113 encuestados 77, que representa un 68,1%, consideran que las Compras por Internet son poco seguras, resultado que guarda mucha concordancia con el obtenido en la pregunta #2, sobre qué tipo de servicio a través de Banca por Internet usa con mayor frecuencia y en el que las compras por Internet obtuvieron el menor porcentaje.

En cuanto a la pregunta #5, ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet?, 67 de 113 encuestados, lo cual representa un 59,3% de los cuentahabientes, manifestó que posee poco conocimiento, a cerca de los delitos informáticos que puedan afectar sus bienes a través de la banca por Internet.

En cuanto a, conocimiento de los riesgos, analizados en la pegunta #6, ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet?, 34 de 113 encuestados, lo que representa un 30,1%, indicaron que siempre se les ha informado de los riesgos producto del mal uso de la banca por Internet, podemos apreciar en la prueba estadística para esta pregunta, que los resultados son muy parejos, en cuanto a si las entidades financieras informan o no al cuentahabiente sobre los riesgos; Más aún, las cifras se inclinan, a que no hay una adecuada información de estos riesgos, a pesar que los encuestados manifestaron que sí se les ha informado, estimación que hacemos por los resultados de las preguntas #7 y 8, respectivamente.

Para dar continuidad, a lo que se refiere al conocimiento que poseen los cuentahabientes de medios o canales electrónicos, pasamos al análisis de las preguntas #7 y 8, respectivamente y que nos ayudarán a ampliar el análisis de los resultados de la pregunta #6. Siendo así, iniciamos con la pregunta #7, ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos?, para esta pregunta 56 de 113 encuestados, lo cual representa un 49,6% indicaron que no tienen conocimiento de regulaciones o Leyes que les ayuden a proteger sus bienes de delitos informáticos, seguido de 49 de 113, encuestados manifestaron, no saber nada, en cuanto a regulaciones o Leyes, los que representan un 43,4% de los cuentahabientes. En cuanto a la pregunta #8, ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá?, con un resultado de 56 de 113 encuestados, el cual representa un 49,6%, indicaron que nada, seguido de 48 de 113 encuestados lo cual representa el 42,5% de los encuestados, informaron que poco.

Para concluir, con las preguntas que corresponden al conocimiento de los cuentahabientes en cuanto aspectos de los delitos informáticos, analizamos la pregunta # 9, ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá?, en la que se puede apreciar que los resultados se inclinan a que no se les da seguimiento ya que 55 de 113 encuestado, que representan un 48,7%, afirma que algunas veces, 35 de 113, que representa el 31,0%, afirma que casi nunca y 17 de 113, que representa un 15,0% afirma que nunca, por lo que se hace evidente la inclinación de los encuestados hacia el seguimiento que se les hace a este tipo de denuncias.

**Interpretación de los resultados:** Con los resultados analizados, podemos afirmar que los cuentahabientes poseen un bajo conocimiento acerca de los delitos informáticos, consideran las compras por Internet como poco seguras, y aunque muchos manifestaron que las entidades financieras donde poseen sus cuentas les informan sobre los riesgos que corren producto del mal uso de la Banca en línea o por Internet, al analizar las preguntas siguientes, los resultados indican que no saben sobre regulaciones o leyes, no saben cuáles son los pasos a seguir para presentar una denuncia por delitos informáticos y consideran que no se les da seguimiento a las denuncias por delitos informáticos. Por lo que, es un claro indicativo que no se les está brindando a los cuentahabientes una adecuada información para que este tenga conocimiento de los riesgos que representa el mal uso de la Banca en línea o por Internet.

En cuanto a, seguridad, analizaremos las preguntas #13, 14 y 18, toda vez podamos verificar, como perciben los cuentahabientes los niveles de seguridad ofrecidos por los bancos, si se hacen responsables por daños u afectaciones ocurridas a sus

cuentas y que niveles de seguridad poseen estos en su computador, toda vez puedan hace frente a cualquier tipo de delito o ataque informáticos.

**Análisis de los resultados:** Iniciamos con la pregunta #13, ¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?, los resultados de esta pregunta indican que 61 de 113 encuestados, los cuales representan un 54,0%, afirman que están parcialmente de acuerdo en que son adecuados. Para la pregunta #14, ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a usuarios de banca por Internet?, en la cual 75 de 113 encuestados, los que representan un 66,4%, porcentaje más alto en todo el estudio, afirman que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a cuentahabientes usuarios de Banca en línea o por Internet. Y respecto a la pregunta #18, ¿Posee algún mecanismo de protección en su computador o medio electrónico para evitar delitos informáticos?, muestra porcentajes bastante parejos en cuanto s su uso, de los cuales destacamos que 38 de 113, el cual corresponde al 33,6% de los encuestados, señala que siempre hace uso de mecanismos de protección en su computador para evitar delitos informáticos, 32 de 113, que representa el 28,3% de los encuestados señala que casi siempre y 20 de 113, que representa un 17,7%, afirma que algunas veces, conformando así la representatividad de esta pregunta.

**Interpretación de los resultados:** Los aspectos de seguridad, tanto del Banco que ofrece el servicio como del usuario o cuentahabiente, son muy importantes, en este sentido, se ha investigado las medidas de seguridad que ofrecen estos a sus clientes de

medios electrónicos para que los servicios sean utilizados de forma segura, sin embargo, el usuario debe seguir estos lineamientos de seguridad y mantener precaución en su uso; Según los resultados obtenidos en base a estas preguntas podemos afirmar que en muchas ocasiones los usuarios no siguen estas medidas o no implementan las mismas en los equipos que utilizan para realizar sus operaciones, ya sea por falta de recursos económicos, negligencia y en muchos casos la inexperiencia de estos, ocasiona que queden en el blanco de cibercriminales que están al asecho de estas fallas de seguridad para realizar su ataques.

## Contraste de resultados con entrevista a expertos en área de riesgo tecnológico

Como mencionamos en líneas anteriores, por efectos de la Pandemia denominada Covid-19, que ha afectado el mundo entero y nuestro país, se vio afectada considerablemente, la consecución de resultados por medio de la aplicación del instrumento denominado entrevista, la cual estaba dirigida a expertos Gerentes de Riesgos en el área tecnológica de bancos de la localidad.

De un total de setenta y dos (72) entrevistas que se tenía planeado realizar, sólo se obtuvieron dos (2), ya que las instituciones bancarias por orden del Ministerio de Salud cerraron sus puertas a la atención al público en las fechas indicadas para realizar estas. Sin embargo, se logró contactar a dos expertos, los cuales cuentan con muchos años de experiencia en el sector de riesgos bancarios, y en el área de tecnología; Por lo que se procedió a realizar dichas entrevistas a estos expertos a través de la plataforma digital

denominada Zoom, una el 24 de septiembre y la segunda el 8 de octubre respectivamente.

Los resultados de las entrevistas obtenidas serán comparados con los de la investigación y con los recabados de otros autores, de manera que se pueda ampliar aún más, con algunas experiencias por parte del sector financiero en cuanto al manejo de los riesgos por los bancos en el área tecnológica.

En relación con, los resultados obtenidos de las entrevistas, la primera fue realizada a un experto en el área de riesgos y vicepresidente ejecutivo de una compañía panameña, dedicada a prestar servicios de consultoría a diferentes tipos de organizaciones, incluyendo, los principales bancos de la localidad. Esta entrevista es enfocada a aspectos como riesgo tecnológico, seguridad de la información y auditoría interna de sistemas y al cual para esta investigación denominaremos el entrevistado #1.

Al efectuar esta, el entrevistado #1, nos indicó lo siguiente: La compañía que preside, fue fundada hace 11 años y los cuatro pilares fundaméntales sobre la que se basa esta, para la prestación de sus servicios menciona este que descansan en: la gestión de riesgo tecnológico, la seguridad de la información, la auditoría interna de sistemas y en la actualidad y debido a la gran demanda que se ha dado por los bancos y organizaciones, producto de los grandes avances tecnológicos, y de la prestación de servicios digitales, a investigar los delitos informáticos, de los que son victima estos, por lo que los datos recabados encajan con el perfil de esta investigación, toda vez que los servicios prestados por esta compañía se dirigen exactamente al estudio de los delitos

informáticos y los riesgos que estos implican a los sistemas de información que utiliza el sector financiero.

La segunda entrevista fue realizada a un experto con muchos años de experiencia y amplio conocimiento en cuanto al manejo del sector financiero de nuestro país, específicamente en el área de riesgo tecnológico de bancos; su experiencia nos ayudará a comprender algunos procedimientos operativos en cuanto a la gestión de riesgos en el área tecnológica de estos, lo cual será de gran utilidad ya que sus datos podrán ser contrastados con los resultados obtenidos de los otros instrumentos, el cual denominaremos el entrevistado #2.

Como mencionamos en apartados anteriores, el diseño del guion de la entrevista aplicada contiene diez (10) preguntas, que fueron aplicadas a ambos entrevistados mismas que serán analizadas, interpretadas y presentados sus resultados en este apartado.

Iniciamos este, con el análisis a la pregunta número #1, ¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por internet?, esta va dirigida a saber sobre la influencia que tienen los delitos informáticos a las operaciones de banca por internet, y aunque se comprenda que la influencia de estos, es negativa tanto a las operaciones de banca por internet como a los sistemas de información, se analizarán los comentarios de los expertos de sus experiencias en torno a estos.

**Análisis de los resultados:** En este sentido, menciona el entrevistado #1, que el impacto de una reincidencia en delitos informáticos en una institución financiera, seria sin lugar a duda negativo, ya que se puede ocasionar violaciones de acuerdos bancarios que tiene la entidad que cumplir con la SBP, además de violaciones a compromisos y aseveraciones contractuales firmadas entre la institución financiera y los usuarios, las cuales pueden desembocar en demandas penales y civiles por afectaciones a estos últimos.

Por otro lado, el entrevistado #2, señala que, toda persona que maneja una cuenta a través de estos medio o canales electrónicos corre el riesgo de ocurrencia de algún fraude informático. En ese sentido la SBP, realiza un balance en cuanto a cantidad y exposición del riesgo; esta medición se realiza ya que los bancos deben reportar las ocurrencias de incidentes de seguridad y de fraude, pues forman parte de sus pérdidas. Factores como el ambiente de control de los bancos son incluidos en este balance, cuyo objetivo es medir su eficiencia y eficacia, ya que los bancos deben gestionar por riesgos y esta gestión debe incluir aspectos como infraestructura organizativa que atienda la seguridad, las políticas y procedimientos que giran hacia esa gestión.

**Interpretación de los resultados:** A pesar que en el desarrollo de la pregunta #1, no se obtuvieron cifras en cuanto a la influencia de los delitos informáticos a las operaciones de banca por internet, sin lugar a duda, las entidades financieras y sus sistemas de información se ven impactados por estos, toda vez, cabe la posibilidad que incurran en violaciones de acuerdos bancarios y compromisos contractuales que pueden

desembocar en demandas penales y civiles por parte de los cuentahabientes afectados por estos delitos.

En cuanto a la pregunta #2, ¿Maneja la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica?, la cual busca saber si las entidades financieras manejan registro de estos datos.

**Análisis de los resultados:** Señala el entrevistado #1, que, pudiese la SBP o la Asociación Bancaria de Panamá, mantener datos estadísticos sobre los delitos que son más recurrentes a las operaciones de banca electrónica, pero estos datos no son divulgados ni disponibles al público, sin embargo, la información accesible sobre estos, es la que ofrecen las fiscalías en Panamá, y que en la mayoría de los casos son cifras no actualizadas que corresponden a años anteriores, datos que han sido recabados producto de las denuncias y en los que se pudo percatar, en ese entonces, que los accesos no autorizados a cuentahabientes de banca por internet estaban en aumento.

Mientras tanto el entrevistado #2, si bien cierto, en la pregunta anterior señaló que no es autorizado a revelar cifras de datos estadísticos, si nos comentó que los bancos deben reportar las incidencias de este tipo de delitos a SBP, datos que utiliza esta para realizar comparaciones o balances, banco a banco, entre el uso de los canales y los fraudes cometidos en estos y así determinar fallas y realizar sugerencias e intervenciones.

**Interpretación de los resultados:** Es evidente entonces, que, si cabe la posibilidad de que existan datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica, pues el entrevistado #2, señalo que realizan comparaciones con datos presentados por los bancos, de incidencias de fraudes por delitos informáticos a la banca electrónica; datos que no son divulgados ni publicados por las entidades bancarias; es así como este resultado, crea concordancia a lo señalado por (Contreras et al, 2019, p.18), "se hace evidente la gran importancia que tiene la ciberseguridad para el sector financiero, en cuanto a la confiabilidad que estos deben proyectar y garantizar hacia sus clientes en el entorno digital como un espacio confiable para la realización de sus operaciones, toda vez, las inversiones realizadas en procesos de digitalización de servicios al cliente, no generarían el impacto positivo esperado, debido a la desconfianza en el uso de canales digitales".

Conviene subrayar, que, otra forma de poder conocer estos datos, aunque no actualizados, es a través de las denuncias emitidas por los cuentahabientes a las instituciones de seguridad del país. En este caso el entrevistado #1, señaló que entre los datos a los que tuvo acceso de años anteriores, producto de sus investigaciones, asesorías y consultorías, por peritajes solicitados por sus clientes, las denuncias por el acceso no autorizado a las operaciones de banca por internet, específicamente a las transferencias de dinero estaban en aumento.

En cuanto a, la pregunta #3, ¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por internet?, en la que se busca conocer de mano del sector financiero ¿Cuáles son los controles ofrecidos por

estos a sus usuarios que manejan este tipo de servicios a través de canales digitales o electrónicos?, se obtuvo el siguiente resultado.

**Análisis de los resultados:** Iniciando con la respuesta del entrevistado #1, a esta pregunta, señaló que los bancos ofrecen mecanismos de autenticación segura y en ocasiones de doble autenticación, en los que se requiera, para que el cliente cuando acceda a los servicios a través de medios o canales digitales, lo haga de manera segura. Además, conoce que, por regulación, estos deben mantener sistemas de información que les permitan identificar oportunamente operaciones atípicas por accesos indebido, para tratar de reducir a niveles aceptables los riesgos por parte del cliente, pues estos en su totalidad nunca se podrán mitigar.

Por otro lado, el entrevistado #2, señala que para que un cliente realice una operación a través de medios o canales digitales, este debe contar con mecanismos de autenticación, entre los que mencionó el Token digital, dispositivo personalizado de autenticación que el cliente solo posee y que le permite mayor seguridad al realizar sus operaciones a través de la banca por internet. Este dispositivo tiene como función principal impedir o hacer que al delincuente le cueste más trabajo lograr acceder a las cuentas, reduciendo así los niveles de riesgo de fraude en estos tipos de operaciones, además los bancos deben contar con un equipo Soft, que sería parte de los requerimientos o estándares solicitados por las normas y acuerdos emitidos por la SBP y herramientas de monitoreo CIEM, la cual sirve para detectar accesos no autorizados, entre otras.

**Interpretación de los resultados:** Es evidente que la SBP, en su función de árbitro entre los bancos y sus clientes, crea normativas y acuerdos que los bancos deben seguir para reducir o mitigar los riesgos en el uso de este tipo de canales o medios digitales. Un conjunto de estándares y herramientas de monitoreo entre otras, son utilizadas por estos, para mitigar los riesgos a los que están expuestos sus clientes al usar la banca por internet, por lo que podemos afirmar que si se ofrecen mecanismos a los clientes para evitar el riesgo. Por otro lado, señala el entrevistado #2, que hay riesgos de parte del cliente que el banco no puede controlar.

Con la pregunta #4, ¿Existe algún mecanismo para ejercer control sobre los delios informáticos ocurridos a la banca por internet?, lo que se busca es saber si existen medidas para ejercer control sobre los delitos informáticos ocurridos a la banca por internet.

**Análisis de los resultados:** En cuanto a esta pregunta el entrevistado #1, señala que existe una batería de acuerdos emitidos por la SBP, entre los que menciono el acuerdo #6-2011que tiene que ver con el uso de la banca electrónica y el 3-2012, que trata sobre los riesgos tecnológicos, en los que se establece que las entidades financieras deben cumplir con protocolos o mecanismos de control para proteger la privacidad y confidencialidad de los datos de sus clientes y su información financiera.

Además, los bancos, usualmente, mantienen unidades de seguridad de la información que buscan establecer mecanismos de control y de monitoreo ante posibles amenazas tecnológicas, así como también incorporan unidades de control de riesgo, las

cuales en conjunto deben establecer un marco de control para reducir o mitigar a niveles tolerables los posibles fraudes informáticos.

Todavía cabe señalar, lo que afirma el entrevistado #2, cada canal tiene sus propias medidas de seguridad, el acuerdo #6-2011, en su artículo #15, indica cuál es la medida mínima de autenticación para poder realizar operaciones en cada medio electrónico. Además, se realizan pruebas de vulnerabilidad para determinar el comportamiento de los delitos informáticos en la infra estructura.

Todos estos elementos forman parte de las actividades que debe realizar la unidad de seguridad de la información, en conjunto con el área de seguridad tecnológica; esta última es la que se encarga de todo lo referente a proporcionar seguridad tecnológica a las entidades bancarias y se conduce de acuerdo a los procedimientos y políticas establecidos por seguridad de la información y a su vez tienen que ver con el planteamiento de todas aquellas herramientas a utilizar para dar seguridad al sistema.

**Interpretación de los resultados:** Se ha comprobado con el desarrollo de esta pregunta que, si existen mecanismos para ejercer control sobre los delitos informáticos ocurridos a la banca por internet, desde la perspectiva de los bancos, pues se mencionan dos acuerdos qué obligan a los bancos a seguir parámetros, procedimientos y políticas que ayuden a dar seguridad a los sistemas de información utilizados para este tipo de operaciones.

Ahora veamos, los resultados de la pregunta #5, ¿Qué tipo de riesgo vulnera más las operaciones de banca por Internet?, en la cual obtendremos datos de las actividades que generan mayor riesgo en las operaciones de este tipo.

**Análisis de los resultados:** Como se mencionó en líneas anteriores, hay riesgos de parte del cliente que los bancos no pueden controlar; la mayoría de los riesgos ocurridos a través de canales o medios electrónicos tienen que ver con el riesgo tecnológico, pero dentro de este tipo de riesgos hay diferentes actividades que son desarrolladas por los bancos las cuales generan un alto apetito de riesgo.

En ese sentido el entrevistado #1, afirmó, que de entre los riesgos tecnológicos, el que mayormente vulnera a los sistemas de información utilizados para las operaciones de banca por internet, son los accesos no autorizados a las credenciales de los usuarios, ya que a través de estas se realizan operaciones no autorizadas o fraudes.

Dicho lo anterior, el entrevistado #2, señala que, de los riesgos tecnológicos, el que más vulnera los sistemas de información utilizados para las operaciones de banca por internet es el e-Commerce, ya que en las páginas electrónicas donde se realiza este tipo de comercio los pagos se realizan a través de banca por internet o por tarjetas de débito o crédito, siendo este el punto en el que se puede dar posibles fraudes por parte de ciberdelincuentes y obtener las credenciales de dichas cuentas o tarjetas para realizar los crímenes.

**Interpretación de los resultados:** El e-Commerce, es una de las nuevas modalidades de realizar compras a nivel mundial, ofrece un gran número de ventajas y la facilidad de comprar en cualquier parte del mundo, sin embargo conlleva un alto grado de riesgos, pues los ciberdelincuentes como se presenta en esta investigación suelen realizar ataques dirigidos o desfiguración de páginas, obteniendo las credenciales de cuentas y tarjetas de créditos de los usuarios, las cuales posteriormente serán utilizadas para efectuar fraudes.

A continuación, se presentan los resultados de la pregunta #6, ¿Bajo qué tipo de riesgos clasifica el banco los delitos informáticos a operaciones de banca por internet?, con la cual se obtuvo el tipo de riesgo bajo el cual se amparan los delitos informáticos.

**Análisis de los resultados:** Señala el entrevistado #1, que todo lo que tenga que ver con las operaciones tecnológicas, está bajo el paraguas de riesgo operacional, ya que dentro de este está el riesgo tecnológico.

En cambio, el entrevistado #2, señaló que el fraude y robo de identidad forman parte de los delitos financieros.

**Interpretación de los resultados:** Del resultado de esta pregunta se desprende que los bancos clasifican los delitos informáticos a operaciones de banca por internet, como riesgo operacional.

Prosigamos nuestro análisis, con los resultados de a pregunta #7, ¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de los delitos informáticos a operaciones a la banca por internet?, con la que se busca obtener el grado de responsabilidad ante estos tipos de delitos.

**Análisis de los resultados:** Ante esta pregunta el entrevistado #1, respondió que, en opinión de muchas personas expertas en temas legales de esta índole, queda muy poco espacio en los contratos entre el cuentahabiente y el banco, para que el usuario pueda ejercer su derecho de protección ante situaciones de delitos informáticos, una vez ocurran las incidencias y estos vuelven a revisarlos; Sin embargo, manifiesta que ha conocido de casos en los que el banco ha aceptado el evento, ha establecido negociaciones y se ha hecho responsable de las incidencias, toda vez no se den demandas, pero en su experiencia son los menos casos.

No obstante, en cuanto a esta pregunta el entrevistado #2, señala que las responsabilidades de los bancos por afectaciones producto de delitos informáticos, están establecidas en los contratos entre los usuarios y los bancos y que en todo caso estos no deben ser abusivos. Además, cuando se dan este tipo de incidencias, las entidades bancarias deben verificar las vulnerabilidades y realizar los ajustes correspondientes.

**Interpretación de los resultados:** No se puede afirmar que el cuentahabiente en caso de sufrir incidencias por delitos informáticos sea el que sufra o asuma las perdidas, tampoco se puede afirmar que las entidades bancarias no asumen sus responsabilidades ante este tipo de incidentes, ni se puede afirmar que el cuentahabiente está en desventaja

ante el prestador del servicio, pues este lee, se le explica y es quien firma el contrato de prestación del servicio, el cual en ningún caso es obligatorio.

Con respecto a, la pregunta #8, ¿De qué manera se indica cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por internet?

**Análisis de los resultados:** Respecto a esta pregunta el entrevistado #1, señaló que, manteniendo una estructura de control interno lo suficientemente fuerte para que se puedan advertir oportunamente y prevenir el tipo de riesgos que conllevan los delitos informáticos. Además, los bancos deben estar dotados de una unidad de sistemas de información, con profesionales y recursos necesarios para lidiar el riesgo tecnológico, y una unidad de gestión de riesgo tecnológico, que es totalmente diferente a la primera, pero que trabajan en conjunto, para saber cuáles son las nuevas amenazas y riesgos que enfrentan los bancos con relación a los delitos informáticos y una tercera unidad, de auditoria interna, dentro de la cual funcione la unidad de auditoría de sistemas, la cual realice auditorías a los sistemas para asegurar el cumplimiento de los controles que el banco ha establecido.

A su vez, el entrevistado #2, señaló en cuanto a esta pregunta, que los bancos para prestar servicios financieros a través de canales o medios electrónicos debe por supuesto, haber seguridad de por medio; en este sentido esa gestión de seguridad inicia con autenticar al cliente. Con estos niveles de autenticación, los cuales están descritos en el acuerdo 6-2011, inicia la gestión de seguridad, pues esto controles indican como va a ser la gestión basada en riesgos. Para que no se cometa un delito financiero a través

de canales electrónicos, todos los sistemas deben seguir una serie de lineamientos, políticas, normas y herramientas para salvaguardar la seguridad de la información y el riesgo por delitos informáticos se mitigue.

**Interpretación de los resultados:** Con este resultado, podemos afirmar que existen lineamientos, normativas, políticas y herramientas que las entidades financieras deben utilizar, señaladas en el acuerdo 6-2011, que indican a estas cómo deben gestionar los riesgos para poder mitigar los delitos informáticos que se deriven de las operaciones realizadas a través de estos canales o medios electrónicos.

En cuanto a la pregunta #9, ¿Con qué frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por internet?

**Análisis de los resultados:** En cuanto a esta pregunta, el entrevistado #1, señaló que, en los acuerdos de SBP, se indica que, estas evaluaciones se deben realizar de forma periódica, ya sea una vez o dos veces al año; se deben realizar pruebas de vulnerabilidad, pues para llevar una adecuada gestión de riesgo tecnológico y de seguridad de la información, hay que estar constantemente evaluando, ya que son actividades o proceso que tienen vida no paran, no tienen inicio ni final, pues la entidad siempre debe estar en constante mejora de los controles para evitar fraudes.

Así mismo, afirma el entrevistado #2, El riesgo tecnológico es evaluado una vez al año, por lo menos. Actualmente, se está tratando de automatizar los procesos para realizar estas en línea. También, se procede a realizar evaluaciones, cuando se reciben reclamos de los usuarios a la SBP, según lo señalado en el acuerdo 1-2008, por lo que se interviene investiga y realiza la evaluación para dar respuesta a estas denuncias. Además, amplía señalando que para evaluar tecnología se debe iniciar con los estándares ISO, que indican que se debe contar con autorización de la alta administración para proceder con estas. Quiere decir que las evaluaciones inician por la parte del gobierno de la tecnología de la información, alineando todas las áreas que tienen participación tecnológica.

Es así como, el gobierno de la tecnología de la información es alineado al negocio, seguido de la estrategia de ciberseguridad y la seguridad de la información alineada a la tecnología y la tecnología al negocio. Por último, señala que existen lineamientos que las entidades financieras deben cumplir, llamadas Normativas técnicas, como también hay normas prudenciales, lo que quiere decir que cada banco puede decidir con qué estándares llevará su gestión de riesgos de acuerdo con los marcos o pautas internacionales.

**Interpretación de los resultados:** Se puede afirmar entonces que las evaluaciones a los riesgos que tienen que ver con los aspectos tecnológicos de las entidades financieras se realizan por lo menos una vez al año, sin embargo, si se dan denuncias o casos de reclamos la SBP interviene y realiza la evaluación al banco de ser necesario.

Ahora veamos, los resultados de la pregunta #10, ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos con relación a los delitos informáticos a operaciones de banca por internet?, con lo que se buscó saber la existencia de alguna clasificación o niveles de control para este tipo de delitos.

**Análisis de los resultados:** En cuanto al entrevistado #1, señala que en teoría se podrían clasificar en preventivos, detectivos y correctivos. Existen otros niveles de clasificación, pero, estos son los más usuales.

Por otra parte, el entrevistado #2, señala la existencia de diversos niveles de control, los cuales aparecen o se pueden encontrar en los diferentes estándares recomendados a los bancos para gestionar el riesgo.

**Interpretación de los resultados:** Es evidente entonces la existencia de clasificaciones para los diferentes niveles de control establecidos para la gestión de riesgos, con relación a los delitos informáticos a operaciones de banca por internet. Dicha clasificación se puede encontrar en los estándares recomendados y esta variará de acuerdo al estándar utilizado por la entidad financiera.

## Contraste de los resultados con la matriz o fichas de investigación

En este apartado, presentaremos los resultados contrastándolos con la información recopilada en la Matriz o fichas de investigación, los cuales están representados por datos estadísticos de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC 2013), Tasas de Victimización de la (UNODC 2013), Informe de Seguridad Ciudadana (CCIAP-PNUD 2017), Informe de Criminalidad año 2016 del Ministerio de Seguridad Pública a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC).

Vamos a dar inicio, contrastando los resultados de las Fichas de investigación con los resultados obtenidos, por lo que procedemos con el análisis de la ficha #1, ver **Anexo 17**. Cifra y tasa de crecimiento de usuarios en Internet de 2000 a 2019, presentado por la Organización de los Estados Americanos (OEA 2019), Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, en la que señala que:

Internet ha revolucionado el mundo que nos rodea y la forma en que interactuamos con los demás. Esto es, particularmente cierto en América Latina y el Caribe, ya que casi 70% de la población está en línea y la tasa de crecimiento de usuarios de Internet es la tercera más alta del mundo – es decir, 2,4% entre 2000-2019. En las Américas y el Caribe, se utiliza Internet para relacionarse con las personas, compartir ideas, gestionar negocios y realizar transacciones. Por todo ello, el sector financiero fue uno de los primeros en adoptar las tecnologías y ofrecerlas a sus clientes. (p.8)

Podemos decir entonces, que para obtener un resultado en cuanto a la tasa de crecimiento en nuestro país, de usuarios de Internet, es necesario se cuenten con cifras confiables y actualizadas, Panamá, no cuenta con estudios cifras o datos estadísticos que cumplan con esta condición, toda vez, se pueda contrastar las cifras obtenidas en esta investigación, o algún estudio en el que se haga referencia a cifras de aumento en nuestro país; lo que podemos mencionar es que de acuerdo al análisis de la pregunta #1, ¿Qué tipo de servicios de banca por electrónica utiliza?, se puede notar que 62,8% menciona que la Banca en línea, o por Internet es la de mayor preferencia en uso, seguido por la Banca móvil, en el que 16,8%, manifestó usarla, lo que representa un alto porcentaje de aceptación entre los cuentahabientes usuarios de este tipo de medios o canales electrónicos, nada más en la ciudad de Panamá.

Este alto porcentaje de uso de medios o canales electrónicos tiene que ver con los porcentajes de ataques exitosos y no exitosos en seguridad digital y motivaciones de estos durante 2017 y 2018, recopilados en la ficha #3, ver **Anexo 19,** presentados por Organización de los Estados Americanos (OEA 2018), en el estudio, El Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, el cual señala que: "el 92% de las entidades bancarias identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital, y el 37% de entidades bancarias manifestaron que sí fueron víctimas de ataques exitosos. La principal motivación de dichos ataques durante el año 2017, fueron motivos económicos (79% de las entidades bancarias víctimas)" (p.8).

En cuanto a, la ficha #4, ver **Anexo 20**, IV Encuesta de victimización y percepción social de la seguridad, denominada, La Victimización y percepción de la seguridad

ciudadana en Panamá, presentado en la VIII Informe de Seguridad Ciudadana (2017), por la Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP), Observatorio de Seguridad Ciudadana, el Programa de las Naciones Unidas para el Desarrollo (PNUD) en el cual en sus gráficos se menciona lo siguiente: “Grafica#8, Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples”; que el 3% de los mismo fueron por Internet” (p.12). […] en la” Gráfica #12, Hurto, Lugar donde ocurrió, el 4% circulando por una ruta/ autopista y por internet” (p.13); Como señalamos en ese apartado, hay que resaltar que en este informe en relación a ciberdelincuencia hay muy poco aporte; podemos apreciar que los delitos ocurridos por internet no se desglosan, por lo que no podemos saber que o a cual tipo de delito se refieren, resaltando así la importancia y contribución al país y a la sociedad, en cuanto a identificar los tipos de delitos más comunes en Panamá, de acuerdo al análisis e interpretación realizado en apartados anteriores y en desarrollo a la pregunta ¿Cuáles son los tipos de delitos que afectan las operaciones de banca por Internet y los Sistemas informáticos en la ciudad de Panamá hasta 2020?, concluimos que son: los Ataques dirigidos, el Malware y el Ransomware respectivamente, según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos.

Además, en cuanto a la gráfica #32, Acciones o medidas para prevenir la delincuencia (p.22), también, mencionada en la ficha #4 del **Anexo 20**, no se observa ninguna que guarde relación a la prevención de los delitos informáticos; Sin embargo, se presentó los diferentes programas de seguridad al servicio de la ciudadanía y podemos apreciar que tampoco existe alguno que asesore, guíe o ayude a prevenir los mismos. Por lo que se reafirma, nuevamente, la interpretación de los resultados presentados en el

apartados anteriores, que tiene que ver con los aspectos de seguridad, tanto del Banco que ofrece el servicio como del usuario o cuentahabiente; en la cual se dijo que estos son muy importantes, y en el que también se afirmó que en muchas ocasiones los usuarios no siguen estas medidas o no implementan medidas de seguridad en los equipos que utilizan para realizar sus operaciones, ya sea por diversos factores como, falta de recursos económicos, negligencia y en muchos casos la inexperiencia de estos, ocasionando que queden en el blanco de cibercriminales que están al asecho de estas fallas de seguridad para realizar su ataques.

En cuanto a, la información recolectada en la ficha #5, ver **Anexo 21,** Cifra de incidencias y denuncias para el año 2016, correspondientes al orden económico, presentada por, Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). Informe de Criminalidad año (2016), se registró que: "El sexto lugar de incidentes y denuncias para el año 2016, corresponden a los Delitos contra el Orden Económico; se presentó 826 casos, entre los que se destacan girar cheques sin fondos, uso indebido de tarjetas de crédito o débito, blanqueo de capitales" (p.18).

Prosiguiendo con el análisis, y para dar continuidad a lo referido en la ficha #5, esta misma encuesta señala que

> Para efectos de análisis y fines consiguientes la ENVI estimó que 11,458 personas de 18 años de edad o más, fueron víctimas del delito de fraude bancario, calculando una prevalencia delictiva de 7 víctimas por cada mil habitantes, con un estimado en pérdidas de USD 9.2 millones, lo que hace obligante analizar y estudiar los actuales procedimientos internos de los cuenta habientes con el objetivo de robustecer aún

> más la tecnología inherente con el objetivo principal de reducir las incidencias en estos delitos. (p.116).

Podemos apreciar que, nuevamente, los datos presentados en este tipo de estudios no son segregados por delitos informáticos, sino de forma global, lo que dificulta hacer comparaciones, e inclusive no menciona cuántos de estos fueron cometidos a la Banca por Internet, lo cual coincide, también, con los datos recolectados en la ficha #6, ver **Anexo 22**, Cifra de incidencia y denuncias para el año 2016, correspondientes a delitos informáticos, por el Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). Informe de Criminalidad año (2016). Este cuadro presentó, datos de incidencias por provincias, pero no segregados, sólo se señala que se cometieron delitos informáticos.

**Interpretación de los resultados:** podemos interpretar de acuerdo con los resultados que, si se hace imperante, la necesidad de realizar análisis a los procedimientos que realizan los cuentahabientes, toda vez se puedan tomar medidas que refuercen la seguridad a estos; por parte de las entidades bancarias, reforzar más las medidas de seguridad y aumentar a través de estos medios la promoción al buen uso de los medios o canales digitales.

También, los Estados juegan un papel fundamental, ya que estos deben reorganizar a través de las instituciones correspondientes, leyes acordes, que beneficien y protejan a la sociedad de este tipo de actos delictivos, iniciando por la segregación de

estos ya que nuestro país no cuenta con cifras ni dados segregados que vallan en concordancia con las pocas y desajustadas Leyes con que contamos en la actualidad.

## Contraste de resultados con los de otros autores presentados en esta investigación

En este apartado presentamos los resultados de esta investigación contrastados con lo que señalan otros autores. En este sentido iniciamos con los resultados de la investigación de Shick (2017), en el que señala que: “Un hallazgo notable en esta investigación encontró que la mayoría de los participantes desconocía o ignoraba las leyes específicas sobre delincuencia informática aplicables a su estado o país de residencia” […] Amplia el investigador, señalando que, “esto se debe en parte la escasa atención dada a la delincuencia informática en el sistema de justicia penal y también, a la falta para educar a los ciudadanos sobre las consecuencias y las leyes en materia de delitos informáticos, aspecto que ha sido evaluado en apartados anteriores de esta investigación”. (p.101)

En cuanto a, resultados presentados en esta investigación en contraste con los de Shick (2017), podemos afirmar, que en efecto la mayoría de los encuestados desconocía o ignoraba las leyes específicas sobre delincuencia informática aplicables a nuestro país y reafirmamos que esto se debe a la escasa atención dada a la delincuencia informática en el sistema de justicia penal y también, a la falta de educación a los ciudadanos sobre las consecuencias y las leyes en materia de delitos informáticos, por parte del Gobierno

e instituciones bancarias, aspecto que ha sido evaluado en apartados anteriores de esta investigación.

En este sentido, amplía Marangunich (2019), señalando que

> lo que representa una gran amenaza, ya que nuestras autoridades no se ponen ni de acuerdo ni al día en la creación de leyes que trabajen en conjunto a los acuerdos adquiridos con anterioridades, ni en la creación de estrategias o planes de contingencia ante incidencias digitales y segundo, estamos situados en una región considerada en vías de desarrollo, y con un alto potencial de nuevos negocios en el ámbito digital, por nuestro sector bancario, como bien habíamos señalado en líneas anteriores de esta investigación, lo que nos ubica en una coyuntura de alto riesgo. (p.64)

Por otra parte, la Organización de los Estados Americanos y La Comisión Nacional Bancaria y de Valores de México, en el libro Estado de la ciberseguridad en el sistema financiero mexicano (2019), señala que

> Según las entidades e instituciones financieras en México, el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes con más frecuencia contra los clientes (socios, asociados o usuarios) de servicios financieros son: i) Phishing, ii) Software espía (Malware o troyanos), y iii) Ingeniería social. También, resulta importante anotar que dentro de las principales motivaciones para la realización de estos ataques se encuentran las

> económicas (74%), y en una menor medida las políticas, el hacktivismo, la reputación personal como hackers y el robo de información personal. (p.9)

En canto a, este señalamiento, de La Comisión Nacional Bancaria y de Valores de México, podemos afirmar que, en nuestro país existe una gran similitud en cuanto a los tipos de actividades que son más frecuentes a las instituciones financieras, en este sentido a la Banca por Internet, en Panamá, los delitos más frecuentes son: los Ataques dirigidos, el Malware y el Ransomware respectivamente, según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos.

Por su parte, en contraste con Moreno (2016), Presidente Banco Interamericano de Desarrollo, afirmó en el documento Observatorio de la ciberseguridad en américa latina y el caribe, Informe Ciberseguridad (2016) que está incluido en el libro: Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, el cual señala lo siguiente:

> Si los lectores han llevado un mensaje de este Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen. Su análisis es un llamado a la acción para empezar a hacer todo lo necesario por proteger esta infraestructura clave para el siglo XXI. (p.9)

Podemos afirmar que, nuevamente, coincidimos que, en Panamá, no estamos preparados para contrarrestar la amenaza del cibercrimen, ya que no contamos con leyes

acordes a los convenios internacionales que se emiten a nivel mundial para tomar acción ante estos, las leyes para delitos informáticos en nuestro país, fueron incluidas como delitos comunes, lo que dificulta el procesamiento de los delincuentes.

Además, podemos mencionar otro factor de gran importancia, la inexistencia de divulgación por parte del Estado y de los bancos en cuanto aspectos como: ¿a dónde se deben dirigir y que deben hacer los usuarios si son víctimas de delitos informáticos?, pues los resultados de esta investigación indican que los usuarios desconocen que hacer en estos casos, por lo que este, tiene la percepción que a estos delitos no se les da seguimiento.

Como resultado, y en concordancia a los factores antes planteados, se hace evidente la gran importancia que tiene la ciberseguridad para el sector financiero, en cuanto a la confiabilidad que estos deben proyectar y garantizar hacia sus clientes en el entorno digital como un espacio confiable para la realización de sus operaciones, toda vez, las inversiones realizadas en procesos de digitalización de servicios al cliente, no generarían el impacto positivo esperado, debido a la desconfianza en el uso de canales digitales, (Contreras et al, 2019, p.18).

De esta manera, concluimos la presentación de los resultados obtenidos en esta investigación y procederemos en el siguiente capítulo a presentar las conclusiones y recomendaciones de acuerdo con estos resultados.

# CAPÍTULO V

# CONCLUSIONES Y RECOMENDACIONES

Como se ha mencionado anteriormente, los grandes avances tecnológicos han modificado la economía mundial y direccionado esta hacia la globalización, la cual guía las relaciones comerciales a través de una vasta trama de dependencias y oportunidades. Mismas que, el sector financiero panameño ha sabido aprovechar, ya que la evolución tecnológica pone elementos y medios a disposición de las organizaciones, para identificar y desarrollar las mejores estrategias que aseguren su permanencia en el mercado frente a sus competidores.

Oportunidades como, la entrada de los negocios en ambientes computacionales o mejor conocidos como “e-comerce” a nuestra llamada sociedad de consumo y la proliferación de opciones de compra para los clientes, se han convertido en ventajas competitivas sustentables, creando vínculos de dependencia entre los usuarios, que permiten mejorar su posición en el contexto en el que actúan, impulsando a estos y organizaciones cada vez más, al uso de nuevos mecanismos ofrecidos.

En Panamá, el sector financiero no se queda atrás, la necesidad de internacionalizar sus operaciones con el fin de competir con empresas de clase mundial hace indispensable la búsqueda de altos niveles de desempeño en sus operaciones, así como la entrega de productos y servicios de gran calidad.

Es por ello que desde hace tiempo atrás, el sector financiero viene trabajando en una serie de productos, conocidos como sistemas de información o softwares, los cuales trabajan a través del internet, y crean una serie de ventajas competitivas; productos como la banca electrónica o mejor conocida como banca en línea, operan de forma electrónica o digital en este entorno para realizar pagos, trasferencias de dinero, entre otros, llevando así sus servicios a nivel mundial, pero al mismo tiempo, se da el inconveniente que, este es el campo de acción de personas inescrupulosas que buscan las oportunidades o vulnerabilidades de los usuarios (en muchas ocasiones inexpertos) para efectuar sus actos ilícitos.

En este apartado se presentan las conclusiones y luego algunas recomendaciones, después de un largo recorrido investigativo, a través de la consulta, a diferentes fuentes secundarias que evidencian la existencia de una situación problemática, en cuanto al avance y desarrollo de los delitos informáticos en todas partes del mundo y del cual Panamá, un país en vías de desarrollo, no escapa; Por lo cual, y como mencionaos en apartados anteriores, se da la necesidad de implementar nuevas y modernas técnicas encaminadas a la correcta visualización y tratamiento de los delitos económicos, financieros y contables, cometidos a través del internet, así como lograr una adecuada investigación de estos.

En el desarrollo de esta investigación se plantea como objetivo, evaluar el impacto de los delitos informáticos a las operaciones de banca por internet en la ciudad de Panamá hasta 2020; para lograrlo, se estableció una serie de objetivos específicos que nos ayudaron en el avance de esta, y que a continuación presentamos.

Para evaluar el impacto que estos ejercen sobre las operaciones de banca por internet, y los sistemas de información que estos utilizan, el primer objetivo a seguir fue identificarlos.

**Objetivo #1:** Identificar cuáles son los tipos de delitos informáticos que afectan los sistemas de información a través de las operaciones de banca por Internet en la ciudad de Panamá hasta 2020.

**Proposición #1:** Es así como, según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos, se pudo identificar que de entre los delitos informáticos que afectan a los sistemas de información a través de las operaciones de banca por internet en la ciudad de Panamá hasta 2020, están los Ataques dirigidos, el Malware y el Ransomware respectivamente.

Sin lugar a dudas, cuando se habla de la palabra impacto, según la definición de la Real Academia de la Lengua, significa: efecto producido en la opinión pública por un acontecimiento, una disposición de la autoridad, una noticia, una catástrofe, etc.; este puede ser positivo o negativo, en el caso de los delitos informáticos, la palabra misma indica que el impacto que estos tengan será negativo en cualquiera de los casos.

**Proposición #2:** Será negativo para las entidades financieras, puesto que las inversiones en infraestructura para el desarrollo y uso de estos sistemas es muy costosa.

Si los usuarios que utilizan este tipo de medios o canales digitales se llegarán a enterar por algún medio, canal, red o noticiero, sobre incidencias en el uso de estos o que estos sistemas sufran frecuente el ataque por parte de cibercriminales, puede causar grandes pérdidas, ya que los usuarios dejarían de usar este y los altos costes de inversión se perderían.

**Proposición #3:** Perjudicial también, para todos aquellos usuarios que confían en este tipo de medios, pues de darse alguna incidencia, su bien jurídico podría verse afectado. Además, de los daños o vulnerabilidad ocurrida a los sistemas de información utilizados para la realización de las operaciones bancarias, y a la vez su contabilidad, la sociedad y la economía del país.

Por otro lado, investigaciones como la de, Blossiers (2018), en su tesis presentada a la Universidad Nacional Federico Villarreal, afirma con cifras estadísticas, que en cuanto a los impactos que puede sufrir la empresa bancaria esta

> Del total de encuestados, 35 (88%) creen que existen serios impactos a la empresa bancaria, la comisión de delitos informáticos, mientras que 5 (12%) considera que no es así (p.47). […] Del total de encuestados, 27 (68%) creen que las comisiones de delitos informáticos generan serios impactos económicos a la empresa bancaria, mientras que 13 (32%) considera que no es así (p.48). […] Del total de encuestados, 38 (95%) creen que la comisión de delitos informáticos genera serios impactos sociales a la empresa bancaria, mientras que 2 (5%) considera que no es así (p.49). […] Del total de encuestados, 38 (95%) creen que la comisión de delitos informáticos

> genera serios impactos sociales a la empresa bancaria, mientras que 2 (5%) considera que no es así (p.50).

En cuanto a, Leyes y regulaciones, señala Blossier (2018), que: “Del total de encuestados, 23 (57%) creen que la tipificación de los delitos informáticos coadyuva a una defensa efectiva de los bienes jurídicos protegidos, mientras que 17 (43%) considera que no es así (p.52).

**Proposición #4:** Consideramos importante la adecuada tipificación de estos delitos, en el Código Penal y Procesal Penal, de acuerdo con su evolución, avance y segregados por delitos, no como son tipificados en la actualidad, como delitos comunes.

En cuanto a la clasificación, señala Blossier (2018), en sus conclusiones que

> es la clasificación inadecuada que se tiene de los delitos informáticos, que afecten a las empresas bancarias, debemos entender que las empresas bancarias son entidades que resguardan el dinero, capital y ahorros de muchas personas; y lo delitos que se cometen contra estas son en suma muy específicos, y denotarlo solo como hurto, o como robo, no identificaría en específico la comisión del delito; por ello es necesario una identificación adecuada en el Código Penal. (p.62)

**Proposición #5:** Como mencionamos en apartados anteriores, nuestro país no cuenta con cifras actualizadas y las existentes no son reflejadas de forma correcta, ya

que no hay una adecuada clasificación por delito. Se hace imperativo, sugerir a las autoridades locales, la adecuación de las leyes al compromiso adquirido como país, con el convenio de Budapest, al cual estamos adheridos desde 2011, toda vez que se puedan unificar estas a la normativa estándar mundialmente utilizada, toda vez las cifras manejadas en datos estadísticos e informes presentados por las diferentes entidades o estudios, sean acordes a las realidades mundiales.

A través de esta recomendación, también, damos respuesta al objetivo específico #3, pues podemos decir que esta es una manera efectiva de mitigar los riesgos producto de los delitos informáticos a las operaciones de banca por internet y por ende a los sistemas de información contables que estos utilizan ya que son los que mayormente se vulneran debido a estos delitos.

**Objetivo #2:** Analizar, cuál de los tipos de delitos informáticos identificados, causa mayores afectaciones a las operaciones de Banca por Internet hasta 2020.

Para el desarrollo del segundo objetivo específico, el cual busca, de los tipos de delitos identificados, ¿Cuál afecta mayormente las operaciones de banca por Internet en la ciudad de Panamá hasta 2020?, y por ende a los sistemas de información contables que estos utilizan.

**Proposición #6:** Podemos afirmar que según la percepción y conocimiento de los encuestados en el uso de medios o canales electrónicos son mayormente el Malware seguido muy de cerca por los Ataques dirigidos.

**Proposición #7:** Es importante la adecuada identificación y clasificación de los delitos informáticos, ya que la Autoridad (Autoridad de Innovación Gubernamental, por sus siglas AIG) que rige la tecnología en nuestro país, aún no cuenta con este tipo de dato, el cual es importantísimo para la creación de herramientas y modelos actualizados para combatir este flagelo tan cambiante.

**Proposición #8:** Si bien es cierto, los avances tecnológicos van a pasos agigantados y los ciberdelincuentes no se quedan atrás, las autoridades de nuestro país no deben perder la pista en cuanto a este tipo de desarrollo por lo que se hace imprescindible estar en constante actualización de los nuevos delitos ocurridos y la creación de una policía especializada para que los riesgos producto de estos, sean mitigados al mínimo y con ello las afectaciones a los usuarios, economía y a la sociedad.

**Objetivo #3:** Determinar la forma de mitigar los riesgos producto de los delitos informáticos.

**Proposición #9:** Otra forma de determinar la manera de mitigar los delitos informáticos que afectan a las operaciones de banca por internet y por ende a los sistemas de información contables que estos utilizan, a parte de los ya mencionados en

apartados anteriores, es crear una fuerte cultura sobre el uso del internet, por parte de las autoridades gubernamentales en conjunto con las instituciones financieras.

Podemos afirmar que en nuestro país no existe una adecuada cultura del uso de internet, así como tampoco una adecuada divulgación del impacto que pueden causar estos tipos de delitos a la sociedad y a la economía, ni por el gobierno y muy escasamente, por las entidades financieras, que son las que, debido al aumento de las operaciones bancarias, a través de la banca por internet, por efectos de la pandemia Covid-19, en el año 2020, envían a través de correo electrónico, sugerencias sobre el uso correcto de estos sistemas.

**Proposición #10:** En cuanto a las denuncias por delitos comunes, los usuarios se aproximan a las instituciones policiales que captan estas para iniciar la investigación; en el caso de delitos informáticos funciona igual, ya que estos, son tipificados en las leyes de nuestro país como delitos comunes;

Por lo tanto, se sugiere, la creación de un sitio especializado en el manejo y recepción de estos, donde las personas puedan acudir a poner sus denuncias, pues en este estudio se determinó, que los usuarios encuestados manifestaron no tienen conocimiento a dónde se deben dirigir, en caso de ser víctimas de este tipo de delitos.

**Proposición #11:** La creación de unidades de policía especializada, para en el futuro con los datos estadísticos suministrados por estos, poder hacer comparaciones

con los países de la región y el mundo. Este es uno de los factores que se plantean en la situación problemática de esta investigación ya que los cibercriminales si son expertos y se preparan para hacer frente a todas aquellas medidas de seguridad implantadas a los sistemas informáticos con el objetivo de vulnerar estos.

Es así como damos por finalizada esta investigación, con la esperanza que las sugerencias y recomendaciones realizadas sean tomadas en consideración por las autoridades gubernamentales y para futuras investigaciones en cuanto a los delitos informáticos y sus repercusiones ya que estos son tan cambiantes que pronto se dará la necesidad de nuevos estudios, además con los datos suministrados se puede en futuras investigaciones proponer a creación de un modelo de sistema de información que coadyuve a mitigar la incidencia de estos delitos.

# REFERENCIAS

Abrego, D. (2017). Influencia de los sistemas de información en los resultados organizacionales. Revista Contaduría y Administración, Vol. 62, (2), 303-320. https://reader.elsevier.com/reader/sd/pii/S0186104216300432?token=7E1153286E9D0DB44CA5F08FBCA4FF73C6D5D4D3D234B23CD09AA1B6EFDE60B55E1A5978AD9198B3129B429506412466

Alkorta, X. (2017). Crisis y nueva dirección bancaria. Universidad de Deusto. Bilbao. http://www.deusto-publicaciones.es/index.php/main/libro/1134/es

Almagro, L. (2019). Prólogo OEA. En Organización de los Estados Americanos & Asociación Bancaria y de Entidades Financieras de Colombia. (Eds.)*, Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.* (pp. 7-9). OEA/Asobancaria. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Arens, A., Elder, R., & Beasley, M. (2007). Auditoria. Un enfoque integral. PEARSON Educación.

Astudillo, M. (2008). Consideraciones para la selección de sistemas de información contables y administrativos en la Pyme colombiana Entramado, Vol. 4, (2), 52-69. https://www.redalyc.org/pdf/2654/265420459005.pdf

Bernal, C. (2010). Metodología de la Investigación. Pearson Editorial.

Bula, J. (1994). John Rawls y la teoría de la modernización. Una retrospectiva analítica. Revista Unual.edu.co. Vol. 14, (21), 67-83. https://www.researchgate.net/profile/Jorge_Bula/publication/227385693_John_Rawls_y_la_teoria_de_la_modernizacion/links/55228dd10cf29dcabb0d7840/John-Rawls-y-la-teoria-de-la-modernizacion.pdf

Blossiers, J., (2018). *El Delito informático y su incidencia en la empresa bancaria.* [Trabajo de grado, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV. http://repositorio.unfv.edu.pe/handle/UNFV/2608

Cámara de Comercio Industrias y Agricultura de Panamá (CCIAP) y Programa de las Naciones Unidas para el Desarrollo (PNUD). (2017). VIII Informe de Seguridad Ciudadana. (Informe, CCIAP, PNUD). http://www.pa.undp.org/content/panama/es/home/library/democratic_governance/viii_informe_seguidad_ciudadana_2017.html

Candanedo, J. (2016). Capítulo III, Delitos Financieros. En Procuraduría General de la Administración. (Ed.), *Texto Único del Código Penal de la República de Panamá (Comentado)*. *Título VII, Delitos contra el orden económico.* (pp. 193-195). Fiscalía Superior de Litigación y la Oficina de Implementación del Sistema Penal Acusatorio de la Procuraduría General de la Nación. https://ministeriopublico.gob.pa/wp-content/uploads/2017/01/Texto-%C3%9Anico-del-C%C3%B3digo-Penal-comentado.pdf

Castro, S. (2019). Prólogo Asobancaria. En Organización de los Estados Americanos & Asociación Bancaria y de Entidades Financieras de Colombia (Eds.), *Desafíos del*

*riesgo cibernético en el sector financiero para Colombia y América* (pp. 11-14). https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Carreño, A. (2015). Los postulados fundamentales de la teoría de la modernidad reflexiva de Anthony Giddens. Acta sociológica. Revista Unam (67), 87-110. http://www.revistas.unam.mx/index.php/ras/article/view/50021

Carrillo, M. (2013). Los Desafíos del Derecho penal frente a los Delitos Informáticos y otras conductas fraudulentas en los medios de pagos electrónicos. Revista IOS, Vol.7, (31). http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100011

Catacora, F. (1997). Sistemas y procedimientos contables. Mc Graw-Hill.

Cerda, H. (1998) Los Elementos de la investigación, Como reconocerlos, diseñarlos y construirlos. Editorial El Búho LTDA.

Cohen, D., & Asín, E. (2009). Tecnologías de información en los negocios. McGraw-Hill/Interamericana Editores.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Serie de tratados europeos-n°185. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Concepción, M., & Gómez, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, Vol. XLVII, 209-234.

España. file:///C:/Users/Prof.%20Jos%C3%A9%20R.%20Godoy/Downloads/Dialnet-Cibercrimen-4639646.pdf

Contreras, B., Bejarano, J., & Garcés, O. (2019). El Estado de la Ciberseguridad en el Sector Financiero en Latinoamérica y el Caribe. En Organización de los Estados Americanos (OEA) & Asociación Bancaria y de Entidades Financieras de Colombia (Eds.), *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*. (pp. 16-25). https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Corral, Y. (2009). Validez y confiabilidad de los instrumentos de investigación para la recolección de datos. Revista Ciencias de la Educación. Vol. 19 (33), 229-247. http://servicio.bc.uc.edu.ve/educacion/revista/n33/art12.pdf

De Latouche, M. & Maldonado, R. (2013). Estudio de la Contabilidad General. Ediciones UC.

Díaz, A. (2010). El delito informático su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR). Vol. 8, 169-203. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

Donadío, A. Dieck, Ma., García de la P. B., Lankenau, D., & Valdés, I. (2004). Negocios en ambientes computacionales. McGraw-Hill Interamericana, S. A. DE C. V.

Echenique, J. (2008). Auditoría en Informática. Segunda edición. McGraw-Hill/Interamericana, S. A. de C. V.

Elhag, H. (2015). Enhancing Online Banking Transaction Authentication by Using Tamper Proof & Cloud Computing. [Tesis doctoral, Universidad de Surrey]. Repositorio Semantic Scholar. https://www.semanticscholar.org/paper/Enhancing-online-banking-transaction-authentication-Elhag/f70444be4b4a9dfb149bcd72e77f6dd5c0217ed4

Espinosa, Y., & Llorénz, L. (2015). Exploración de la capacidad de liderazgo para la incorporación de TICC en educación; Validación de un instrumento. Revista Relatec, Vol. 14, (13), 35-47. https://relatec.unex.es/article/view/2068/1392

Estrada, M. (2008). Delitos Informáticos. Universidad abierta. México. http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Finel-Honigman, I. & Sotelino, F. (2015). International Banking for New Century. Editorial Routledge. London/New York.

Forouzan, B. (2007). Transmisión de datos y redes de comunicaciones. Cuarta edición, España. McGraw-Hill/Interamericana de España, S. A. U.

Fratti, S. (2018). Un país con la necesidad de una legislación sobre cibercrimen. Instituto Panameño de derecho y Nuevas Tecnologías (IPANDETEC). https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

Gobierno de la República de Panamá. (2014). Plan Estratégico de Gobierno 2015-2019. Un solo país. https://observatorioplanificacion.cepal.org/es/planes/plan-estrategico-de-gobierno-2015-2019-un-solo-pais-de-panama

González, J. (2013). Delincuencia Informática: Daños informáticos del artículo 264 del Código penal y propuesta de reforma. [Tesis doctoral, Universidad Complutense de Madrid]. Repositorio de la Universidad Complutense de Madrid. https://eprints.ucm.es/23826/1/T34976.pdf

Gonzalez, M., Lankenau, D., Lankenau, M., Valdez, M., Almaguer, A., Dieck, M., García, B., Garza, M. (2010). Tecnologías de la información. Mc Graw-Hill. Segunda Edición.

Giddens, A., Bauman, Z., Luhmann N., & Beck, U. (1996). Las Consecuencias Perversas de la modernidad: Modernidad, Contingencia y Riesgo. Editorial Cultura Libre.

Gutiérrez, H. (2014). Calidad Total y Productividad. Cuarta Edición. McGraw Hill/Interamericana Editores, S. A. DE C. V.

Hernández, R., Fernández, C., & Baptista, M. (2014). Metodología de la investigación. México. McGraw-Hill Interamericana, S. A. DE C. V

Juárez, F., Villa Toro, J., & López, E. (2002). Apuntes de estadística inferencial. Instituto Nacional de Psiquiatría Ramón de la Fuente, Dirección de Investigación Epidemiológicas y Psicosociales. Primera Edición.

Landino, M., Villas, P., & López, A. (2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. Scientia Et Technica, Vol. 17, (47), 334-339. https://www.redalyc.org/pdf/849/84921327061.pdf

Laudon, K. & Laudon J. (2008). Sistemas de Informacion Gerencial, Administración de la empresa Digital. México. Pearson Educación de México; S. A. DE C.V.

Maldonado, R. (2006). Estudio de la contabilidad General. Editorial Félix Varela, Habana.

Marangunich, J. (2019). Riesgo cibernético y su relación con el sistema financiero en América Latina. En Organización de los Estados Americanos (OEA) & Asociación Bancaria y de Entidades Financieras de Colombia (Eds.), *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.* (pp. 58-86). https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Mardonez, J. & Ursúa, N. (1991). Filosofía de las Ciencias Humanas y Sociales. Editorial Fontamara. España.

Mercado, J. (2014). Banca Múltiple y Reforma Financiera en México. MA Porrua Libero-editor. México.

Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). (2016). Informe de Criminalidad 2016. (Informe, SIEC). http://www.siec.gob.pa/index.php?option=com_phocadownload&view=category&download=231:informe-de-criminalidad-2016&id=9:informes

Montaño-Ardilla, V., Combita-Niño, H., & De la Hoz, E. (2017). Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Prácticas TI en cumplimiento de la Ley Sarbanes–Oxley. Revista Espacios. Vol. 38 (23), 3. https://www.revistaespacios.com/a17v38n23/a17v38n23p03.pdf

Morales, C., Memije, M., Mendoza, H. & Ventura, P. (2017). Delitos informáticos en el Estado de Guerrero. Primera Edición. Universidad Autónoma de Guerrero. México.

Morales, R. (2019). Cooperación internacional y su papel en la gestión del riesgo cibernético. En Organización de los Estados Americanos & Asociación Bancaria y de Entidades Financieras de Colombia (OEA) (Eds.), *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina* (pp. 26-42). https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Moreno, L. (2016). Mensaje del Presidente del Banco Interamericano de Desarrollo. En Organización de los Estados Americanos (OEA) & Banco Interamericano de Desarrollo (Eds.), *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016* (p. IX). https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Norton, P. (2006). Introducción a la computación. México. McGraw-Hill/Interamericana Editores; S. A. DE C.V.

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2013). Metodología de la investigación cuantitativa-cualitativa y Redacción de Tesis. Colombia. Ediciones de la U.

Ocaña, C., & Uría, F. (2017). KPMG & FUNCAS. El Nivel de Madurez Digital, Sector financiero en España. https://www.funcas.es/publicaciones/docs/informe01.pdf

Organización de los Estados Americanos & Comisión Nacional Bancaria y de Valores. (2019). Ciberseguridad en las entidades e instituciones del Sistema Financiero Mexicano. En Organización de Estados Americanos (OEA) (Eds.), *Estado de la Ciberseguridad en el Sistema Financiero Mexicano* (p. 16). http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno. (Informe, UNODC). https://www.unodc.org/documents/organizedcrime/cybercrime/Cybercrime_Study_Spanish.pdf

Paz, N. (2015). Contabilidad general. Quinta edición. McGraw-Hill/Interamericana Editores S. A. de C.V.

Parodi, W. (2014). Breve análisis de los principales delitos financieros en Panamá. Revista del Ministerio Público. Vol. 1. (1), 90-103. https://ministeriopublico.gob.pa/publicacion-libros/revista-ano-1-volumen-1-2014/

Pinilla, J. (1994). Auditoría Informática, un enfoque operacional. Ecoe Ediciones.

Puig, S. (2014). La Prueba electrónica: sus implicaciones en la seguridad de la empresa. [Tesis doctoral, Universitat Ramón Llull]. Repositorio Tesis Doctorals en Xarxa. https://www.tdx.cat/bitstream/handle/10803/285237/TESI%20DOCTORAL%20S%C3%92NIA%20PUIG%20FAURA.pdf?sequence=1&isAllowed=y

Price Waterhouse & Cooper. (2016). Encuesta Global sobre Delitos Económicos 2016. Capítulo Argentina. Hacia una nueva ética en los negocios. Delitos económicos e informáticos. https://www.pwc.com.ar/es/publicaciones/assets/encuesta-delitos-economicos-2016.pdf

Rayport, J. & Bernard, J. (2007). e-Commerce. México. McGraw-Hill Interamericana Editores, S. A. DE C. V.

Reyna, L. (2002). Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal, JURISTA Editores E.I.R.L., 125.

Rincón, J. (2015). El delito en la cibersociedad y la justicia penal internacional. [Tesis doctoral, Universidad Complutense de Madrid]. E-Prints Complutense, Repositorio institucional de la Universidad Complutense de Madrid. https://eprints.ucm.es/33360/1/T36457.pdf

Rojas-Parra, J (2016). Análisis de la penalización del cibercrimen en países de habla hispana. Revista LOGOS CIENCIA & TECNOLOGÍA. Vol. 8. (1), 221-222. https://doi.org/10.22335/rlct.v8i1.339

Shick, K. & Toro-Álvarez., M. (2017). Cibercriminología, Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital. Fondo editorial Universidad Antonio Nariño.

Superintendencia de Bancos de Panamá. (2014). Tabla Ban08 de Banca Electrónica, Glosario de Términos. https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/circulares/2014/Anexo_117.pdf

Superintendencia de Bancos de Panamá. (2015). Informe Plan estratégico 2015-2019. https://www.superbancos.gob.pa/superbancos/documentos/noticias/2015/09_sep/Plan_Estr_15-19.pdf

Superintendencia de Bancos de Panamá. (2015). Dirección de estudios financieros. Informe de bancarización 2015. https://www.superbancos.gob.pa/superbancos/documentos/financiera_y_estadistica/estudios/Inf_Bancarizacion15.pdf

Stracuzzi, S., & Pestana, F. (2012). Metodología de la investigación cuantitativa. Fondo Editorial de la Universidad Pedagógica Experimental Libertador. (FEDUPEL). La editorial pedagógica de Venezuela. 1° reimpresión.

Téllez, J. (2008). Derecho Informático. Mc Graw Hill Educación. Cuarta edición.

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances conceptos y características. En Parada, R., & Errecaborde, J. (Eds). *CIBERCRIMEN Y DELITOS INFORMÁTICOS, Los nuevos tipos penales en la era de internet* (pp. 59-68).

https://erreius.com/actualidad/12/penal-y-procesal-penal/Nota/244/suplemento-especial-cibercrimen-y-delitos-informaticos

Temperini, M. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf

Valverde, F. (2015). Análisis de la banca por Internet entre los usuarios particulares. Un modelo en Dinámica de Sistemas. [Tesis doctoral, Universidad de Valladolid]. Repositorio Documental de la Universidad de Valladolid. https://uvadoc.uva.es/bitstream/10324/14079/1/Tesis707-151005.pdf

# ANEXOS

**Anexo 1** *Matriz de consistencia.*

| **JOSÉ R. GODOY T. 8-442-236** | | | | | **ITEMS** | | |
|---|---|---|---|---|---|---|---|
| **PROBLEMA** | **VRIABLES** | **DIMENSIONES** | **INDICADORES** | **OBJETIVOS ESPECÍFICOS** | **CUESTIONARIO #16** | **MATRIZ#9** | **ENTREVISTA#7** |
| ¿Cómo influyen los delitos informáticos a las operaciones de banca por Internet en la ciudad de Panamá hasta el 2019?<br>¿Cuál es su recurrencia, su porcentaje, afectaciones contables y las posibles soluciones que coadyuven a controlar o mitigar estos hechos? | **INDEPENDIENTE:** Delitos informáticos. | 1.Fraude Informático.<br>1.Falsificación Informática. | 1. Cifra de los tipos de delitos que afectan las operaciones de banca por Internet y los sistemas infromáticos. | 1.Identificar cuáles son los tipos de delitos informáticos que afectan las operaciones de banca por Internet en la ciudad de Panamá y sus repercusiones. | 1.De los delitos enunciados señale cúal considera el tipo más común que afecta a los servicios de banca por Internet.<br>1.De los delitos enunciados señale cúal considera el tipo más común que afecta a los sistemas informáticos. | | 1. ¿Mencione de qué forma influyen a la entidad los delitos informáticos a operaciones de banca por Internet? |
| | | 2.Magnitud de daños al bien privado. | 2.Cifras de las conductas ilicitas más comunes a la banca por Internet<br>2.Cifras de Agresiones a los sistemas de banca por Internet.<br>2.Cifras de daños por recurrencia de robos, fraudes, intrusiones, a cuentahabientes que manejan banca por Internet. | 2.Analizar cuáles son los delitos informáticos más recurrentes a este tipo de operaciones. | 2. ¿Sabes cuáles son lo pasos a seguir para denunciar los delitos informáticos en Panamá?<br>2.¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas por delitos informáticos a usuarios de banca por Internet?<br>2. Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá?<br>2. ¿Consideras la solución a las denuncias por | 2.Cifra de los delitos más recurrentes a los servicios de banca por Internet.<br>2.Cifra de los delitos más recurrentes a los sistemas informáticos. | |
| | | 3.Tecnológicas. | 3.Cantidad de personas que estan enteradas o poseen conociminetos sobre la problemática social que representan estas malas prácticas.<br>3.Cifra de personas que están informadas sobre los riesgos producto del mal uso de la banca por Internet.<br>3. Cifra de personas que tienen conocimiento de regulaciones o leyes que le protejan de los delitos informáticos<br>3.Cifra de personas que poseen conocimiento en el uso de la tecnología (hardware/software).<br>3.Cifra de personas que poseen mecanismos de protección en sus computadores o medios electrónicos. | 3.Determinar la forma de mitigar los riesgos producto de los delitos informáticos que se deriben de estas operaciones. | 3.¿Consideras las compras por Internet seguras?<br>3.¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes y a la sociedad?<br>3.¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet?<br>3.¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos?<br>3.¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier mecanismo electrónico?<br>3.¿Posee algún mecanismo de protección en su computador o medio electrónico para evitar delitos | | |
| | | | | | | | |
| | **DEPENDIENTE**: Operaciones de banca electrónica. | 1.Servicios financieros. | 1.Cifra de servicios financieros utilizados a través de algún medio o canal electrónico.<br>1.Cifra de servicios financieros más utilizados por cuentahabientes de banca por Internet. | 1.Identificar cuáles son los tipos de delitos informáticos que afectan las operaciones de banca por Internet en la ciudad de Panamá y sus repercusiones. | 1.¿Qué tipo de servicios de banca electrónica utiliza con?<br>1.¿Qué tipo de servicios de banca por Internet utiliza? | | |
| | | 2. Operacional | 2.Frecuencia de operaciones de banca por Internet.<br>2.Niveles de afectaciones a operaciones banca por Internet producto de delitos informáticos | 2.Analizar cuáles son los delitos informáticos más recurrentes a este tipo de operaciones. | 2.¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos?<br>2.¿De los delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Internet? | 2. Cifras estadísticas de afectaciones a la entidad bancaria por los delitos informáticos a operaciones de banca por Internet.<br>2.Cifras estadísticas de delitos más recurrentes a operaciones de banca por Internet? | 2.¿Mantiene la entidad datos estadísticos de delitos más recurrentes a operaciones de banca por Internet? |
| | | 3.Controles | 3.Niveles de control ejercidos por las entidades bancarias. | 3.Determinar la forma de mitigar los riesgos producto de los delitos informáticos que se deriben de estas operaciones. | 3.¿Considera Ud. que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | 3.Niveles de control ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet.<br>3.Mecanismo de control a los delitos informáticos ocurridos a la banca por Internet. | 3.¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet?<br>3.¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet? |
| | | 4.Riesgos | 4.Evaluar los riesgos que afectan las operaciones de banca por Internet. | 3.Determinar la forma de mitigar los riesgos producto de los delitos informáticos que se deriben de estas operaciones. | | 4.Tipos de riesgo que vulneran más las operaciones de banca por Internet.<br>4.Nivel de riesgo en el que se clasifican los delitos informáticos a operaciones de banca por Internet.<br>4.Nivel de responsabilidad por afectaciones producto de delitos informáticos a operaciones | 4.¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet? 4.¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet?<br>4.¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos |

**Anexo 2** *Cronograma.*

| | | FEBRERO/MARZO | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | SEMANA #1 | | | | | SEMANA #2 | | | | | SEMANA #3 | | | | | SEMANA #4 | | | | | SEMANA #5 | | | | |
| No. | Actividad | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V |
| 1 | Anteproyecto | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Escogencia del tema | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Recolección de datos | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Estructuracion del proyecto | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Levantado de texto | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Entrega del protocolo | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | MARZO | | | | | | | | | | | | | | | | | | | | | | | | |
| | | SEMANA #1 | | | | | SEMANA #2 | | | | | SEMANA #3 | | | | | SEMANA #4 | | | | | SEMANA #5 | | | | |
| No. | Actividad | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V |
| 2 | Desarrollo de la tésis | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Diseño metodológico | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Capítulo II | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Capítulo III | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Conclusiones | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Entrega de borrador | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | ABRIL | | | | | | | | | | | | | | | | | | | | | | | | |
| | | SEMANA #1 | | | | | SEMANA #2 | | | | | SEMANA #3 | | | | | SEMANA #4 | | | | | SEMANA #5 | | | | |
| No. | Actividad | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V | L | M | M | J | V |
| 3 | Mejoras y correcciones | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Correcciones y cambios | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Entrega | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Revision de español | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Sustentación | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Entrega Final | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|---|---|
| | Actividad |
| | Actividad Realizada |
| | Finalizado |
| | Actividad por realizar |

**Cuadro de elaboración propia**

**Anexo 3** *Guion de Entrevista.*

Universidad de Panamá
Facultad de Administración de Empresas y Contabilidad
Dirección de Investigación y Postgrados
Entrevista sobre Gestión de Riesgos Bancarios

La presente entrevista va dirigida a profesionales y/o Gerentes de Riesgos. Busca determinar si la entidad guarda concordancia con las normas de Gobierno Corporativo en lo que respecta a adopción de políticas, normas, procedimientos, estructuras de control interno que garanticen la integridad y eficiencia de los procesos de gestión de riesgo**.**

1. **¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet?**
2. **¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica?**
3. **¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet?**
4. **¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet?**
5. **¿Cuál es la clasificación o tipos de los delitos Informáticos identificados por los bancos?**
6. **¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet?**
7. **¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet?**
8. **¿Con qué frecuencia se realizan evaluaciones de los riesgos tecnológicos que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?**
9. **¿Con qué frecuencia se realizan evaluaciones de los riesgos operacionales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?**
10. **¿Con qué frecuencia se realizan evaluaciones de los riesgos legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?**

**11. ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet?**

## Cambios realizados por sugerencias de los expertos

1. Se descarta el uso del ítem número 4, ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet?, ya que obtuvo un puntaje de 0.50 y su eliminación no compromete los resultados.

2. Se modifica el ítem número 6, a, ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet?, por sugerencia de los expertos, con esta modificación lo que se busca es que el entrevistado indique los tipos de delitos informáticos identificados por los bancos.

3. Se extiende el ítem número 9, ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?, a tres preguntas, por sugerencia de los expertos, con la finalidad que se obtengan resultados separados con cada una de estas.

## **Anexo 4** *Cuestionario.*

Universidad de Panamá
Facultad de Administración de Empresas y Contabilidad
Dirección de Investigación y Postgrados
Encuesta sobre Delitos Informáticos

El presente Cuestionario es dirigido a Cuentahabientes que manejan Banca por Internet. Busca determinar el conocimiento que posee el público acerca de los delitos informáticos y su influencia a las operaciones de banca por Internet**. Favor marcar una sola vez por pregunta con un gancho o palomita; la información suministrada será manejada bajo estricta confidencialidad. Agradecemos su colaboración.**

1. ¿Qué tipo de servicios de banca electrónica utiliza?
   ( ) Banca en línea
   ( ) Banca Móvil
   ( ) Banca por teléfono
   ( ) Terminales de punto de venta (POS)
   ( ) Tarjeta Bancaria (Visa/Clave)

2. ¿Qué tipo de servicios de Banca por Internet utiliza con más frecuencia?
   ( ) Compras por Internet
   ( ) Pagos a terceros
   ( ) Transferencias

3. ¿Con qué frecuencia utiliza los servicios de banca a través de medios o canales electrónicos?
   ( ) Siempre
   ( ) Casi siempre
   ( ) Algunas Veces
   ( ) Casi nunca
   ( ) Nunca

4. ¿Considera las compras por Internet seguras?
   ( ) Nada
   ( ) Poco
   ( ) Mucho

5. ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet?
   ( ) Nada
   ( ) Poco
   ( ) Mucho

6. ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet?
   ( ) Siempre
   ( ) Casi siempre
   ( ) Algunas Veces
   ( ) Casi nunca
   ( ) Nunca

7. ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos?
   ( ) Nada

( ) Poco
( ) Mucho

8. ¿Sabes cuáles son los pasos por seguir para denunciar los delitos informáticos en Panamá?
( ) Nada
( ) Poco
( ) Mucho

9. ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos?
( ) Siempre
( ) Casi siempre
( ) Algunas veces
( ) Casi nunca
( ) Nunca

10. ¿De los tipos de delitos enunciados señale cual considera el más común a los servicios de banca por Internet?
( ) Hackeo
( ) Robo de identidad (*Phishing o Pharming*)
( ) Malware
( ) Ataques dirigidos (*Sniffing o Spoofing, Desfiguración de sitios web)*

11. ¿De los tipos delitos enunciados señale cual considera el más común a los sistemas informáticos?
( ) Hackeo
( ) Piratería informática
( ) Malware
( ) Ransomware
( ) Ataques dirigidos (*Sniffing, Spoofing, Desfiguración de sitios web, etc.)*

12. ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Internet?
( ) Hackeo
( ) Robo de identidad (*Phishing o Pharming*)
( ) Malware
( ) Ataques dirigidos (Sniffing o Spoofing, Defiguración de sitios web)

13. ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados?
( ) Totalmente de acuerdo
( ) Parcialmente de acuerdo
( ) Ni de acuerdo ni en desacuerdo
( ) Parcialmente en desacuerdo,
( ) Totalmente en desacuerdo.

14. ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos?
( ) Totalmente de acuerdo
( ) Parcialmente de acuerdo
( ) Ni de acuerdo ni en desacuerdo
( ) Parcialmente en desacuerdo
( ) Totalmente en desacuerdo.

15. ¿Posee alguna experiencia en el uso de redes de comunicación?
( ) Nada
( ) Poco
( ) Mucho

16. ¿Posee alguna experiencia en el uso de sistemas de información?
( ) Nada
( ) Poco
( ) Mucho

17. ¿Posee alguna experiencia en el uso de cualquier medio electrónico?
( ) Nada
( ) Poco
( ) Mucho

18. ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informáticos?
( ) Siempre
( ) Casi siempre
( ) Algunas veces
( ) Casi nunca
( ) Nunca.

## Cambios realizados por sugerencias de los expertos

1. Se descarta el uso de ítem número 1, de identificación del informante, “Edad”, debido a que obtuvo un puntaje de 0.50, y eliminarlo no compromete los resultados.
2. El ítem número 11, de la variable delitos informáticos, ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias?, fue considerada no esencial por los jueces, también se descarta por que obtuvo un puntaje de 0.5, su eliminación tampoco compromete los resultados.
3. El ítem número 17, correspondiente a la variable delitos informáticos, ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico?, por sugerencia de los expertos se extiende a tres preguntas. Con el instrumento anterior se buscaba saber el grado de experiencia del cuentahabiente en aspectos tecnológicos específicos. Se sugiere separar este ítem en varias preguntas, toda vez que se puedan obtener resultados separados, por lo que se realiza el ajuste en base a estas observaciones.

**Anexo 5** *Descripción del instrumento.*

| DESCRIPCIÓN DEL INSTRUMENTO | | | | |
|---|---|---|---|---|
| | Tipo de instrumento | Encuesta | Entrevista | Matrtiz |
| | Total de preguntas | 15 | 6 | 4 |
| Obj./Variabes | | | | |
| E1 | Identificar cuáles son los tipos de delitos informáticos que afectan las operaciones de banca electrónica de entidades bancarias en la ciudad de Panamá y sus repercusiones. | 7,9,11 | 1,4 | 2 |
| E2 | Analizar cuáles son los delitos informáticos más recurrentes en las operaciones de banca electrónica de bancos que manejen este tipo de transacciones en la ciudad de Panamá. | 8 | 3 | 4 |
| E3 | Determinar la forma de mitigar los riesgos de delitos informáticos que se derivan de las operaciones de banca electrónica de bancos de la ciudad de Panamá. | 5,6,13 | 5,6,8,10 | 3 |
| VI | Delitos informáticos. | 4,14,15 | 2 | 1 |
| VD | Operaciones bancarias | 1,2,3,10,12 | 7,9,11 | 0 |

**Anexo 6** *Validación del instrumento Cuestionario.*

| VALIDACIÓN DE INSTRUMENTO-CUESTIONARIO | | | | | | |
|---|---|---|---|---|---|---|
| **Variable** | **Indicador** | **#Item** | **A** | **B** | **C** | **$CVR_1$** |
| ID del informante | Edad | 1 | 4 | 4 | 0 | 0,500 |
| Independiente | ¿Consideras que las compras por Internet seguras? | 5 | 6 | 2 | 0 | 0,750 |
| | ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? | 6 | 7 | 1 | 0 | 0,875 |
| | ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet? | 7 | 7 | 1 | 0 | 0,875 |
| | ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | 8 | 7 | 1 | 0 | 0,875 |
| | ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | 9 | 8 | 0 | 0 | 1,000 |
| | ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | 10 | 7 | 1 | 0 | 0,875 |
| | ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias? | 11 | 4 | 3 | 1 | 0,500 |
| | ¿De los tipos de delitos enunciados señale cuál considera el más común que afeca a los servicios de banca por Internet? | 12 | 8 | 0 | 0 | 1,000 |
| | ¿De los tipos de delitos enunciados señale cuál considera el más común que afecta a los sistemas informáticos? | 13 | 7 | 0 | 1 | 0,875 |
| | ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos? | 16 | 6 | 2 | 0 | 0,750 |
| | ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico? | 17 | 4 | 4 | | 0,500 |
| | ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informáticos? | 18 | 6 | 2 | 0 | 0,750 |
| Dependiente | ¿Qué tipo de servicios de banca electrónica utiliza? | 2 | 6 | 2 | 0 | 0,750 |
| | ¿Qué tipo de servicios de banca por Internet utiliza? | 3 | 8 | 0 | 0 | 1,000 |
| | ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | 4 | 8 | 0 | 0 | 1,000 |
| | ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Internet? | 14 | 7 | 0 | 1 | 0,875 |
| | ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | 15 | 8 | 0 | 0 | 1,000 |
| | Suma= | | 118 | 23 | 3 | 14,750 |
| | **A=ESENCIAL** | | | CVI global= | | 0,819 |
| | **B=ÚTIL PERO NO ESENCIAL** | | CVI items aceptables= | | | 0,883 |
| | **C= NO ESENCIAL** | | | | | |

**Anexo 7** *Validación del instrumento Entrevista.*

| VALIDACIÓN DE INSTRUMENTO-ENTREVISTA | | | | | | |
|---|---|---|---|---|---|---|
| Variable | Indicador | #Item | A | B | C | CRV |
| Independiente | ¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet? | 1 | 7 | 1 | 0 | 0,875 |
| Dependiente | ¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica? | 2 | 6 | 2 | 0 | 0,75 |
| | ¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet? | 3 | 8 | 0 | 0 | 1 |
| | ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet? | 4 | 4 | 4 | 0 | 0,5 |
| | ¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet? | 5 | 8 | 0 | 0 | 1 |
| | ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet? | 6 | 6 | 2 | 0 | 0,75 |
| | ¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet? | 7 | 7 | 1 | 0 | 0,875 |
| | ¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet? | 8 | 7 | 1 | 0 | 0,875 |
| | ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet? | 9 | 7 | 1 | 0 | 0,875 |
| | ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet? | 10 | 5 | 3 | 0 | 0,625 |
| | SUMA = | | 65 | 15 | 0 | 8,125 |
| | A=ESENCIAL | | | CVI global= | | 0,8125 |
| | B=ÚTIL PERO NO ESENCIAL | | | CVI Items aceptables= | | 1,0156 |
| | C= NO ESENCIAL | | | | | |

## Anexo 8

*Validación del Instrumento por Juicio de expertos, Dra. Maricela Sevilla Caro.*

---

| Validación de Instrumento Cuestionario-Dra. Maricela Sevilla Caro | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E** | **No esencial** | **Validación** |
| 1 | Edad | | X | | |
| 2 | ¿Qué tipo de servicios de banca electrónica utiliza? | | X | | |
| 3 | ¿Qué tipo de servicios de banca por Internet utiliza? | X | | | |
| 4 | ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | X | | | |
| 5 | ¿Consideras que las compras por Internet seguras? | X | | | |
| 6 | ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Interr | X | | | |
| 7 | ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Inter | X | | | |
| 8 | ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | X | | | |
| 9 | ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | X | | | |
| 10 | ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | X | | | |
| 11 | ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias? | X | | | |
| 12 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afeca a los servicios de banca por Internet | X | | | |
| 13 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afecta a los sistemas informáticos? | X | | | |
| 14 | ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Inte | X | | | |
| 15 | ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | X | | | |
| 16 | ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos? | X | | | |
| 17 | ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico? | | X | | |
| 18 | ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informático | X | | | |

***La Doctora Maricela Sevilla no emitio comentarios sobre las preguntas del cuestionario.**

**Anexo 9** *Validación del instrumento por Juicio de expertos, Dr. Carlos Flores.*

| Validación de Instrumento Cuestionario-Dr. Carlos Flores | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E.** | **No esencial** | **Validación** |
| 1 | Edad | | | | |
| 2 | ¿Qué tipo de servicios de banca electrónica utiliza? | x | | | |
| 3 | ¿Qué tipo de servicios de banca por Internet utiliza? | x | | | |
| 4 | ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | x | | | |
| 5 | ¿Consideras que las compras por Internet seguras? | x | | | |
| 6 | ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? | x | | | |
| 7 | ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet? | x | | | |
| 8 | ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | x | | | |
| 9 | ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | x | | | |
| 10 | ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | x | | | |
| 11 | ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias? | x | | | |
| 12 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afeca a los servicios de banca por Internet? | x | | | |
| 13 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afecta a los sistemas informáticos? | x | | | |
| 14 | ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Internet? | x | | | |
| 15 | ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | x | | | |
| 16 | ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos? | x | | | |
| 17 | ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico? | x | | | |
| 18 | ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informáticos? | x | | | |
| **#Item** | **Observaciones del experto** | | | | |
| 1 | Agregaria otra pregunta sobre estudios, como proxi de ingresos | | | | |
| 2 | Agregaria opcion de Nose y Otros | | | | |
| 3 | Agregaria opcion de Nose y Otros | | | | |
| 4 | Medir frecuencia con tiempo, por ejemplo una vez a la semana, o dos veces o de 1 a 2, de 3 a 4, o por mes | | | | |
| 5 | Usar escala likert de 5 y formular pregunta como percepción | | | | |
| 6 | Usar escala likert de 5 y formular pregunta como percepción | | | | |
| 7 | Descomponer esta pregunta en varias, en funcion de la cantidad de riesgos que se identifican en la literatura que manejan | | | | |
| 8 | Usar escala likert de 5 y formular pregunta como percepción | | | | |
| 9 | Usar escala likert de 5 y formular pregunta como percepción | | | | |
| 10 | ok | | | | |
| 11 | ok | | | | |
| 12 | Agregaria opcion de Nose y Otros | | | | |
| 13 | Agregaria opcion de Nose y Otros | | | | |
| 14 | Agregaria opcion de Nose y Otros | | | | |
| 15 | Ok | | | | |
| 16 | ok | | | | |
| 17 | Separar en varias, una de uso de redes, otra de sistemas de información y otra con posibles otros medios electronicos | | | | |
| 18 | Agregar no se, indica que hay falta de informacion y nunca significaria que sabe pero que no lo usa. | | | | |

**Anexo 10** *Validación del instrumento por Juicio de expertos, Dra. Magdalena Serrano.*

| Validación de Instrumento Cuestionario-Dra. Magdalena Serrano | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E** | **No esencial** | **Validación** |
| 1 | Edad | | X | | |
| 2 | ¿Qué tipo de servicios de banca electrónica utiliza? | X | | | |
| 3 | ¿Qué tipo de servicios de banca por Internet utiliza? | X | | | |
| 4 | ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | X | | | |
| 5 | ¿Consideras que las compras por Internet seguras? | | X | | |
| 6 | ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Interr | X | | | |
| 7 | ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Inter | X | | | |
| 8 | ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | | X | | |
| 9 | ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | X | | | |
| 10 | ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | | | | |
| 11 | ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias? | | X | | |
| 12 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afeca a los servicios de banca por Internet | X | | | |
| 13 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afecta a los sistemas informáticos? | X | | | |
| 14 | ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Inte | X | | | |
| 15 | ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | X | | | |
| 16 | ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos? | | X | | |
| 17 | ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico? | X | | | |
| 18 | ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informático | X | | | |
| | | | | | |
| | **Observación general:** | | | | |
| | REVISAR LAS POSIBLES RESPUESTAS DE LAS PREGUNTAS 4,5,6,7,8,9,10,11, 15,16,17,18,19 | | | | |
| | DEBE REPLANTEAR SUS RESPUESTAS ESPERADAS. | | | | |

**Anexo 11** *Validación del instrumento por Juicio de expertos, Mcc. Hernán Parra.*

| Validación de Instrumento Cuestionario-Mcc. Hernán Parra | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E** | **No esencial** | **Validación** |
| 1 | Edad | X | | | |
| 2 | ¿Qué tipo de servicios de banca electrónica utiliza? | X | | | |
| 3 | ¿Qué tipo de servicios de banca por Internet utiliza? | X | | | |
| 4 | ¿Con que frecuencia utiliza los servicios de banca a través de medios o canales electrónicos? | X | | | |
| 5 | ¿Consideras que las compras por Internet seguras? | | X | | |
| 6 | ¿Posee algún conocimiento sobre los delitos informáticos que pueden afectar sus bienes a través de la banca por Internet? | X | | | |
| 7 | ¿La entidad financiera donde posee su cuenta le ha informado de los riesgos producto del mal uso de la banca por Internet? | | X | | |
| 8 | ¿Posee algún conocimiento de regulaciones o leyes que le ayuden a proteger sus bienes de los delitos informáticos? | X | | | |
| 9 | ¿Sabes cuáles son los pasos a seguir para denunciar los delitos informáticos en Panamá? | X | | | |
| 10 | ¿Consideras que se les da seguimiento a las denuncias por delitos informáticos en Panamá? | | X | | |
| 11 | ¿Consideras la solución a las denuncias por delitos informáticos en Panamá son satisfactorias? | | | X | |
| 12 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afeca a los servicios de banca por Internet? | X | | | |
| 13 | ¿De los tipos de delitos enunciados señale cuál considera el más común que afecta a los sistemas informáticos? | | | X | |
| 14 | ¿De los tipos delitos enunciados señale cual considera causa mayores afectaciones a las operaciones de banca por Internet? | | | X | |
| 15 | ¿Considera usted que los niveles de seguridad ofrecidos por los bancos a los cuentahabientes son adecuados? | X | | | |
| 16 | ¿Considera usted que las entidades bancarias deben hacer frente a las afectaciones ocurridas a usuarios de banca por Internet por delitos informáticos? | | X | | |
| 17 | ¿Posee alguna experiencia en el uso de redes, sistemas de información o cualquier medio electrónico? | | X | | |
| 18 | ¿Utiliza algún mecanismo de protección en su computador o medio electrónico para evitar daños por delitos informáticos? | X | | | |
| **#Item** | **Observaciones del experto** | | | | |
| 12 | No usar tecnisismo o simplificarlo, usar terminos(palabras) entendibles para cualquier persona cuentahabiente. | | | | |

**Anexo 12** *Validación del instrumento por Juicio de Expertos, Dra. Maricela Sevilla Caro.*

| Validación de Instrumento Entrevista-Dra. Maricela Sevilla Caro | | | | | |
|---|---|---|---|---|---|
| #Item | Dimesión/Constructo | Esencial | Útil pero N.E | No esencial | Validación |
| 1 | ¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet? | X | | | |
| 2 | ¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica? | X | | | |
| 3 | ¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet? | X | | | |
| 4 | ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet? | X | | | |
| 5 | ¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet? | X | | | |
| 6 | ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet? | | X | | |
| 7 | ¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet? | X | | | |
| 8 | ¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet? | X | | | |
| 9 | ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet? | | X | | |
| 10 | ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet? | | X | | |

**Anexo 13** *Validación de instrumento por Juicio de Expertos, Dr. Carlos Flores.*

| Validación de instrumento Entrevista- Dr. Carlos Flores | | | | | |
|---|---|---|---|---|---|
| #Item | Dimesión/Constructo | Esencial | Útil pero N.E. | No esencial | Validación |
| 1 | ¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet? | X | | | |
| 2 | ¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica? | X | | | |
| 3 | ¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet? | X | | | |
| 4 | ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet? | | X | | |
| 5 | ¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet? | X | | | |
| 6 | ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet? | X | | | |
| 7 | ¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet? | X | | | |
| 8 | ¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet? | X | | | |
| 9 | ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet? | X | | | |
| 10 | ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet? | X | | | |

**Anexo 14** *Validación de instrumento por Juicio de Expertos, Dra. Magdalena Serrano.*

| Validación de Instrumento Entrevista-Dra. Magdalena Serrano | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E** | **No esencial** | **Validación** |
| 1 | **¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet?** | X | | | |
| 2 | **¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica?** | X | | | |
| 3 | **¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet?** | X | | | |
| 4 | **¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet?** | | X | | |
| 5 | **¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet?** | X | | | |
| 6 | **¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet?** | X | | | |
| 7 | **¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet?** | | | | |
| 8 | **¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet?** | x | | | |
| 9 | **¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet?** | X | X | | |
| 10 | **¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet?** | X | | | |
| **#Item** | **Observaciones del experto** | | | | |
| 6 | No esta muy clara esta pregunta, creo que es algo com¿Cual es la clasificación o tipos de los delitos Informáticos identificados por los bancos? | | | | |
| 8 | Me parece que tiene 3 preguntas en 1, por lo que después de cierto punto se pierde el sentido de la pregunta, favor de replantearla. | | | | |

**Anexo 15** *Validación de instrumento por Juicio de Expertos, MCC Hernán Parra.*

| Validación de Instrumento Entrevista-MCC Hernán Parra | | | | | |
|---|---|---|---|---|---|
| **#Item** | **Dimesión/Constructo** | **Esencial** | **Útil pero N.E.** | **No esencial** | **Validación** |
| 1 | ¿Mencione de qué forma influyen a la entidad los delitos informáticos a las operaciones de banca por Internet? | X | | | |
| 2 | ¿Mantiene la entidad datos estadísticos de los delitos informáticos más recurrentes a las operaciones de banca electrónica? | | X | | |
| 3 | ¿Qué tipo de controles son ofrecidos a los cuentahabientes para evitar el riesgo por mal uso de la banca por Internet? | X | | | |
| 4 | ¿Existe algún mecanismo para ejercer control sobre los delitos informáticos ocurridos a la banca por Internet? | | X | | |
| 5 | ¿Qué tipo de riesgo de los mencionados vulnera más las operaciones de banca por Internet? | X | | | |
| 6 | ¿Bajo qué tipo de riesgo clasifica el banco los delitos informáticos a operaciones de banca por Internet? | X | | | |
| 7 | ¿En qué medida la entidad bancaria se hace responsable por afectaciones producto de delitos informáticos a operaciones de banca por Internet? | X | | | |
| 8 | ¿Indica la Gestión de Riesgo Tecnológico cómo se puede mitigar los delitos informáticos que se derivan de operaciones realizadas a la banca por Internet? | X | | | |
| 9 | ¿Con que frecuencia se realizan evaluaciones de los riesgos tecnológicos, operacionales y legales que tienen que ver con delitos informáticos a operaciones realizadas a banca por Internet? | X | | | |
| 10 | ¿Sabe usted si la entidad mantiene alguna clasificación para los niveles de control ejercidos por el Gobierno Corporativo con relación a delitos informáticos a operaciones de banca por Internet? | X | | | |

**Anexo 16** *Anexo 117_ Ban08 Glosario.*

## Definiciones

**Banca Electrónica:**

**Banca electrónica**: Es la prestación de servicios bancarios a través de medios o Canales electrónicos. La banca electrónica involucra los servicios ofrecidos por: banca por internet, banca móvil, banca por teléfono, terminales de puntos de venta (POS), mensajería instantánea (chat), redes sociales, correo electrónico, firma electrónica, dinero electrónico, red ACH, redes especializadas, cajeros automáticos, monedero o pago móvil, tarjeta bancaria con circuito integrado, medios de pago electrónico o cualquier otro medio o canal electrónico.

**Medios o canales electrónicos**: Dispositivo tecnológico de acceso, medios de transporte de datos, sistemas de almacenamiento o cualquier otra tecnología actual y futura, que sea empleada para consultar, ingresar, transportar, proteger, procesar y/o almacenar datos de clientes y sus transacciones bancarias.

**Canales:**

| Cód. De Canal | Canal de Banca Electrónica | Definición |
|---|---|---|
| 01 | Banca por Internet | Servicios de banca electrónica suministrados a clientes a través de internet, en el sitio que corresponda a uno o más dominios del banco, mediante protocolos HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure), o protocolos con propósitos equivalentes, indistinto del dispositivo tecnológico de acceso. |
| 02 | Banca por Teléfono (IVR) | Servicio de banca electrónica mediante el cual, el cliente envía instrucciones al banco a través de un sistema telefónico, fijo o móvil, por medio de tonos, pulsos o mecanismos de reconocimiento de voz, y recibe respuesta grabada o interactiva de voz. |
| 03 | Banca Telefónica voz a voz (Centro de Llamadas) | Servicio de banca electrónica mediante el cual el cliente provee instrucciones a través de un sistema telefónico, fijo o móvil, al banco por intermedio de un representante autorizado por la institución, ubicado en un centro de llamadas. |

| | | |
|---|---|---|
| 04 | Banca Móvil | Servicios de banca electrónica provistos a clientes a través de un teléfono móvil, cuyo número de línea se encuentre afiliado al servicio, mediante protocolos SMS (Short Message Service), WAP (Wireless Access Protocol) o protocolos con propósitos equivalentes. |
| 05 | Pago o Monedero Móvil | Servicio de banca electrónica en el cual el dispositivo tecnológico de acceso consiste en un dispositivo electrónico o un teléfono móvil del cliente, cuya línea telefónica se encuentra asociada al servicio. |
| 06 | Pago o Monedero Móvil Corresponsal no bancario | Servicio de banca electrónica en el cual el dispositivo tecnológico de acceso consiste en un dispositivo electrónico o un teléfono móvil del cliente, cuya línea telefónica se encuentra asociada al servicio y este es manejado por un corresponsal no bancario |
| 07 | ACH – Plataforma – Banco (Redes Especializadas) | Sistemas de transferencias de información y/o fondos, local, entre instituciones financieras y cualquier otra entidad que contenga información de clientes (la que utiliza el área de plataforma del banco), en este caso ACH |
| 08 | Redes Sociales | Medio o canal tecnológico de acceso, mediante el cual el cliente interactúa con un banco por internet o similar, y consulta o provee información por intermedio de un representante autorizado de la institución, sea o no en tiempo real. |
| 09 | Correo electrónico | Medio o canal tecnológico de acceso, mediante el cual el cliente intercambia información con un banco por internet, y consulta o provee información por intermedio de un representante autorizado de la institución |
| 10 | Kioscos electrónicos | Dispositivo tecnológico propio del banco que cuenta con una aplicación diseñada específicamente para el mismo y que brinda servicios de banca electrónica al cliente mediante un autoservicio; este se accede mediante un proceso de autenticación. |
| 11 | Kioscos electrónicos con Proveedores | Dispositivo tecnológico que pertenece a un proveedor (tercero), que cuenta con una aplicación diseñada específicamente para el mismo y que brinda servicios |
| | | de banca electrónica al cliente mediante un autoservicio; este se accede mediante un proceso de autenticación, para lo cual media un contrato entre el banco y el proveedor. |

| | | |
|---|---|---|
| 12 | Cajeros Automáticos propios | Dispositivo tecnológico de acceso propiedad del banco, que provee servicios de banca electrónica, al cual se accede mediante el uso de una tarjeta y/o procedimientos de autenticación. |
| 13 | Cajeros Automáticos con proveedores | Dispositivo tecnológico de acceso propiedad de un tercero, que provee servicios de banca electrónica para uno o varios bancos, al cual se accede mediante el uso de una tarjeta y/o procedimientos de autenticación, en el que media un contrato entre el banco y el proveedor (tercero). |
| 14 | Autobanco Electrónico | Dispositivo tecnológico de acceso que provee servicios de banca electrónica, al cual se accede mediante el uso de una tarjeta y/o procedimientos de autenticación, ubicado en un autobanco. |
| 15 | POS (Puntos de Venta) propios | Dispositivos tecnológicos de acceso, propiedad del banco, que permiten proveer servicios de banca electrónica, tales como datafonos, terminales electrónicas micro-computarizadas, teléfonos móviles y programas de cómputo, que pueden ser operados por individuos o comercios para debitar o acreditar cuentas bancarias, o bien para hacer cargos a tarjetas. |
| 16 | POS (Puntos de Venta) con proveedores | Dispositivos tecnológicos de acceso, propiedad de un tercero, que permiten proveer servicios de banca electrónica, tales como datafonos, terminales electrónicas micro-computarizadas, teléfonos móviles y programas de cómputo, que pueden ser operados por individuos o comercios para debitar o acreditar cuentas bancarias, o bien para hacer cargos a tarjetas; para lo cual media un contrato entre el banco y el proveedor |
| 17 | POS (Puntos de Venta) Corresponsales no bancarios | Dispositivos tecnológicos de acceso situados en un corresponsal no bancario, autorizado por el banco y este a su vez autorizado por la Superintendencia de Bancos, que permiten proveer servicios de banca electrónica, tales como datafonos, terminales electrónicas micro- computarizadas, teléfonos móviles y programas de cómputo, que pueden ser operados por individuos o comercios |
| | | para debitar o acreditar cuentas bancarias, hacer pagos a servicios o bien para hacer cargos a tarjetas. |

| | | |
|---|---|---|
| 18 | SWIFT (Redes Especializadas) | Sistemas de transferencias de información y/o fondos, internacional, entre instituciones financieras y otras entidades subscritas a la red, en este caso para las realizadas por la red SWIFT. |
| 19 | Comercio Electrónico (Redes Especializadas) | Sistemas de transferencias de información y/o fondos, internacional, entre instituciones financieras y otras entidades subscritas a la red (de la industria de las tarjetas), producto de la venta en comercios electrónicos |
| 20 | Fax | Dispositivo tecnológico de acceso, medios de transporte de datos, sistemas de almacenamiento o cualquier otra tecnología actual y futura, que sea empleada para consultar, ingresar, transportar, proteger, procesar y/o almacenar datos de clientes y sus transacciones bancarias. En este caso para realizar solicitudes, notificaciones, consultar, o sea servicios no transaccionales. |

**Anexo 17** *Fichas para la recolección de datos 1.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#1** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Cifra y tasa de crecimiento de usuarios en Internet de 2000 a 2019.** | |
| **Referencia Bibliográfica: Organización de los Estados Americanos (OEA 2019), Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.** | |
| **Texto:** "Internet ha revolucionado el mundo que nos rodea y la forma en que interactuamos con los demás. Esto es particularmente cierto en América Latina y el Caribe, ya que casi 70% de la población está en línea y la tasa de crecimiento de usuarios de Internet es la tercera más alta del mundo – es decir, 2,4% entre 2000-2019.1 En las Américas y el Caribe, se utiliza Internet para relacionarse con las personas, compartir ideas, gestionar negocios y realizar transacciones. Por todo ello, el sector financiero fue uno de los primeros en adoptar las tecnologías y ofrecerlas a sus clientes" (p.8). | |

**Anexo 18** *Fichas para la recolección de datos 2.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#2** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Cifra de población bancarizada y que ha hecho operaciones de banca por Internet en Colombia 2018.** | |
| **Referencia Bibliográfica: Organización de los Estados Americanos (OEA 2019), Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.** | |
| **Texto:** "El sector financiero ha experimentado uno de los mayores índices de digitalización en los últimos años. Cada día un mayor número de clientes usan medios no presenciales para realizar transacciones por internet, pagos a través de dispositivos móviles o cualquier otro tipo de trámites bancarios. En Colombia, se estima que la población bancarizada dentro del universo de internautas es de 81%, y que 79,4% de la población bancarizada internauta ha consultado o hecho operaciones bancarias en línea en 2018" (p.8). | |

**Anexo 19** *Ficha para la recolección de datos 3.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#3** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Porcentajes de ataques exitosos y no exitosos en seguridad digital y motivaciones de estos durante 2017 y 2018.** | |
| **Referencia Bibliográfica: Organización de los Estados Americanos (OEA 2018), Estudio "El Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe** | |
| **Texto:** "el 92% de las entidades bancarias identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital, y el 37% de entidades bancarias manifestaron que sí fueron víctimas de ataques exitosos. La principal motivación de dichos ataques durante el año 2017 fueron motivos económicos (79% de las entidades bancarias víctimas)" (p.8). | |

**Anexo 20** *Ficha para la recolección de datos 4.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#4** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: IV Encuesta de victimización y percepción social de la seguridad, denominada La Victimización y percepción de la seguridad ciudadana en Panamá.** | |
| **Referencia Bibliográfica: Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP), Observatorio de Seguridad Ciudadana, el Programa de las Naciones Unidas para el Desarrollo (PNUD), VIII Informe de Seguridad Ciudadana (2017).** | |
| **Texto:** Grafica#8, Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples (p.12), que el 3% de los mismo fueron por Internet, en la Grafica #12, Hurto, Lugar donde ocurrió (p.13), el 4% circulando por una ruta/ autopista y por internet, cabe resaltar que en este informe en relación a ciberdelincuencia hay muy poco aporte; podemos apreciar que los delitos ocurridos por internet no se desglosan, por lo que no podemos saber que o a cual tipo de delito se refieren, además, en cuanto a la gráfica #32, Acciones o medidas para prevenir la delincuencia (p.22), no se observa ninguna que guarde relación a la prevención de los delitos informáticos; Sin embargo, se presentan los diferentes programas de seguridad al servicio de la ciudadanía y podemos apreciar que tampoco existe alguno que asesore, guíe o ayude a prevenir los mismos. | |

**Anexo 21** *Ficha para la recolección de datos 5.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#5** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Cifra de incidencias y denuncias para el año 2016 correspondientes al orden económico.** | |
| **Referencia Bibliográfica: Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). Informe de Criminalidad año (2016).** | |
| **Texto:** "El sexto lugar de incidentes y denuncias para el año 2016, corresponden a los Delitos contra el Orden Económico: registrando 826 casos, entre los que se destacan girar cheques sin fondos, uso indebido de tarjetas de crédito o débito, blanqueo de capitales (p.18). "Para efectos de análisis y fines consiguientes la ENVI estimó que 11,458 personas de 18 años de edad o más, fueron víctimas del delito de fraude bancario, calculando una prevalencia delictiva de 7 víctimas por cada mil habitantes, con un estimado en pérdidas de USD 9.2 millones, lo que hace obligante analizar y estudiar los actuales procedimientos internos de los cuenta habientes con el objetivo de robustecer aún más la tecnología inherente con el objetivo principal de reducir las incidencias en estos delitos" (p.116). | |

**Anexo 22** *Ficha para la recolección de datos 6***.**

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#6** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Cifra de incidencia y denuncias para el año 2016 correspondientes a delitos informáticos.** | |
| **Referencia Bibliográfica: Ministerio de Seguridad Pública, a través del Sistema Nacional Integrado de Estadísticas Criminales (SIEC). Informe de Criminalidad año (2016a).** | |
| **Texto:** Cuadro N° 01. (SIEC 2016b) Número, tasa y porcentaje de cambio en la tasa de incidencias y denuncias registradas en la república de Panamá por año, según clase de incidentes: años 2015 - 2016 (Continuación), si se ubica una línea para los delitos informáticos la cual señala que en 2016 se dio una incidencia de 35 casos en comparación con 2015 en la cual se dio una incidencia de 26 casos (p.21). Además, en el Cuadro N° 02. (SIEC 2016c) Incidencias y denuncias registradas en la república de Panamá por provincias y comarcas, según clase de incidentes: al mes de diciembre, año 2016 (p.25), muestra que, de los 35 casos, 24 fueron ocurridos en la provincia de Bocas del Toro, lo que indica que esta es la provincia con mayor número de casos o incidencias registradas, seguida de Panamá con 8 casos y las provincias de Colón, Chiriquí y Herrera con un caso respectivamente. Seguido, el Cuadro N° 03. (SIEC 2016d) Incidencias y denuncias registradas en la república de Panamá por mes, según clase de incidentes: al mes de diciembre año 2016, en el cual señala que el mes en que más incidencias se registraron fue en abril con 24, seguido de junio y septiembre con 2 respectivamente y enero, marzo, mayo, octubre y noviembre con 1 caso respectivamente. | |

**Anexo 23** *Ficha para la recolección de datos #7.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#7** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Porcentajes de victimización que tienen que ver con la ciberdelincuencia.** | |
| **Referencia Bibliográfica: Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP), Observatorio de Seguridad Ciudadana, el Programa de las Naciones Unidas para el Desarrollo (PNUD), VIII Informe de Seguridad Ciudadana (2017).** | |
| **Texto:** Grafica#8, Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples (p.12), que el 3% de los mismo fueron por Internet, en la Grafica #12, Hurto, Lugar donde ocurrió (p.13), el 4% circulando por una ruta/ autopista y por internet, cabe resaltar que en este informe en relación a ciberdelincuencia hay muy poco aporte; podemos apreciar que los delitos ocurridos por internet no se desglosan, por lo que no podemos saber que o a cual tipo de delito se refieren, además, en cuanto a la gráfica #32, Acciones o medidas para prevenir la delincuencia (p.22), no se observa ninguna que guarde relación a la prevención de los delitos informáticos; Sin embargo, se presentan los diferentes programas de seguridad al servicio de la ciudadanía y podemos apreciar que tampoco existe alguno que asesore, guíe o ayude a prevenir los mismos. | |

**Anexo 24** *Ficha para la recolección de datos #8.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#8** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Cifras y porcentajes de usuarios en Internet, en países en desarrollo y porcentajes de suscriptores a banda ancha en 2011.** | |
| **Referencia Bibliográfica: Oficina de Naciones Unidas contra la Droga y el Delito (UNODC 2013). Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno".** | |
| **Texto:** "En 2011 al menos 2.300 millones de personas, equivalente a más de un tercio de la población total del mundo, tuvo acceso a Internet. Más del 60% de todos los usuarios están en los países en desarrollo y el 45% de todos los usuarios de Internet tienen menos de 25 años. Se estima que para 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70% de la población mundial". | |

**Anexo 25** *Ficha para la recolección de datos #9.*

| **FICHA PARA LA RECOLECCIÓN DE DATOS** | **#9** |
|---|---|
| **UNIVERSIDAD DE PANAMÁ** | |
| **FACULTAD DE ADMINISTRACIÓN DE EMPRESAS Y CONTABILIDAD** | |
| **DOCTORADO EN CIENCIAS EMPRESARIALES** | |
| **Título: Tasas de victimización por fraude en línea.** | |
| **Referencia Bibliográfica: Oficina de Naciones Unidas contra la Droga y el Delito (UNODC 2013). Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno".** | |
| **Texto:** 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). | |