UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE NEGOCIOS

PROGRAMA ACADÉMICO DE ADMINISTRACION DE EMPRESAS

Análisis de los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años.

TESIS

Para optar el título profesional de Licenciado en Administración de Empresas

AUTORES

Aroni Córdova, Nancy (0000-0002-2192-1760)

Barrios Elías, Rita (0000-0002-7189-6532)

ASESOR

Jorge Ruíz, Marisol (0000-0003-0949-2876)

Lima, 19 de julio de 2018

DEDICATORIA

A DIOS Por la bendición de permitirnos llegar a esta etapa de nuestra carrera profesional, y permitirnos culminar con éxito y sobre todo llenos de salud y en compañía de nuestras familias.

A Nuestros Padres por su dedicación, amor y apoyo incondicional a lo largo de nuestras vidas. De igual forma a nuestros compañeros de vida por su cariño, ayuda y motivación en nuestro día a día.

AGRADECIMIENTOS

Agradecemos ante todo a Dios nuestro señor, por permitirnos vivir experiencias gratificantes como el alcanzar esta meta.

Así mismo, agradecemos de manera muy especial a nuestra asesora Licenciada Marisol Jorge por su guía y apoyo incondicional.

RESUMEN

El presente trabajo de investigación tiene por objetivo analizar el impacto en la gestión operacional, financiera e imagen institucional de los principales bancos de Lima Metropolitana como son el BCP Y BBVA debido al incremento de los ciberdelitos o delitos informáticos en el sistema financiero en los últimos 5 años. Este acto es cometido principalmente de forma digital, por lo que no permite que las entidades financieras puedan controlar en su totalidad. En el primer capítulo, desarrollamos el marco teórico que es fundamental para analizar de manera amplia y concisa el impacto que viene teniendo en los últimos 5años; identificaremos las distintas definiciones de ciberdelito, su clasificación, impacto económico a nivel mundial y finalmente su impacto en el Perú y en el sistema financiero peruano. En el capítulo siguiente, desarrollaremos la metodología de la investigación realizando un análisis claro y conciso de los principales bancos que vienen siendo afectados por los delitos informáticos. Todo ello se llevará a cabo a través del método de investigación y las técnicas e instrumentos de recopilación de datos, de modo que nos permitan identificar el impacto y la magnitud real con la cual los bancos se ven afectados por este hecho delictivo.

En el tercer capítulo realizaremos el análisis de la investigación realizada en el segundo capítulo; esto nos permitirá dar respuesta a nuestra pregunta de investigación ¿Cuáles son los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años?

En el capítulo cuarto, presentaremos los hallazgos, brechas y barreras encontradas durante nuestro proceso de investigación que nos permitirán tener un panorama más claro del problema propuesto.

Finalmente, en el quinto y último capítulo presentamos las conclusiones y recomendaciones a partir de los resultados arrojados de acuerdo a nuestra investigación desarrollada en los capítulos anteriores.

Palabras claves: Factores financieros, Reputación empresarial. Delitos informáticos, Entes reguladores, Ciberdelito.

ABSTRACT

The objective of this research is to analyze the impact on the operational and financial management of the main banks of Metropolitan Lima, due to the increase in cybercrimes or cybercrime in the financial system in the last 5 years. Cybercrime is committed mainly digitally, so it does not allow financial entities to control this criminal act in its entirety. In the first chapter, we develop the theoretical framework that is fundamental to analyze in a broad and concise way the impact that has been taking place in recent years; we will identify the different definitions of cybercrime, their classification, economic impact at world level and finally their impact on Peru and the Peruvian financial system. In the next chapter, we will analyze the main banks that are being affected, identifying the impact and the magnitude with which they are affected.

In the third chapter we will carry out the analysis of the research carried out in the second chapter. This will allow us to answer our research question. What are the main financial, operational and business reputation factors that are being impacted by the increase in cybercrime in the main banks in Peru, such as Banco de Crédito Del Peru and Banco Continental in the last 5 years?

In the fourth chapter, we will present the findings, gaps and barriers found during our research process that will allow us to have a clearer picture of the proposed problem. Finally, in the fifth and final chapter we present the conclusions and recommendations based on the results obtained according to our research developed in the previous chapters.

Keywords: Financial factors, Corporate reputation, Computer crimes, regulatory bodies, cybercrime.

INTRODUCCIÓN

En los últimos años, la evolución y desarrollo de la tecnología informática ha puesto disposición de nuestra sociedad una cantidad creciente de información de toda naturaleza. La producción, transmisión e intercambio de esta información ha ayudado de manera significativa a la transformación de las sociedades, organizaciones económicas y gubernamentales en general; sin embargo, este gran avance también implica una alta vulnerabilidad en todos los niveles sociales de un país o una sociedad debido a que han dado paso a la formación de nuevas conductas antisociales y delictivas no tradicionales como son los llamados “Ciber delitos” o Delitos informáticos que últimamente vienen representando un gran amenaza para las organizaciones ,inclusive para la economía de los países, ya que día a día se incrementan y van, inclusive, más rápido que los códigos penales establecidos de cualquier país.

Cada año los Ciber delitos o delitos informáticos vienen incrementándose se manera significativa a nivel global y nuestro país no es la excepción, siendo el sector financiero uno de los sectores más vulnerables. Durante los últimos años, las entidades bancarias vienen luchando contra los ataques informáticos que tienen día a día, ya sea hacia la misma entidad o teniendo como objetivo sus clientes. El impacto económico que se tiene a causa de este delito es muy alto. Un artículo publicado el 26 de setiembre por el diario Gestión indico que el líder mundial, representante de la consultora The Boston Consulting Group, Stefan Deustcher, en su presentación en el evento “Ciberseguridad: más allá de los bits & bytes" realizado en Lima en el 2017, indicó que los delitos informáticos le cuestan al mundo USD $ 575 mil millones de dólares al año y que el costo promedio por cada ciber ataque es de 11 millones de dólares y el 72% de las infracciones son causadas por fallas humanas . Es por ello que diversas entidades, entre ellas las entidades financieras, se han visto en la obligación de invertir más en la prevención de dichos delitos; además vienen realizando cambios en sus sistemas operativos y procesos operacionales con el fin de evitar más robos, clonaciones y fraudes. En nuestro país, uno de los más claros ejemplos de prevención contra estos delitos lo realizó en el 2018 la SBS (Superintendencia de Banca y Seguros) quien emitió una nueva norma donde, de manera obligatoria, las entidades financieras tenían que entregar a sus clientes tarjetas de débito y crédito con chip, con el fin de evitar las clonaciones de tarjeta.

Ante esta coyuntura, hemos identificado el siguiente problema de investigación ¿Cuáles son los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años?

La hipótesis planteada es que, tanto el incremento de presupuesto en gastos relacionados a tecnología de la información destinada a ciberseguridad; así como los cambios o la redefinición de los procesos operacionales; además de la pérdida de credibilidad, serían los principales factores que se ven afectados por el incremento de los ciberdelitos en los principales bancos de Lima Metropolitana como el BCP y el Banco Continental en los últimos 5 años.

Es por ello que planteamos como objetivo principal del presente trabajo de investigación, analizar el impacto en la gestión financiera y operacional e imagen de los principales bancos de Lima Metropolitana, debido al incremento de los ciberdelitos en los últimos 5 años.

Siendo los objetivos específicos:

1. Describir las variaciones en los procesos operacionales, de los principales bancos de Lima como son el BCP y BBVA debido al incremento de los ciberdelitos.
2. Analizar el impacto en la imagen y reputación de las principales entidades financieras de Lima como son el BCP y BBVA debido al incremento de ciberdelitos.
3. Analizar las variaciones en el incremento de presupuesto de gastos relacionados a tecnología de la información en el sistema financiero de los principales bancos de Lima como son el BCP Y BBVA.

En ese sentido justificamos la realización del presente trabajo de investigación porque consideramos su relevancia académica, social y práctica para las empresas involucradas y para la sociedad en su conjunto. Con respecto al primer plano consideramos de que siendo el "Ciberdelito" un fenómeno reciente de impacto mundial que año tras año viene atacando indiscriminadamente a todos los sectores y niveles de nuestra patria, todavía no existen suficientes estudios e investigaciones académicas sobre este fenómeno y su impacto en nuestra sociedad y sobre todo en las grandes empresas como la Banca nacional peruana; en ese sentido, consideramos que este estudio contribuirá y alentara a los futuros profesionales a que sigan investigando de modo que podamos seguir aportando información actualizada y valiosa a toda la comunidad estudiantil.

Por otro lado, nos referimos a la relevancia practica porque a partir de nuestro aporte las principales entidades financieras podrán obtener información actualizada y relevante sobre este fenómeno de modo que puedan tomar las acciones necesarias para seguir implementando métodos y sistemas de seguridad informática para así poder contrarrestar y evitar las consecuencias nefastas de este tipo de acciones ilegales; esto conllevará a que las entidades las entidades podrán brindarle mayor seguridad y protección a cada uno de sus clientes.

Finalmente, consideramos que esta tesis debe ser valorada, principalmente, por su contribución a la concientización de esta problemática a nuestra sociedad en general, ya que la información proporcionada desde el marco teórico analiza y abarca a todos ámbitos del quehacer cotidiano.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

CAPÍTULO I. MARCO TEÓRICO

1.1 Delitos Informáticos o Ciberdelitos

1.1.1 Definición

Uno de las primeras definiciones acerca del Ciber Delito lo hizo Parker (1976) quien define el Ciber Crimen o Delito Informático como “cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio” (p.12).

Por esas mismas épocas Camacho (1987) considerando que no había una definición clara del ciber crimen considera a este hecho como:

> Toda acción dolosa que provoca un perjuicio a personas o entidades sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas (p.25).

Sin embargo, con la expansión universal del internet en los últimos 10 años ha dado paso a nuevos análisis y nuevos conceptos ajustados más a nuestra realidad actual. En ese sentido Tellez-Valdez (2017) indica lo siguiente:

> Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable a través de vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática. (p.187)

En un sentido más amplio LINARES (2012) comprende al Ciber crimen como “todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión” (p .44)

Finalmente, tomando en consideración un entorno más cercano y ajustado a nuestra realidad como país, tomamos en consideración el aporte Villavicencio Terreros (2014)

quien define el delito Informático como “aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología” (p. 49)

De acuerdo a las definiciones encontradas y bibliografía consultada, llegamos a la conclusión que el ciber delito es un acto criminal realizad de manera digital en contra de una persona o entidad con el fin de obtener beneficio a raíz de dicho acto, así mismo podemos decir que no siempre genera un beneficio económico o material.

Clasificación de los Ciberdelitos o Delitos Informáticos.

Según una publicación del portal iberoamericano de ciencias penales el Convenio de Ciberdelincuencia del consejo de Europa firmado en Budapest por la Unión Europea propone la clasificación de los delitos informáticos en 4 grupos:

1. Delitos contra la confidencialidad, integridad y la disponibilidad de datos y sistemas informáticos.

- Acceso Ilícito
- Espionaje de datos
- Intervención ilícita
- Manipulación de datos

2. Delitos relacionados al contenido

- Material erótico
- Pornografía infantil
- Juegos Ilegales
- Difamación e información falsa

3. Delitos contra la religión.

- Delitos relacionados al Contenido
- Delitos en Materia de derechos del autor
- Infringir los derechos de autor para obtener ganancias financieras
- Delitos en Materia de marcas

4. Delitos Informáticos

Dichas definiciones las encontramos en la página del Banco de Crédito del Perú.

- **Phising / Spoofing:** Acceder ilegalmente un ordenador y enviar múltiples correos electrónicos; volver a enviar varios mensajes de correo electrónico comercial con la intención de engañar a los destinatarios; o falsificar información del encabezado en varios mensajes de correo electrónico.
- **Extorsión:** El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.
- **Hacking:** El hacking es acceder de forma ilegal a datos almacenados en un ordenador o servidor. El último caso sonado de hacking fue el robo de datos de los clientes de Ashley Madison.
- **Fraude:** La elaboración de cualquier plan para defraudar, o para la obtención de dinero o bienes mediante pretextos falsos o fraudulentos, usando Internet con el fin de ejecutar el plan.
- **Ciberbulling**: Uso de Internet para molestar, abusar, amenazar o acosar a la persona, a menudo de forma anónima. Los casos de ciberbulling parecen haber ido en aumento en los últimos años, con trágicas consecuencias en ocasiones
- **Malware**: También conocido como software malicioso (virus en general, troyanos, spyware…). Son programas informáticos que, una vez instalados y ejecutados en los equipos, puede dar el control parcial o total de estos a los criminales lo que les permite acceder fácilmente a cualquier información sensible o dañar/robar datos.
- **Ransomware:** Un ataque de 'ransomware' consiste en cifrar los archivos de un ordenador para impedir que el usuario tenga acceso a ellos. Una vez conseguido, lo más habitual es que aparezca un mensaje en la pantalla exigiendo el pago de unos 300 dólares en Bitcoins en un plazo de entre 48 y 72 horas. A cambio, el criminal promete entregar al usuario la clave que le permitirá desbloquear su dispositivo

5. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

- Copia y distribución de materiales informáticos
- Piratería Informática

Característica del Ciberdelito

En la segunda edición del libro Derecho informático 2010 el mexicano Julio Téllez Valdés presenta las siguientes características del Ciber delito:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen «beneficios» de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Repercusiones de los delitos informáticos.

1.2.1 Panorama mundial

Los ataques informáticos se han convertido en una industria global que crece día a día con cifras alarmantes. Según la encuesta global “Delitos económicos 2016 - Capítulo Argentina” realizada por la consultora internacional PWC (Price Whaterhouse Cooper) a 6400 participantes de 115 países; los delitos más comunes que han sido reportados por

las compañías en los últimos años son los delitos de malversación de activos y los delitos informáticos.

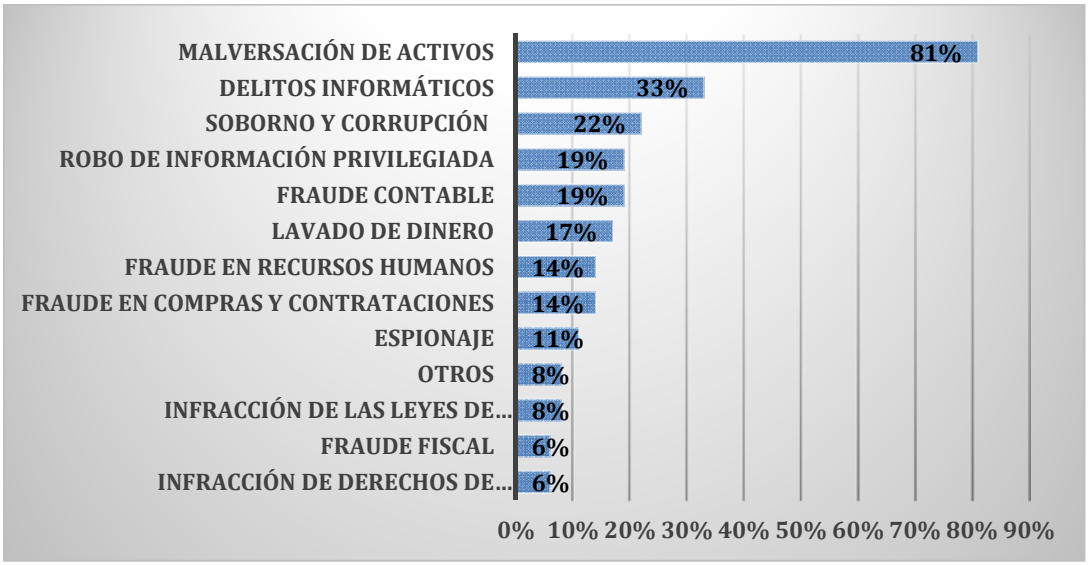

Figura 1: Delitos económicos más frecuentes reportados por las organizaciones en los últimos 24 meses, adaptado de la encuesta realizada por PWC Price whaterhouse Coopers, 2016.

En esa misma línea la evolución de los delitos informáticos se ha ido incrementando año a año consolidándose como el segundo delito de fraude más frecuente a nivel mundial. Según esta encuesta 1 de cada 3 empresas manifestaron haber sufrido un ataque cibernético con costos mayores a los US $ 50.000.

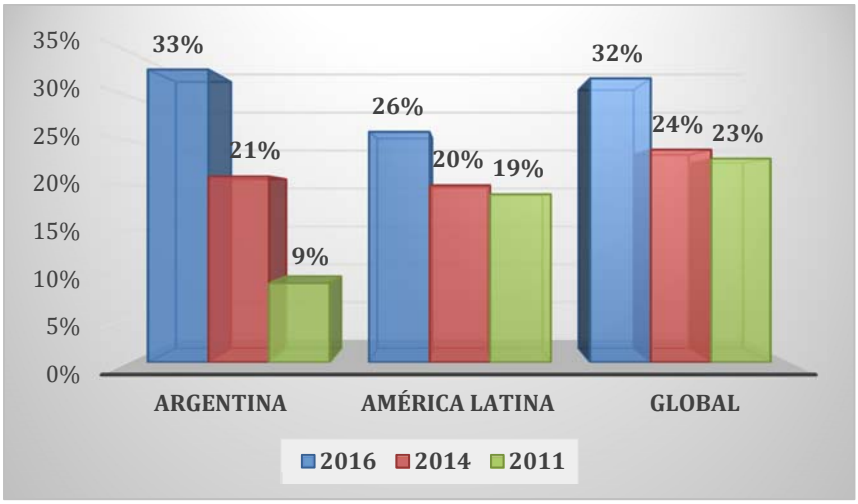

Figura 2: Evolución de los delitos informáticos, adaptado de la encuesta realizada por PWC Price Whaterhouse Coopers, 2016.

A pesar de los esfuerzos de inversiones millonarias en seguridad, las compañías todavía no han podido controlar los principales puertos de acceso a los delitos informáticos, siendo los empleados las principales causantes de dar acceso a los atacantes a través de la descarga de páginas infectadas con virus, uso de dispositivos infectados, etc. En el 2016 según un artículo llamado "las 15 estadísticas de TI para el 2017" publicado en su página web por la empresa Argentina TechTrade especialista en gerenciamiento y soluciones de TI; en los próximos 5 años (del 2017 al 2020) los gastos por ciber seguridad a nivel mundial superarán el billón de dólares esto incluye daños y desaparición de datos, robo de dinero, pérdida de productividad y sobre todo perjuicios a la reputación de las empresas. Este también indicó que en el año 2014 el mercado de ciber seguridad fue de US$ 3500 millones y en el 2017 llegaría a US$ 120.000 millones creciendo aproximadamente 35 veces en 13 años.

Por otro lado, según un artículo publicado por el Diario Gestión el 26 setiembre del 2017 el Cibercrimen le cuesta al mundo US $ 575 mil millones año al año, mientras que en Sudamérica y el Caribe tiene un costo de US$ 90 mil millones, cifra que representa casi el 50% del PBI del Perú. Este artículo también indica que de acuerdo al World Economic Forum Global Risk Report 2017, el Ciber crimen sigue siendo el segundo riesgo global no climático o migratorio afectando a todos los niveles de las industrias y sectores.

Los especialistas indican que estas cifras no son exactas ante la ausencia de datos de muchas partes del mundo.

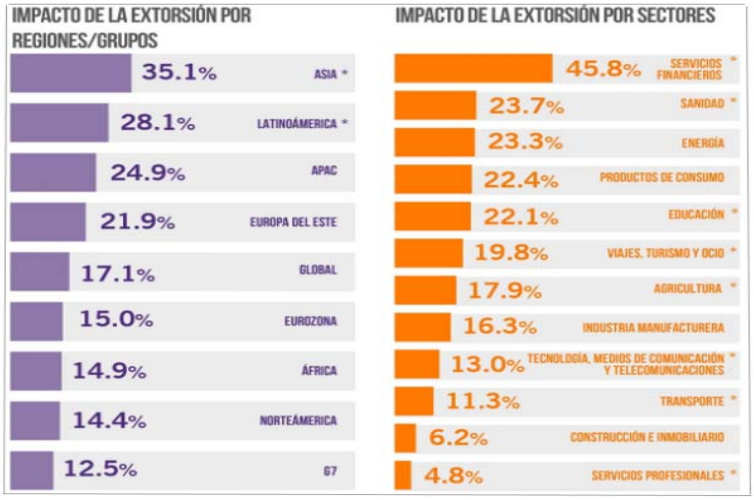

Figura 3: Impacto por Regiones y Sectores de delitos informáticos según encuesta trimestral "El impacto del Ciber Crimen en el mundo" realizada por International Bussines Report de Grand Thorton 2017.

Desde una mirada global y analizando los datos obtenidos, podemos inferir que gracias a las nuevas conexiones digitales y evolución tecnológica, los ataques cibernéticos seguirán incrementando con el paso de los años y todas las industrias están expuestas a sufrir un ataque, inclusive las menos pensadas; Sin embargo, al parecer las industrias a nivel mundial, todavía no son conscientes de la magnitud de este fenómeno ya que en el 2016 según los líderes del Banco Inter Americano de Desarrollo (BID) en conjunto con la Organización de Estados Americanos hicieron un llamado a los países de América Latina y el Caribe de modo que estas puedan acelerar sus esfuerzos en combatir el Ciberdelito. Esto debido al informe llamado Seguridad Cibernética 2016 que previamente se había realizado en apoyo con el centro global de seguridad cibernética la universidad de Oxford el cual reveló que cuatro de cada cinco países de la región no tienen estrategias de Ciberseguridad y tres de cada 4 países no cuentan con planes de protección de infraestructura crítica.

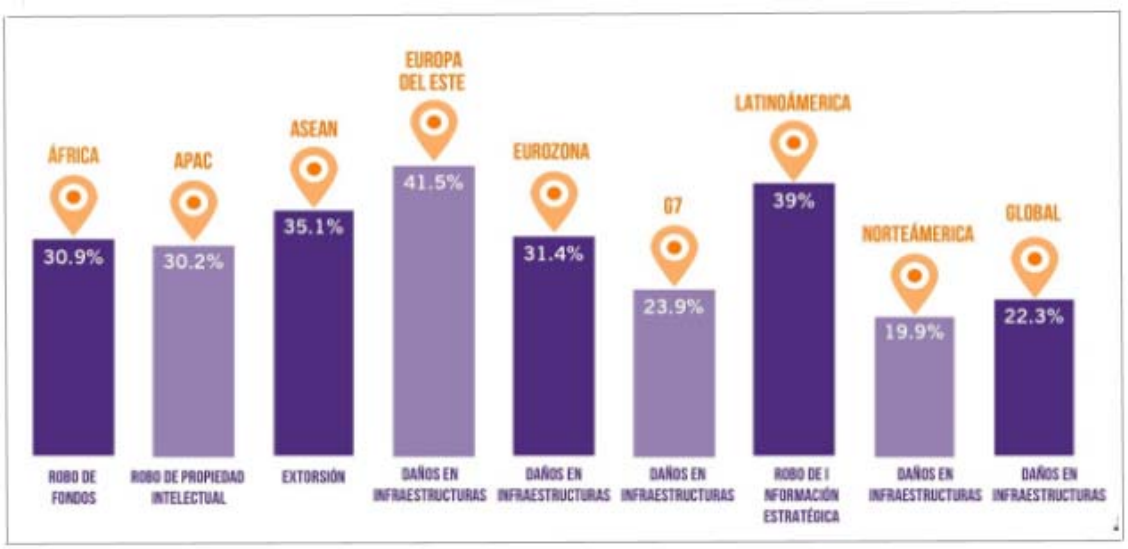

Figura 4: Tipos más comunes de ciberataques por regiones y países adaptado de la encuesta trimestral realizada por International Bussines Report de Grand Thorton 2017.

1.2.2 Latinoamérica y el Caribe

Una publicación realizada el 18 de setiembre del 2017 por la revista colombiana El Tiempo indicó que durante la cumbre de analistas de seguridad de la compañía Rusa KASPERSKY realizada en Argentina del 10 al 13 de setiembre , reveló que entre el 1ro de Enero y el 31 de agosto de ese mismo año se presentaron 677 millones de amenazas cibernéticas en todo Latinoamérica, eso quiere decir que cada hora se registraron 117

ataques concluyendo que estos incidentes aumentaron en un 59 % en comparación con el 2016.

En esa misma cumbre, también se determinó que Brasil es el país que más ataques registra con un 53 % seguido de México con un 17% y finalmente Colombia con 9% generando pérdidas económicas que ascienden a US$ 76,766 millones de dólares. Entre los países más afectados nuevamente se encuentra Brasil, con US$ 19,291 millones en pérdidas; seguido por México (US$ 11,921 millones), Venezuela (US$ 9,142 millones) y Argentina (US$ 7,400 millones).

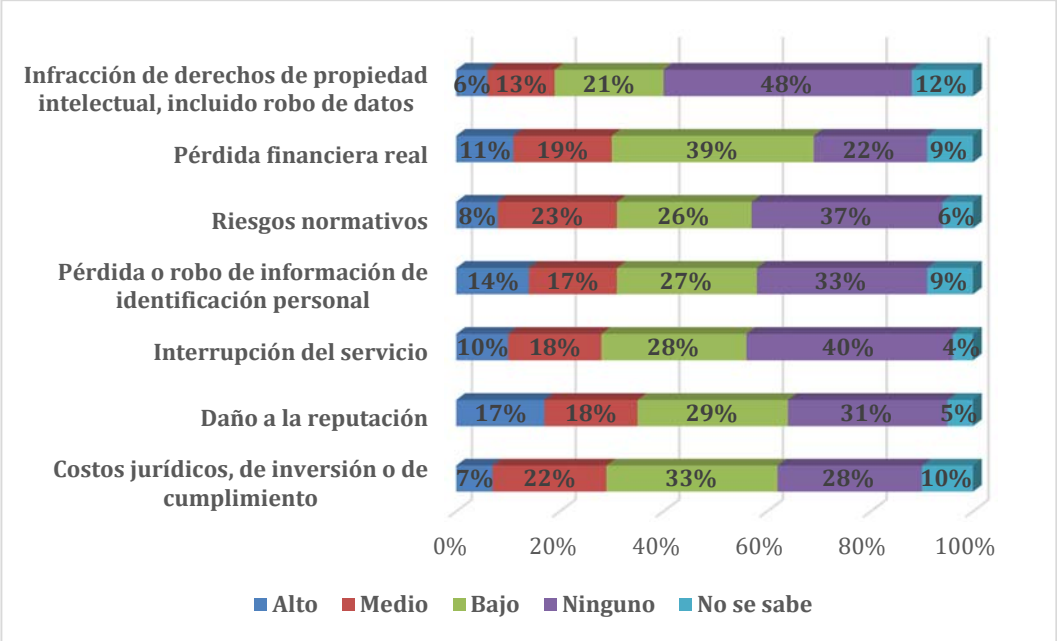

Figura 4: Pérdida financiera a causa de delitos informáticos según las organizaciones de América Latina, adaptado de la encuesta realizada por PWC Price Whaterhouse Coopers, 2016

Por otro lado, según KASPERSKY, la amenaza con mayor impacto en América Latina entre el 2016 y 2017 ha sido el Secuestro de datos, el incremento ha sido relevante tanto en la región como a nivel mundial por lo que este ataque se ha convertido en una epidemia global que ha generado pérdidas millonarias y daños irreparables en las distintas industrias. En esa misma línea, según el reporte "ESET Security Report Latinoamérica 2017" lanzado por la compañía de seguridad informática ESET, indica que los códigos maliciosos (Malware) se han posicionado como la principal causa de incidentes de seguridad en las compañías de la región con un considerable crecimiento en el 2017. Esto

quiere decir que el 46% (una de cada 2 empresas) de los 113 países que participaron en la encuesta afirmaron que fueron víctimas de algún tipo de malware.

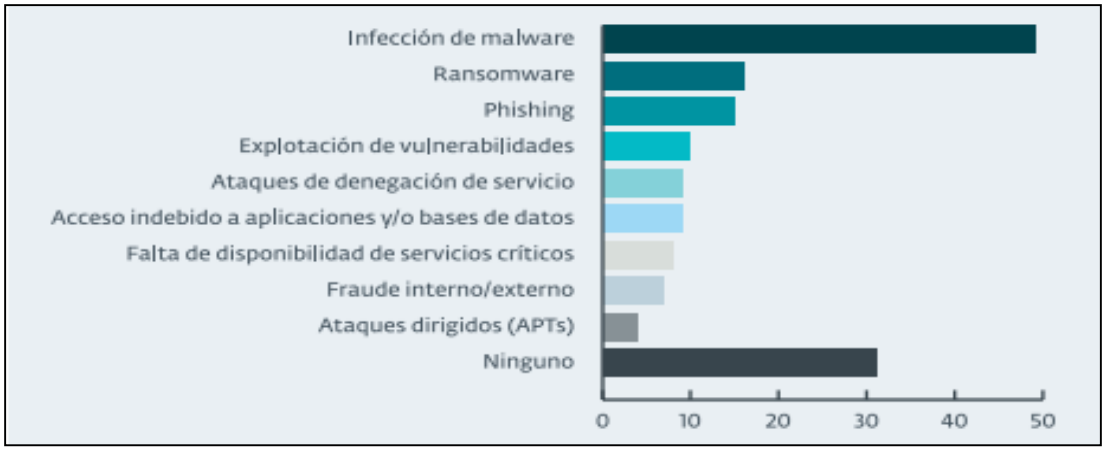

Figura 5: Incidentes de seguridad en empresas de Latinoamérica, adaptado del reporte ESET Security Report Latinoamérica 2017 realizado por la empresa WeLiveSecurity.

Como podemos observar, tanto a nivel mundial como a nivel Latinoamérica los delitos informáticos vienen siendo un potencial peligro; no solamente por las cuantiosas pérdidas económicas que se registran año a año, sino también por que las empresas a nivel mundial están siendo perjudicadas en su imagen y reputación, algo que es mucho más peligroso aún. En ese contexto, la firma de consultoría tecnológica e innovación Estadounidense Grand Torthon lo reafirmó en su encuesta "El impacto del Cibercrimen en el mundo" realizada en el 2017 a 2500 directivos empresariales de 36 economías a nivel mundial donde 26% de los encuestados indicaron que los Ciberdelitos habían afectado la reputación de las empresas en el que laboraban y que, además, no disponían de ciberseguros para poder contrarrestar estos ataques.

Figura 6: Principales consecuencias de delitos informáticos según encuesta trimestral realizada por International Bussines Report de Grand Thorton 2017.

1.2.3 Panorama Nacional – Perú

El crecimiento sostenido que ha tenido nuestro país en los últimos años ha traído consigo, entre otras cosas, la generación y desarrollo de empresas competitivas y tecnológicas quienes queriendo ser más eficientes poniéndose a la vanguardia de las grandes empresas multinacionales se han convertido 100% digitales, un claro ejemplo de esto lo podemos ver en las entidades bancarias quienes poco a poco han ido cambiado por completo sus procesos. Muchas de las actividades que antes lo clientes lo realizaban de manera personal, acercándose a una entidad bancaria, hoy en día lo pueden hacer a través de una computadora realizando pago de servicios, abrir una cuenta de ahorros, solicitar un crédito, etc.

Sin embargo, este gran avance ha dado paso a que nuestro país también forme parte de los países que vienen luchando sin tregua contra los delitos informáticos. En el año 2014 Según estudio hecho por la consultora Rusa Kaspersky Lab especialista en Ciber seguridad, Perú fue el segundo país en Latino América que más recibió ataques del cibercrimen en el primer semestre de ese año, con un 39.8% de usuarios afectados por amenazas locales, detrás de Brasil que contó con un 43% de afectados por este flagelo, con 32 millones de ataques efectuados. En esa misma línea, el reporte "ESET Security Report Latinoamérica 2017" lanzado por la compañía de seguridad informática ESET en el 2017 indicó que el Perú es el segundo país con más incidentes de Pishing entre los países de toda la región.

1.- Ecuador: 20.9 %

2.- Perú: 16.6 %

3.- México: 16. 1 %

Figura 7: Principales países afectados por el ciberdelito según Consecuencias de delitos informáticos ESET Security Report Latinoamérica 2017.

Así también para el 2016 Kaspersky realizó un informe sobre los países más afectados por el "Malware" el cual arrojó otra cifra preocupante para nuestro país. Este nuevamente ocupaba el segundo lugar con un 41.9%.

Intentos de ataque por usuarios conectados

País	Porcentaje
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

Figura 8: Intentos de ataque por usuario conectado según informe realizado por la consultora Rusa Kaspersky Lab 2016.

Por otro lado, en ese mismo año, la firma estadounidense especialista en detención de amenazas digitales Rapid7 Labs lanzó de forma pública un informe National Exposure Index (Índice de Exposición Nacional) el cual mide la exposición de datos sensibles en Internet frente a ataques informáticos maliciosos y de eventos hostiles. Según este informe el Perú se encuentra en el puesto 29 en nivel de exposición a nivel mundial y en comparación con toda la región de América Latina, este, ocuparía el segundo lugar, solo después de El Salvador.

En el año 2015 el mismo grado de vulnerabilidad para nuestro país, ya había sido identificado por la compañía americana especializada llamada Fire Eye en su reporte Regional Advanced Threat Repot Fire Eye-2015 en el cual indicaba que el Perú se encontraba dentro de los 5 países con mayor exposición dentro de la región ocupando el cuarto lugar. Esto indica que, del 2015 al 2016 el Perú pasó del cuarto lugar al segundo lugar de exposición en tan solo un año.

1. Brasil
2. Chile
3. México
4. **Perú**
5. Argentina

En ese mismo reporte, la firma Fire Eye también realiza una acotación importante acerca del Perú; si bien es cierto, este, ocupaba el cuarto lugar en nivel de exposición o vulnerabilidad; estos, también, mencionan que nuestro país ocupaba el segundo lugar entre los países con más vulnerabilidad y con riesgo de que los ataques recibidos sean exitosos.

	Más amenazados	**Más amenazados con ataques exitosos**
1	Brasil	Brasil
2	Chile	**Perú**
3	México	México
4	**Perú**	Chile
5	Argentina	Argentina

Figura 9: Ciberataques exitosos – Vulnerabilidad en Perú según reporte Regional Advanced Threat Repot Fire Eye-2015.

Como podemos observar, a pesar de que Chile tiene el segundo lugar como el país más vulnerable del grupo, el informe indica que los ciber ataques que reciben no son efectivos debido a que Chile si posee efectivas políticas de Ciberserguridad mientras que Perú todavía posee deficiencias en este aspecto siendo considerado uno de los países con más alto ratio de ataques exitosos luego de Brasil. Esto se ve reflejado en el llamado que hizo la OEA (Organización de Estados Americanos) en al año 2015 indicando que América Latina debería preocuparse más por la Ciber Seguridad Industrial debido a que la mayoría de los países analizados no habían destinado suficiente presupuesto para la ciber seguridad. Esta afirmación lo hizo luego de haber realizado un estudio previo llamado "Ciberseguridad y la Protección de la Infraestructura Crítica de las Américas" en coordinación con la compañía especializada en seguridad digital Trend Micro.

Figura 10: Países cuyos presupuestos para la ciberseguridad aumentó en el último año, según el reporte Ciberseguridad y la Protección de la Infraestructura Crítica de las Américas 2015 realizado por la OEA en coordinación con la compañía especializada en seguridad digital Trend Micro.

En este mismo informe realizado por la OEA también se reveló que el Perú tiene considerables deficiencias a nivel país respecto a la Ciber Seguridad. Ellos consideraron lo siguiente:

1. Ausencia de una estrategia y una cadena de mando clara que impide el fortalecimiento de la seguridad cibernética del país.
2. Las fuerzas armadas tienen un nivel básico de capacidad de defensa cibernética.
3. No existe una política de defensa cibernética.
4. Limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado. (DIVINDAT)
5. En operadores de infraestructura, las Tecnologías de seguridad y la Infraestructura Crítica Nacional (ICN) son gestionadas de manera informal.
6. Conciencia social de seguridad cibernética es generalmente baja. No hay una amplia campaña de sensibilización que esté actualmente vigente.

Como podemos observar, la situación para nuestro país no es alentadora más aún cuando las pérdidas económicas que genera este fenómeno son realmente alarmantes; según una publicación realizada por el diario Gestión en agosto del 2017 el Perú registraría pérdidas hasta por US$ 4782 millones de dólares a causa de los ciberdelito en ese mismo año. El crecimiento continuo de ataques es de gran preocupación; sin embargo, las autoridades y el gobierno no tienen, todavía, un real interés y conocimiento profundo de este problema, a eso debemos sumarle la falta de conciencia social que hace que nuestro país sea un país potencialmente expuesto y vulnerable a estos ataques.

1.3 El ciberdelito o delito Informático y su impacto en el sistema financiero Peruano

1.3.1 Estructura del sistema financiero en el Perú

Según el portal de la SBS - Superintendencia de Banca y Seguros el sistema financiero en el Perú está conformado por 54 empresas (Incluidas entidades bancarias financieras y demás empresas e instituciones, debidamente reguladas por la SBS) que realizan operaciones múltiples y que poseen activos por 404 millones de soles. Estas empresas son encargadas de realizar el flujo monetario y tienen como principal función canalizar el dinero de los que desean ahorrar hacia los inversionistas. Las entidades que cumplen con esta función se llaman intermediarios financieros o mercados financieros.

1.3.2 Instituciones que conforman el sistema financiero.

- Bancos.
- Financieras.
- Compañía se Seguros.
- AFP.
- Banco de la Nación.
- COFIDE.
- Bolsa de Valores.
- Bancos de Inversiones.
- Sociedad Nacional de Agentes de Bolsa

1.3.3 Entes reguladores y de control del Sistema Financiero.

1.3.3.1 Banco Central de Reserva del Perú

La actual constitución política del Perú establece como finalidad única del BCRP la de preservar la estabilidad monetaria y para ello cumple cuatro funciones principales

1. Propiciar que las tasas de interés de las operaciones del sistema financiero, sean determinadas por la libre competencia, regulando el mercado.
2. La regulación de la oferta monetaria
3. La administración de las reservas internacionales (RIN)
4. La emisión de billetes y monedas.

La creación de esta institución que inició sus actividades en abril de 1922 respondió a la necesidad de contar con un sistema monetario que no provocara inflación ni deflación como la generada por la inflexibilidad crediticia del patrón de oro de aquellos años.

1.3.3.2 Superintendencia de Banca y Seguro (SBS)

La SBS es el Organismo encargado del control, regulación y supervisión del sistema financiero nacional; controla en representación del estado a las empresas bancarias, financieras, de seguros y del sistema privado de pensiones.

La Superintendencia de Banca y Seguros es un órgano autónomo, reconocida por la constitución política del Perú cuyo objetivo principal es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SSP.

1.3.3.3 Superintendencia de Mercado de Valores (SMV)

Institución Pública del sector Economía y Finanzas, cuya finalidad es promover el mercado de valores, velar por el adecuado manejo de las empresas y normar la contabilidad de las mismas. Tiene personería jurídica de derecho público y goza de autonomía funcional administrativa y económica.

1.3.3.4 Superintendencia de Administración de Fondos de Pensiones (SAFP).

Al igual que la SBS, es el organismo de Control del Sistema Nacional de AFP.

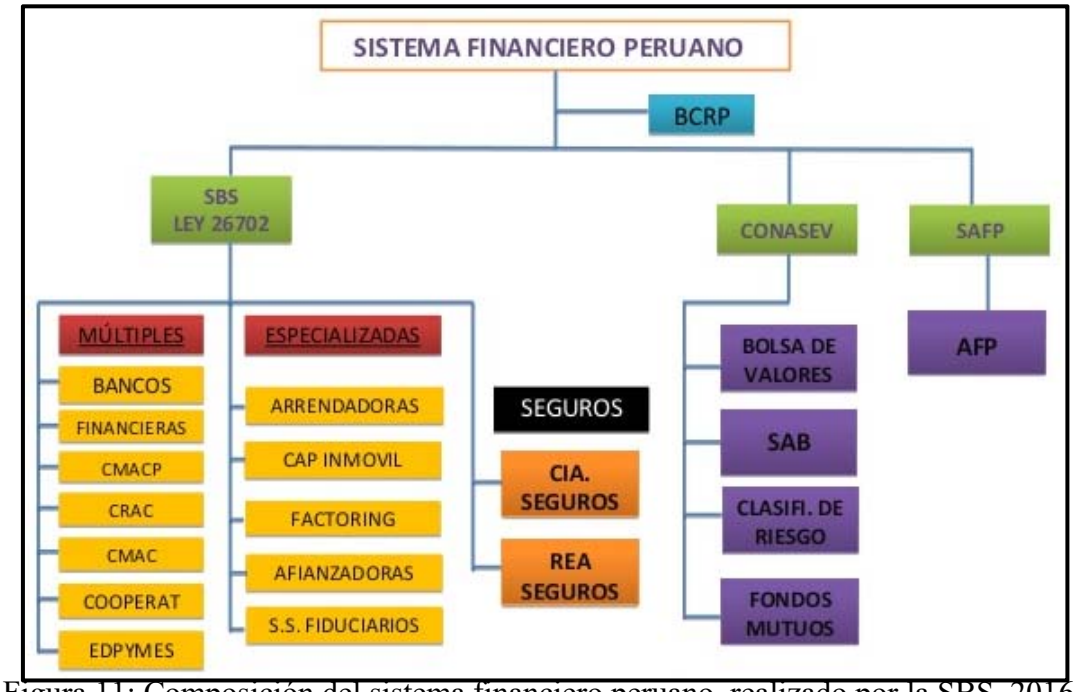

Figura 11: Composición del sistema financiero peruano, realizado por la SBS, 2016

1.3.4 Sistema Financiero Bancario

Este sistema está constituido por el conjunto de instituciones bancarias del país. En la actualidad el sistema financiero Bancario está integrado por el Banco Central de Reserva, el Banco de la Nación y la Banca Comercial y de Ahorros. A continuación, examinaremos cada una de éstas instituciones.

1.3.4.1 Banco Central de Reserva del Perú (BCRP)

Como ya se mencionó anteriormente, el BCR es la autoridad monetaria encargada de emitir la moneda nacional, administrar las reservas internacionales del país y regular las operaciones del sistema financiero nacional.

1.3.4.2 Banco de la Nación

De acuerdo al portal del Banco de la Nación, este es una empresa de derecho público, integrante del Sector Economía y Finanzas, que opera con autonomía económica, financiera y administrativa. El Banco se rige por su Estatuto, por la Ley de la Actividad Empresarial del Estado y, supletoriamente, por la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros. Tiene como misión prestar servicios a entidades estatales y público en general, entre sus principales funciones tenemos.

1. Brindar servicios bancarios para el Sistema Nacional de Tesorería, de acuerdo con las instrucciones que dicta la Dirección Nacional del Tesoro Público. En concordancia con lo establecido en el primer párrafo del presente numeral, dichos servicios serán ofrecidos en competencia con las demás empresas y entidades del sistema financiero.
2. Brindar servicios de recaudación, por encargo del acreedor tributario, debiendo existir aprobación del Banco y un convenio específico de recaudación.
3. Efectuar por delegación las operaciones propias de las subcuentas bancarias del Tesoro Público.

1.3.4.3 Banca Comercial

Instituciones financieras cuyo negocio principal consiste en recibir dinero del público en depósito o bajo cualquier otra modalidad contractual, y en utilizar ese dinero, su propio capital y el que obtenga de otras cuentas de financiación en conceder créditos en las diversas modalidades, o a aplicarlos a operaciones sujetas a riesgos de mercado.

Indicadores de gestión Bancaria

Los indicadores de gestión bancaria tiene como principal propósito el de medir en forma transparente y uniforme el ratio de eficiencia de las entidades bancarias. En el Perú, se toman en cuenta las siguientes:

Captaciones.

Hacen referencia a la cantidad de dinero que tienen las personas, tanto naturales como jurídicas, como depósitos/ahorros en la institución financiera. Los bancos trabajan de manera constante buscando siempre atraer estos recursos con la menor tasa posible y que impliquen plazos de devolución lo más amplios posibles. La cantidad de depósitos captados estará en función de la confianza y del rendimiento que prometan a sus depositantes.

Patrimonio y apalancamiento

Definido como el conjunto de aportes de los inversionistas/propietarios y las ganancias retenidas propias de la misma empresa

Índice de morosidad

Este hace referencia al ratio obtenido de la cartera de crédito vencida o en cobranza judicial, es decir, en calidad de incumplimiento, sobre el total de la cartera que mantiene la entidad financiera. Es uno de los indicadores más utilizados como medida de riesgo de una cartera de crédito. El índice de morosidad resulta importante no solo para la empresa o entidad financiera, puesto que esta información también permitirá al regulador financiero, según cuál sea la situación del sistema, implementar políticas para mantener o mejorar la calidad de las carteras de colocaciones.

A través del análisis de los indicadores mencionados líneas arriba determinamos el porcentaje de la participación que tiene cada banco sobre el mercado financiero peruano. En esta oportunidad estamos tomando el índice de captaciones en tarjetas de crédito debido a que es el producto en donde se presentación los mayores fraudes cibernéticos.

Como podemos apreciar en el siguiente cuadro elaborado por la SBS en el mes de noviembre del 2017, vemos la participación que tienen las entidades bancarias en el mercado.

Tomamos la participación de mercado por el lado de productos activos porque es donde más incidentes de fraudes se presentan como lo podremos ver más adelante.

Tabla 1.Participación de Mercado: Total Créditos (miles de soles)

Empresas	Cuentas Corrientes	Tarjetas de Crédito	Descuentos [1/]	*Préstamos*	Hipotecarios para Vivienda	Otros [3/]	**Total Créditos (En miles de nuevos soles)**
B. de Crédito del Perú (sucursales en el exterior)	0.33	9.42	2.27	53.44	16.09	4.80	**79,445,574**
B. Continental	0.38	4.81	2.20	44.69	23.04	24.87	**51,189,114**
Scotiabank Perú	0.97	6.16	1.12	55.98	15.16	20.62	**40,938,408**
Interbank (sucursales en el exterior)	0.18	15.03	1.61	48.29	20.65	14.24	**27,579,853**
B. Interamericano de Finanzas	0.16	3.63	3.23	40.13	17.25	35.60	**9,312,867**
Mibanco	-	-	-	95.04	4.96	- 0.00	**9,155,161**
B. Financiero	0.57	5.50	1.82	58.54	15.71	17.85	**6,370,551**
B. GNB	0.02	1.67	0.88	49.59	30.75	17.09	**3,893,670**
B. Falabella Perú	-	96.37	-	3.50	0.12	- 0.00	**3,419,977**
B. Santander Pe	0.20	-	21.08	43.62	-	35.11	**2,786,429**
Citibank	3.39	0.28	0.53	50.41	-	45.39	**1,804,010**
B. Ripley	-	47.24	-	52.76	-	0.00	**1,781,168**
B. de Comercio	0.02	0.16	0.23	91.45	2.42	5.73	**1,398,554**
B. Cencosud	-	100.00	-	-	-	-	**549,259**
B. Azteca Perú	-	17.20	-	82.80	-	- 0.00	**377,736**
B. ICBC	-	-	-	94.38	-	5.62	**209,374**
TOTAL BANCA MÚLTIPLE	**0.43**	**9.21**	**2.03**	**51.89**	**16.97**	**2.30**	**240,211,705**

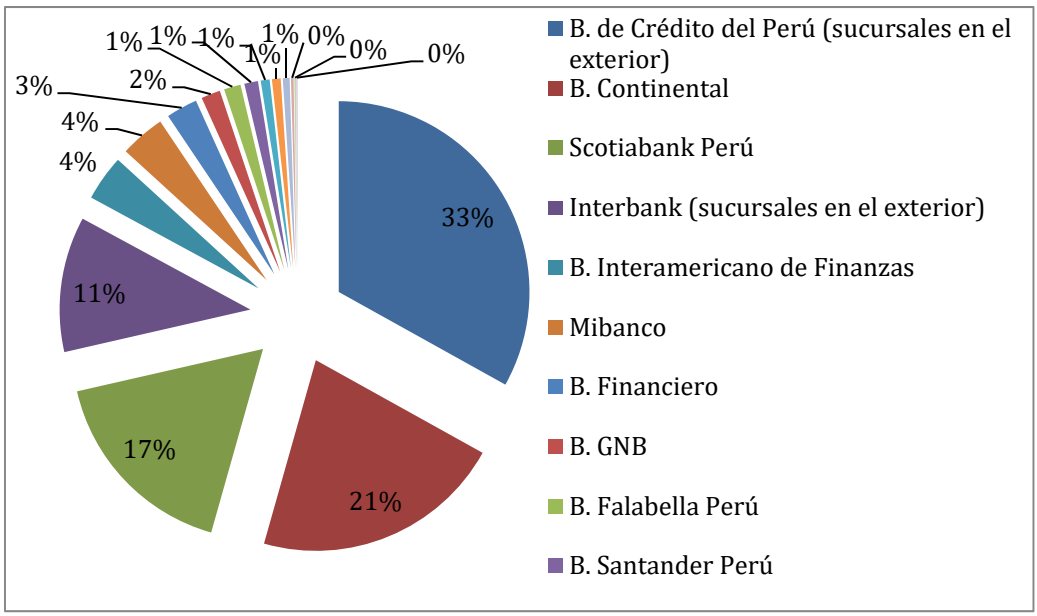

Figura 12: Participación de Mercado, elaborado en el Boletín Mensual de noviembre 2017, SBS.

A continuación, escribimos los dos principales bancos que son objeto de análisis para la presente investigación:

1 Banco de crédito del Perú

Según su portal de internet el Banco de Crédito del Perú llamado durante sus primeros 52 años Banco Italiano, inició sus actividades el 9 de abril de 1889. El 1 de febrero de 1942 se acordó sustituir la antigua denominación social por la de Banco de Crédito del Perú.

Durante los 90, la oficina de representación en Santiago de Chile desarrolló una interesante actividad, dado el notable incremento de los capitales chilenos invertidos en empresas peruanas. Al cumplir 125 años en el mercado local, esta institución cuenta con 375 agencias, más de 1.800 cajeros automáticos, más de 5.600 agentes BCP y más de 15.000 colaboradores, así como bancos corresponsales en todo el mundo. El Banco de Crédito del Perú es el principal activo del grupo financiero Credicorp, al que contribuye con el 79,70% de las utilidades generadas durante el ejercicio 2014 por el mencionado holding.

2. Banco Continental

De acuerdo a su portal el BVA Continental se origina en 1951 como un banco privado, y se ha mantenido como tal hasta el año 1970 cuando fue adquirido por el Estado peruano. Posteriormente, en 1995 se llevó a cabo la privatización del banco bajo la modalidad de subasta, en la que resultaron ganadores el Holding Continental S.A., propiedad del grupo español Banco Bilbao Vizcaya (BBV) y Breca (en ese entonces Grupo Brescia), de origen peruano. En julio de 1998, el Estado transfirió el remanente de sus acciones (19,12%) bajo el mecanismo de oferta pública de valores.

En 1999 el BBV y Argentaria anunciaron su fusión, dando inicio al Banco Bilbao Vizcaya Argentaria–BBVA, que constituyó uno de los grupos financieros más importantes a nivel internacional: alcanzó un mayor tamaño y solvencia, bajo la adecuada diversificación geográfica de riesgos y, consecuentemente, un mayor potencial de beneficios. El grupo económico al que pertenece es el Holding Continental S.A. y junto con sus subsidiarias conforman el conglomerado mixto Banco Continental

1.4 El problema del incremento de la criminalidad en el Peru en los últimos años

En los últimos años nuestro país viene enfrentando una creciente ola de criminalidad que día a día nos golpea con mayor frecuencia. Esto se ve reflejado en diversos informes y estudios los cuales nos indican que hoy en día, la principal preocupación de los peruanos es el problema de la inseguridad ciudadana. Esto lo afirmó el gerente general de CPI (Compañía peruana de estudios de mercado y opinión pública) en el año 2017 a través de una entrevista realizada a la cadena de radio RPP (Radio Programas del Perú), según la encuesta Nacional urbana rural que realizaron en enero del 2017 existe un 51. 3 % de peruanos que indican que el principal problema del Perú, en la actualidad, es la delincuencia y la inseguridad ciudadana, esto también lo afirmó el observatorio ciudadano Lima Cómo Vamos en su reporte anual 2016, este informe reportó que la delincuencia e inseguridad ciudadana han sido consideradas como el principal problema que afecta la calidad de vida en Lima y Callao; en cuanto al aspecto de seguridad ciudadana un 61.3 % señaló que se siente inseguro en la ciudad.

Esta creciente ola de criminalidad también ha dado paso entre, otros actos delictivos, al incremento de delitos no comunes como son los delitos de estafas, fraudes, suplantaciones realizados de forma virtual, a través de un ordenador. Hoy en día es más común encontrar falsos correos o páginas con concursos o premios muy interesantes que tienen como objetivo principal el robo de datos personales, claves de tarjetas y finalmente nuestro dinero de manera digital.

Es así que en junio del 2017 el Jefe de la DIVINDAT (División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú) a través de una entrevista al diario Gestión manifestó que manifestaron que en el Perú, a diario, existen por lo menos 4 personas que son afectados por algún ataque cibernético; esto quiere decir que reciben aproximadamente 120 casos al mes y que un 50 % de esos casos son fraudes electrónicos; 20% vinculados a pornografía infantil; y 10% suplantación de identidad.

Esta afirmación lo vemos reflejado en el reporte “Ciberterrorismo” realizado por la dirección ejecutiva contra el terrorismo de la policía nacional del Perú 2016.

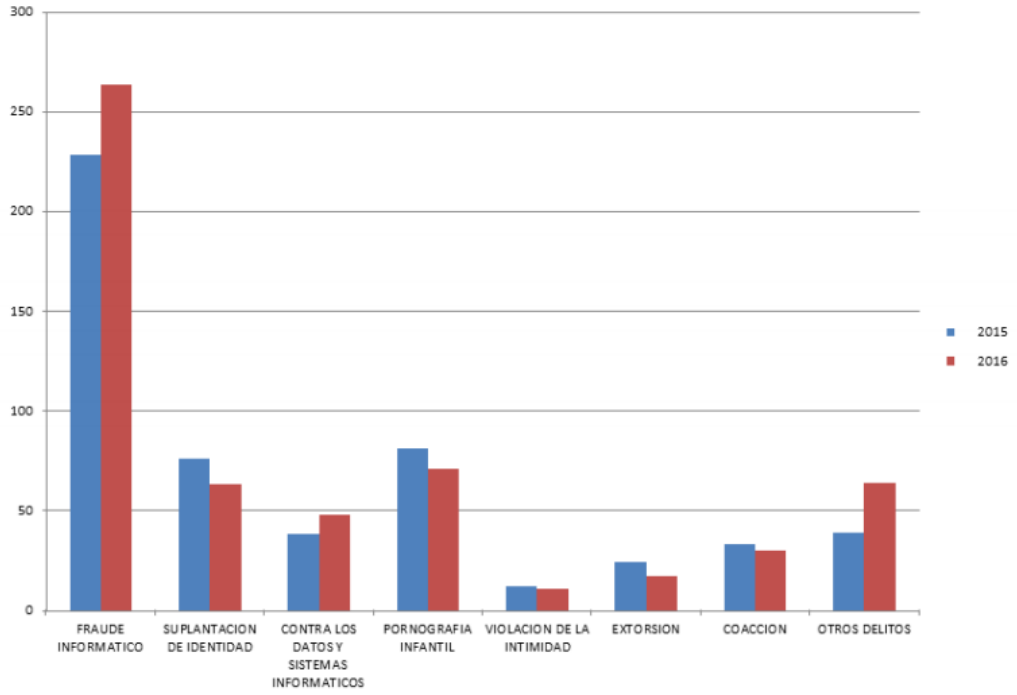

Figura 12: Comparación del crecimiento del fraude informático 2015 -2016 realizado por la división de investigación de delitos de alta tecnología de la Divincri – 2016.

DELITOS INFORMATICOS	2014	2015	2016
FRAUDE INFORMATICO	320	470	263
SUPLANTACION DE IDENTIDAD	214	133	63
CONTRA LOS DATOS Y SISTEMAS INFORMATICOS	57	64	48
PORNOGRAFIA INFANTIL	94	133	71
VIOLACION DE LA INTIMIDAD	46	22	11
EXTORSION	63	50	17
COACCION	42	63	30
OTROS DELITOS	46	69	64
TOTAL	882	1004	567

Figura 13: Incidencia delictiva sobre delitos informáticos 2014 -2016 realizado por la división de investigación de delitos de alta tecnología de la Divincri – 2016

Otra información valiosa es la que nos proporciona el INEI- (Instituto Nacional de Estadística Informática del Perú) en su informe técnico sobre seguridad Ciudadana Enero 2018. Indican a la estafa como el segundo hecho delictivo más común durante el 2017.

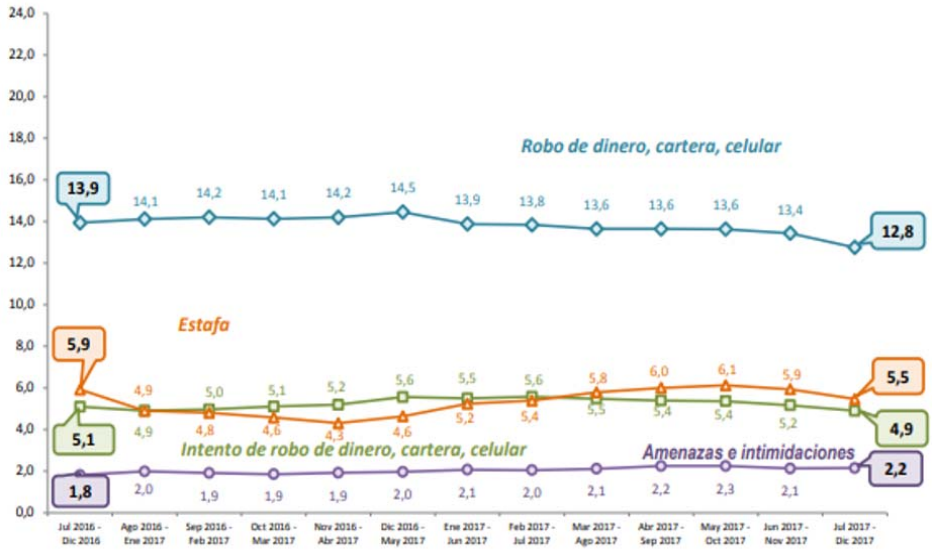

Figura 14: Informe Estadístico de seguridad ciudadana. Elaborado por el Instituto Nacional de Estadística e Informática, diciembre 2017.

1.4.1 Los delitos informáticos y las entidades bancarias de Lima Metropolitana

En el año 2014 un estudio realizado por la consultora Deloitte "Seguridad de los Bancos en Latinoamérica" reveló que el Perú ocupa el segundo lugar en la región con mayor cantidad de bancos tacados por los ciber crímenes. 67% de los bancos del Perú fueron blancos de estos ataques, siendo los propios empleados quienes cometen estos actos. Esta tasa fue la segunda de Latinoamérica, solo detrás de Colombia.

Desde esa fecha hasta el día de hoy, los ataques a las entidades financieras no han cesado, más bien se ha incrementado de manera considerable. Según el Banco de crédito del Perú, 1 de cada 100.000 transacciones que se realizan en esa entidad es un fraude, además al menos 700 personas al mes son víctimas de algún tipo de fraude bancario. De acuerdo al reporte anual del ASBANC 2016, en ese año se registró una mayor cantidad de uso fraudulento de tarjetas de crédito 12% más en relación al año anterior.

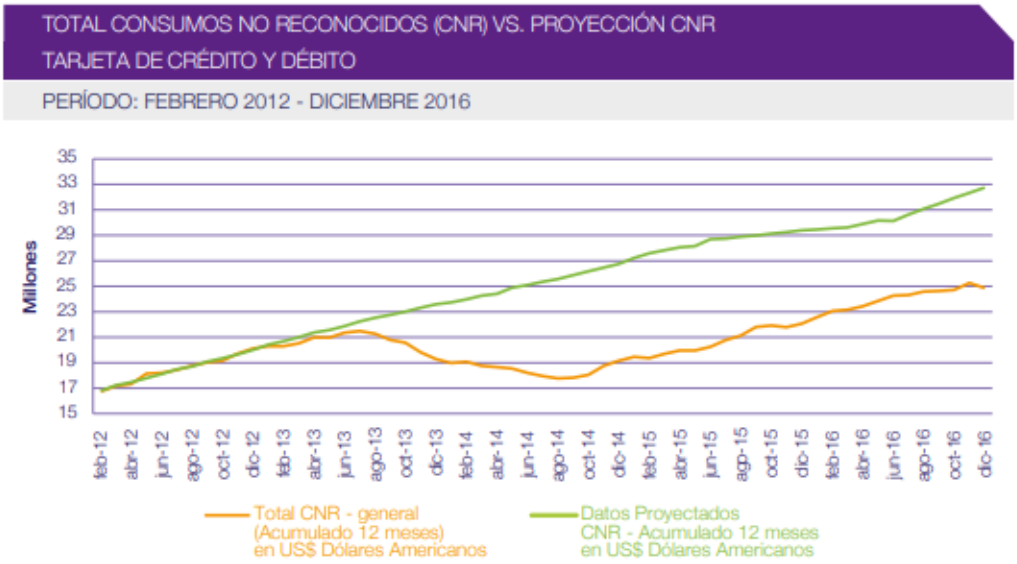

Figura 15: Consumos no reconocidos de tarjetas de crédito. Informe Anual 2016 elaborado por ASBANC.

En ese mismo reporte, se reveló que los fraudes por clonación de tarjetas de crédito a través de los cajeros se han incrementado, así también el robo de información de tarjetas de crédito y débito, sin embargo, ahora están migrando hacia otra modalidad como es la usurpación de identidad para obtener préstamos.

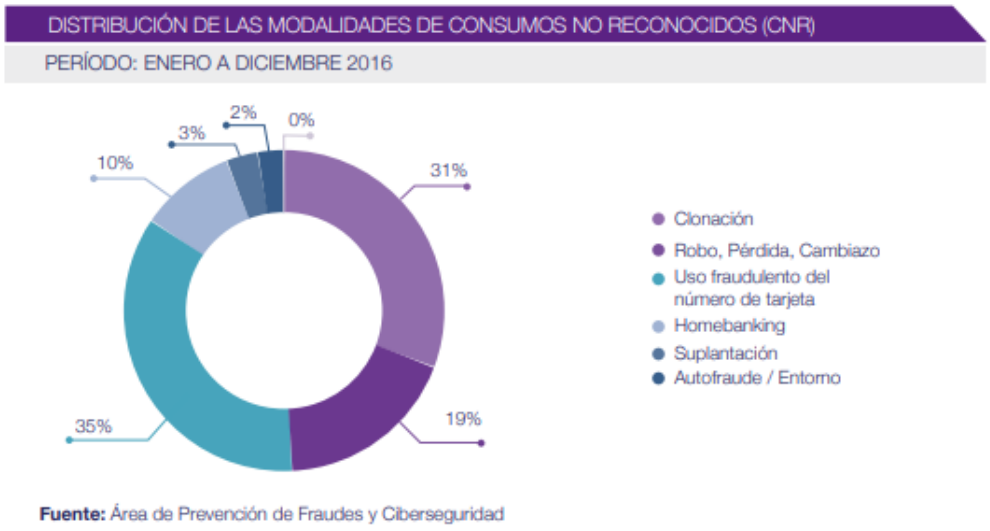

Figura 16: Modalidades Consumos No Reconocidos, Informe Anual 2016 elaborado por ASBANC.

Las pérdidas que se generan en este tipo de delitos son por montos considerables, donde se ven afectados tanto los clientes como las entidades bancarias. Según este mismo reporte realizado por el Asbanc, las pérdidas económicas por fraudes financieros en el

Perú superan los 5 millones de dólares anuales y las entidades tienen el reto de evitar y disminuir estos delitos; en ese sentido con la finalidad de contrarrestar este mal y dar mayor seguridad al sistema financiero, la asociación de bancos del Perú ha definido 5 áreas de servicios para los banco como son Instalaciones, Mantenimiento, Control Técnico; Monitoreo de Alarmas y Prevención de Fraudes y Ciberseguridad

1.4.2 Los delitos informáticos más comunes en los Bancos

En una entrevista a José Marangunich, gerente del área de Seguridad integral para los negocios del BCP, realizada por el diario menciona que además del phishing, la modalidad de robo más común es el robo de datos. Esto se da a través de la conexión de los dispositivos a redes Wi-Fi en lugares públicos que muchas veces coincide con señales de internet simuladas por ciberdelincuentes que, al momento de brindar acceso a internet, obtienen datos de los usuarios de las laptos, tables o celulares, como claves, contraseñas o números de tarjetas".

Esta afirmación, coincide con el reporte anual 2016 presentado por el Asbanc el cual indica que enero del 2016 se registraron 988 ataques de Pishing, esta fue similar al año 2015 debido a que se implementaron soluciones tecnológicas preventivas aplicadas por todas las entidades financieras. Todo ello se tradujo en la minimización de pérdidas por el uso de tarjetas de crédito fraudulentas.

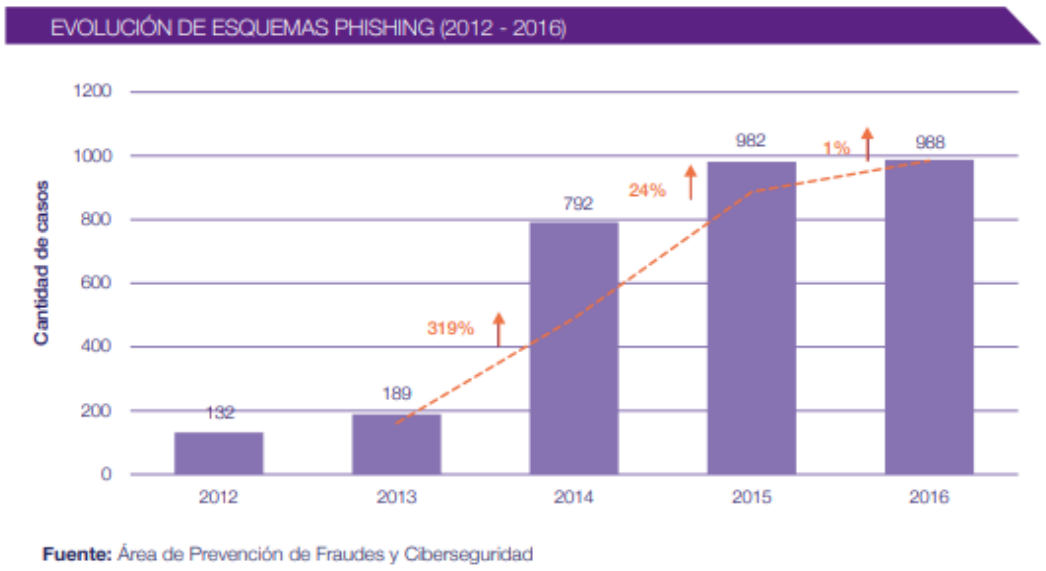

Figura 17: Evolución de Phishing 2012-2016, Informe Anual 2016 elaborado por ASBANC.

Muy contrario al Pishing, el informe no registró ataques por los llamados “Troyanos Bancarios” ya que se considera que a los ciber delincuentes generan más ganancia e inclusive se le hace más fácil crear páginas web fraudulentas que programar un troyano, que puede ser detectado por los antivirus.

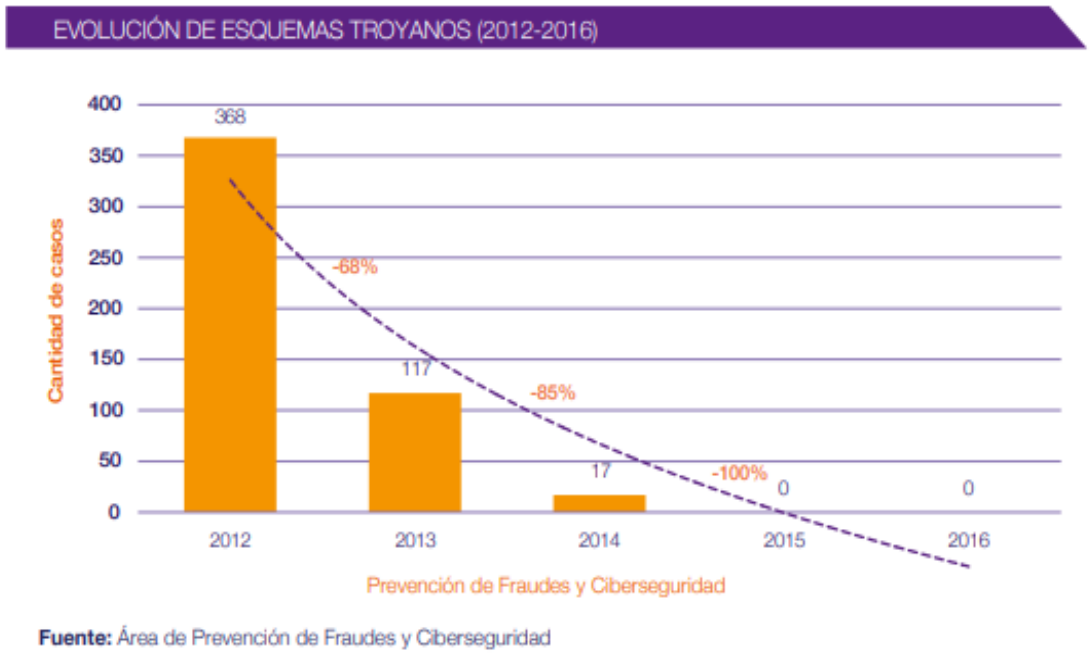

Figura 18: Evolución Esquemas Troyanos 2012 – 2016. Informe Anual 2016 elaborado por ASBANC.

CAPÍTULO II. METODOLOGÍA DE LA INVESTIGACIÓN

2.1. Planteamiento de la investigación

2.1.1 Propósito de la Investigación

El presente trabajo de investigación tiene como propósito, analizar el impacto que vienen teniendo los principales bancos del Perú en los últimos 5 años debido al incremento de los delitos informáticos o ciber delitos. A través de este análisis podremos identificar los principales factores de Operatividad, finanzas, de imagen y reputación que han sido afectadas debido al incremento de estos actos delictivos; esto nos permitirá obtener información actualizada de modo que se obtenga un marco de referencia verídica para el manejo de estas situaciones; así también podamos contribuir de alguna forma con la prevención de este fenómeno, establecer recomendaciones que ayuden a las organizaciones a contrarrestar y minimizar las amenazas que presentan estos actos delictivos.

2.1.2 Tipo de Investigación

El enfoque que utilizaremos para el presente trabajo de investigación es cualitativo, porque nos permitirá analizar y entender los diversos factores que vienen siento impactados en las principales entidades financieras debido al incremento de los delitos informáticos o ciber delitos; esto nos permitirá analizar los procesos operativos, incremento de los gastos en seguridad informática y tecnología y finalmente, imagen reputacional, de modo que nos permita validar la hipótesis planteada en el presente trabajo de investigación.

El estudio de la investigación es descriptiva, pues nos describe cada factor impactado por los delitos informáticos en el sistema financiero peruano, específicamente en el BCP y BBVA, además explicativo debido a que nos explica básicamente de qué manera están siendo afectados el sistema financiero y la forma en la que están siendo afectados hoy en día.

La presente investigación está basada en la teoría fundamentada, cuyo propósito es desarrollar una teoría basada en datos empíricos y que se aplica para áreas específicas, tomando data a través de las entrevistas a profundidad con el fin de analizar la información mediante herramientas preparar y organizar lo obtenido de estas entrevistas.

2.1.3 Preguntas de Investigación

Las preguntas a realizar durante las entrevistas a profundidad son fundamentales para poder responder a la hipótesis planteada, es así que detallamos las 5 principales preguntas de las cuales partiremos para las entrevistas.

En el anexo N° 1 se encuentran a detalle las preguntas de acuerdo a cada segmento entrevistado.

¿Cuáles son las principales variaciones en los procesos operacionales, de los principales bancos de Lima como son el BCP y BBVA debido al incremento de los ciberdelitos.?

¿Cuál es el impacto en la imagen y reputación de las principales entidades financieras de Lima como son el BCP y BBVA debido al incremento de ciberdelitos?

¿Cuáles son las variaciones en el incremento de presupuesto de gastos relacionados a tecnología de la información en el sistema financiero de los principales bancos de Lima como son el BCP Y BBVA?

2.2 Contexto

2.2.1 Descripción del contenido interno y externo

En este punto se tendrá la descripción específica y geográfica del ambiente donde se desarrollará cada entrevista, esta descripción se basa en el método de la observación, es así que se analizará el contexto interno y externo antes, durante y después de la entrevista.

A continuación, presentación la bitácora donde se visualizará el contexto del desarrollo de nuestra investigación de campo hacia los diferentes entrevistados de las dos entidades financieras:

2.3 Muestra

2.3.1 Descripción de la muestra

Para la presente investigación se ha contemplado tomar una muestra correspondiente a nuestro tipo de investigación, se ha decido entrevistar a veintitrés (23) personas, ya que con dicho número de entrevistas esperamos obtener las respuestas a nuestra pregunta de investigación, es así que detallamos cada unidad a entrevistar en el siguiente cuadro:

Unidades a entrevistar	**N° de entrevistas**
Gerente de Seguridad de la Información	1
Sub Gerente de Control de la Operativa y Negocio – Engeniering	1
Subgerente Adjunto de Monitoreo Transaccional	1
Subgerente Adjunto de Prevención del Fraude	2
Analista de Reclamos	5
Proveedor de Sistema de Seguridad	1
Clientes	13
Total	23

2.4 Diseño o abordaje principal

2.4.1 Identificación de la estructura de la entrevista

En el trabajo se utilizaremos la técnica de la entrevista a profundidad teniendo como base una guía de preguntas semi-estructuradas, ya que nos da la opción de ir realizando las preguntas necesarias de acuerdo a la respuesta brindada o en todo caso llevar a otro contexto la entrevista. Así mismo, nos permite profundizar y ahondar más en los temas relevantes que vayamos tocando durante la entrevista.

2.4.2 Guía de preguntas

La elaboración de la guía de preguntas tuvo como base los objetivos de esta investigación. La metodología de investigación y preguntas realizadas se detallan en el Anexo N° 1.

2.4.3 Segmentos

Los segmentos elegidos para entrevistar son 7, donde se levantará información a través de las entrevistas semi-estructuradas.

Unidades a entrevistar	**N° de entrevistas**
Gerente de Seguridad de la Información	1
Sub Gerente de Control de la Operativa y Negocio – Engeniering	1
Subgerente Adjunto de Monitoreo Transaccional	1
Subgerente Adjunto de Prevención del Fraude	2
Analista de Reclamos	5
Proveedor de Sistema de Seguridad	1
Clientes	13
Total	**23**

2.4.4 Categorías

Los temas que trataremos con las entrevistas son los siguientes.

1 Procesos Operativos del Sistema Financiero

¿Cuáles son los procesos operativos que se realizan dentro del banco con el fin de evitar delitos informáticos?

¿Cuáles son las medidas de seguridad que se tienen en las operaciones realizadas a través de los canales digitales del banco?

¿Cuáles son las características que evalúa el área de prevención con el fin de identificar eficazmente operaciones realizadas por ciberdelincuentes?

¿Cuál es el tiempo que se tiene para frenar una operación inusual o sospechosa?

De acuerdo a su experiencia como cliente, ¿Cree usted que el banco cuenta con las medidas de seguridad adecuadas en las operaciones realizar en banca por internet, app móvil o cajero?

2 Imagen y Reputación de las entidades financieras BCP y BBVA

¿Cuáles son los factores que más impactan en la imagen y reputación del banco?

¿Cuáles son los rangos o los niveles de criticidad que se manejan ante un reclamo por ciberdelito?

¿Cómo impacta la imagen y reputación del banco que los medios de comunicación expongan casos de fraude digital?

¿Cuál es su opinión al respecto al ver en los medios de comunicación denuncias de personas, clientes como usted que han sido víctimas de fraude y delitos cibernéticos?

¿Ha sido víctima del ciberdelito en los últimos años?

3 Presupuesto de Gastos en relación a la seguridad de tecnología de la información

¿Cómo se ha incrementado a través de los últimos 5 años el presupuesto de gastos en seguridad de la información?

¿Cuentan actualmente con un presupuesto destinado para ciberseguridad?

¿Qué estrategias se vienen desarrollando ante el agresivo desarrollo que tiene la tecnología?

¿Cuáles son las pérdidas que han enfrentado debido a los ciberdelitos a los que han sido víctimas?

2.4.5 El Instrumento de investigación

Los instrumentos utilizados en el proceso de investigación fueron los cuestionarios de preguntas preparadas de acuerdo a nuestros objetivos específicos, además del apoyo en fuentes de información primaria (interna) ya que se realizaron dentro de las instalaciones de las entidades bancarias analizadas; y secundaria, (externa) que se realizó a través de bibliografías e internet.

2.5 Procedimiento (procesamiento de la información)

Para el desarrollo de la investigación del presente trabajo, se realizaron las entrevistas en las diversas oficinas de las entidades bancarias (BCP Y BBVA); además de las oficinas de empresas de seguridad como RSA y otros espacios públicos. Las entrevistas fueron

realizadas por las integrantes del presente trabajo de investigación, en la cual una de ellas era encargada de llevar a cabo la entrevista; mientras que la otra persona tomaba nota de los aportes resaltantes, además del entorno en el cual se llevaba a cabo la entrevista.

Cabe mencionar, que al inicio de cada entrevista se le hacía de conocimiento al entrevistado que los resultados obtenidos de dicha entrevista, solo serían usados para el presente trabajo de investigación, salvaguardando así los principios éticos de confidencialidad, anonimato y reserva de la información proporcionada.

A continuación, presentamos la matriz de procesamiento de la información relevante, obtenida durante las entrevistas a profundidad considerando las categorías y segmentos asignados.

2.5.1 Matriz de procesamiento – Codificación:

	Código	Gerente de Seguridad de Información	Subgerente Control de Operaciones	Monitoreo	Subgerente de Prevención del Fraude	Analista de Reclamos	Proveedor de Seguridad Bancaria	Clientes
Proceso Operativo	POCO			X			X	X
	POMO		X	X			X	
	POPF			X	X	X	X	X
	POAA		X	X	X	X	X	
	POPF			X	X		X	
	POMS	X	X	X	X	X	X	X
Plan de Contingencia	PCVT				X	X	X	
	PCPF			X	X		X	
	PCMS	X	X	X	X	X	X	X
	PCPD		X	X			X	
	PCCD		X	X	X		X	
	PCTA			X		X	X	
	PCCP	X	X	X		X		
Imagen Institucional	IITD			X		X	X	X
	IISC	X	X	X		X	X	
	IIPC	X	X	X	X	X		

CODIFICACION:

1. POCO: proceso operativo confirman operaciones
2. POMO: proceso operativo monitorean operaciones
3. POPF: proceso operativo posible fraude
4. POAA: proceso operativo aumenta anual
5. POPF: proceso operativo prevención del fraude
6. POMS: proceso operativo monto sospechoso
7. PCVT: plan de contingencia verificación token
8. PCPF: plan de contingencia prevención del fraude
9. PCMS: plan de contingencia monto sospechoso
10. PCPD: plan de contingencia proceso diferente
11. PCCD: plan de contingencia captación y devolución
12. PCTA: plan de contingencia tiempo de atención
13. PCCP: plan de contingencia captar portafolio
14. IITD: imagen institucional tiempo de respuesta
15. IISC: imagen institucional sentimiento del cliente
16. IIPC: imagen institucional percepción del cliente

CAPÍTULO III. ANÁLISIS DE DATOS Y RESULTADOS

Este capítulo tiene como finalidad analizare interpretar a profundidad la información obtenida durante las entrevistas a profundidad realizadas en las entidades financieras (BCP y BBVA), así como también a sus clientes externos e internos. Todo esto con la finalidad de responder a las preguntas de investigación planteadas y a su vez realizar la validación de la hipótesis del presente trabajo de investigación.

Se han tomado en cuenta todas las preguntas relacionadas a los procesos operacionales de prevención de fraudes desde diferentes perspectivas (Clientes, Proveedores, personal del Banco) como estos procesos han ido cambiando con el tiempo debido al crecimiento de los delitos informáticos.

3.1. ¿Cuáles son las principales variaciones en los procesos operacionales, de los principales bancos de Lima como son el BCP y BBVA debido al incremento de los ciberdelitos?

De acuerdo a las entrevistas desarrolladas a profundidad, los procesos operacionales relacionados con la prevención de fraudes que actualmente se desarrollan en los bancos, tanto en el BCP como el BBVA, se han ido optimizando y cambiando con el tiempo de modo que puedan cumplir con la prevención, detección y monitorización de transacciones y actividades sospechosas en todos los niveles. En los últimos años se han incrementado la implementación de normas y procedimientos que ha traído consigo la generación de toda una cultura de alerta constante entre los colaboradores de ambos bancos, por ejemplo, se ha implementado un sistema el cual valida que el cliente que ha ingresado a banca de internet se haya conectado desde dominio que ya ha sido reconocido en anteriores ocasiones; en caso de ser un dominio totalmente nuevo y sospechoso, la operación se bloquea inmediatamente; por otro lado, un ejemplo claro es la implementación de un dispositivo de seguridad “Token” para realizar transacciones a través de internet. Este cuenta con una clave dinámica, seudónimo, clave de seguridad y pre matrícula de cuentas de modo que puedan garantizar el una transacción rápida y

segura hacia sus clientes. (En los últimos años, inclusive, se ha añadido la impresión de las huellas digitales como código adicional de autenticación).

> (…) Ha habido meses que la banca nacional ha reportado hasta 16 millones de transacciones bancarias a través del celular y 50% de ellas corresponden a nuestro banco. Esto ha significado una reinvención de nuestros procesos internos, Por ejemplo, una de los procesos que se tuvo que implementar cuando adquirimos el nuevo sistema de seguridad TOKEN, fue integración y creación de nuevos canales internos los cuales se encargarían de brindan orientación al usuario a través de diversos medios acerca de cómo usar el dispositivo, así también cómo promocionarlo. **(Subgerente Adjunto de Prevención del Fraude BCP)**

> (…) Nosotros como banco moderno, estamos en constante innovación en todos los niveles de la banca. En este caso, año tras año nos preocupamos por brindar mayor seguridad para nuestros clientes debido a que los fraudes bancarios van en incremento. **(Subgerente Adjunto de Prevención del Fraude BBVA)**

En otros casos, se ha adicionado un procedimiento más a un proceso ya establecido; por ejemplo, en el área de monitoreo transaccional del BCP, ahora se recibe mes a mes una relación de tarjetas las cuales después de haber sido analizadas probablemente han sido expuestas a algún tipo de fraude; luego de ser evaluadas y analizadas con el mismo cliente, se puede proceder con la anulación de la tarjeta para evitar futuros ataques.

> **(…)** Anteriormente el proceso de recepción, evaluación y cierre de un reclamo por fraude podría durar hasta 30 días. En ese lapso de tiempo se determinaba la devolución o no del dinero; sin embargo, ahora, debido al incremento de este tipo de fraudes hemos tenido que adicionar un procedimiento adicional como es devolución inmediata de dinero (dependiendo del monto) y luego proseguir con todo el proceso antes mencionado de manera regular. Esto con la finalidad de ofrecer a nuestros clientes mayor confianza y seguridad**. (Subgerente Adj. De Monitoreo Transaccional BCP)**

Respecto a lo indicado anteriormente, acerca de la implementación de una cultura de alerta se puede observar que el reparto de circulares con procedimientos a seguir en determinadas situaciones (como por ejemplo "Qué procedimientos seguir en caso de recibir una alerta por un tipo de fraude de grandes magnitudes") y hasta encuestas han sido de vital ayuda con el fin de concientizar a todos los trabajadores respecto a la importancia con la cual se tiene que abordar el tema de los fraudes y delitos informáticos en su institución. En el caso de las encuestas, en el BBVA trimestralmente se realiza la "Encuesta de Exposición de riesgos informáticos" a todos los empleados del banco de

modo que les permita medir la percepción que ellos tienen respecto a la exposición a este tipo de delitos informáticos.

> (…) Los delitos digitales están creciendo día a día y nosotros estamos consciente de ello, es por ellos que vamos creando y adquiriendo nuevos mecanismos de defensa como por ejemplo la implementación de nuevos procedimientos que ayudan prevenir este tipo de actos delictivos. Un ejemplo específico es la repartición de cartillas a nuestros empleados en los cuales indica las estrategias antifraudes que vamos a implementar durante el año. **(Segmento 04: Subgerente de Prevención del Fraude BBVA)**

> (…) Nosotros como banco moderno, estamos en constante innovación en todos los niveles de la banca. En este caso, año tras año nos preocupamos por brindar mayor seguridad para nuestros clientes debido a que los fraudes bancarios van en incremento. **(Subgerente Adjunto de Prevención del Fraude BBVA)**

Siguiendo esta línea, la percepción en cuanto a la transformación de procesos operacionales también viene tanto de parte de los proveedores de sistemas de seguridad, así como de los mismos clientes ya que de algún u otro modo han sentido el cambio y sobre todo la molestia por parte de los clientes.

> (…) Es obvio que los procesos operacionales han sido modificados y hasta a veces se ha creado nuevos procesos debido al incremento de los delitos informáticos; cada vez que nosotros como proveedores de seguridad implementamos un nuevo sistema de seguridad hay que capacitar personas, modificar, crear nuevos procedimientos y hasta implementar nuevos ambientes lo que implica también costos y gastos. **(Segmento 6: Proveedor de sistemas de seguridad).**

> (…) Me incomoda un poco de que hoy en día me pidan tantas cosas para realizar una transacción a través de internet, antes era mucho más fácil, ahora hasta me piden poner mi huella digital, pero también entiendo que es por mi propia seguridad. (**Cliente: Patricia Sagastegui - BEX BCP).**

Por otro lado, también queremos remarcar que la transformación de procesos se debe no solamente la constante innovación y transformación al cual se someten los bancos año tras año, sino también a que se reconoce un incremento significativo de estos actos delictivos. Según hemos podido observar el número de reclamos por día referente a alguna operación no reconocida o algún otro tipo de fraude es de 12 a 20 reclamos por día dependiendo de la temporada (Los reclamos por clonación o fraude se incrementan durante las temporadas de los llamados “CyberDays” o comercio electrónico) suma que

se ha ido incrementando en los últimos años. Esta percepción de incremento ha sido corroborada por los mismos empleados.

> (…) Yo trabajo en el banco desde hace 12 años y hace 7 años como analista de fraudes y antes no se recibían tantos casos clonación de tarjetas o gastos no reconocidos, eran 1 o dos casos por día máximo. **(Analista de fraude BCP)**

> (…) Hace unos 5 años éramos solo 2 analistas de fraude en esta sede; debido a la gran demanda de casos a manejar contrataron a 2 personas más. Ahora los reclamos que más recibimos son por intento de secuestro de datos (Pishing) y clonación de tarjetas. **(Analista de fraude BBVA).**

Otro factor relevante a destacar es que no solamente los bancos perciben el crecimiento de este tipo de ataques si no también son los mismos clientes potenciales quienes corroboran este hecho. Alguno de ellos ha indicado que por ejemplo en los últimos 4 años ha sido víctima, en dos oportunidades, de la clonación de su tarjeta; así también otros

Señalan que el incremento de seguros ofrecidos hacia las tarjetas u otros servicios que poseen hace suponer el evidente crecimiento de este fenómeno. A esto también le sumamos el incremento de las coberturas de las tarjetas que ofrecen los seguros como, por ejemplo.

1. Cobertura por robo y extravío de tarjetas.
2. Cobertura por operaciones no reconocidas vía internet.
3. 3.- Cobertura por robo de identidad o datos.
4. 5.- Protección de retiro en efectivo en ventanilla o Cajero

> (…) En solo 4 años me clonaron la tarjeta dos veces! Y lo peor de todo en el mismo banco, para mí fue la gota que derramó el vaso. Tuve que cambiar de banco; sin embargo, eso no quiere decir que estoy del todo tranquila, porque veo que este tipo de delito crece cada vez más. Yo creo que en ningún banco tenemos seguridad al 100%**. (Cliente: Giannina Rodríguez - Masa BBVA)**

> (…) No sé por qué me ofrecen tantos seguros para mis tarjetas, veo que este tipo de fraudes se están incrementando y creo que es responsabilidad del banco proteger a como dé lugar a sus clientes y no trasladar el problema a nosotros con la venta de seguros… **(Cliente: Diandra Curich BCP).**

> **(…)** No tenemos por qué pagar por eso porque se supone que el banco es un lugar seguro y no tendría por qué pagar por algo adicional, pero al final uno lo paga porque no tenemos otra opción **(Cliente: John Cavalie - Masa BCP)**

Categoría 2 – Imagen y Reputación Institucional

También se ha analizado los diversos puntos de vista, opiniones y percepciones de las personas que están involucradas directa e indirectamente con los bancos, respecto a la imagen y reputación de los mismos.

3.2. ¿Cuál es el impacto en la imagen y reputación de las principales entidades financieras de Lima como son el BCP y BBVA debido al incremento de ciberdelitos?

Sabemos que la imagen y reputación en las organizaciones es fundamental para el crecimiento y desarrollo de las mismas ya que la mayoría de las veces, estas, determinan la elección de clientes potenciales respecto al hecho de elegir una institución financiera o también mantenerse en la misma, creando así un lazo de confianza que si se llega a perder repercutirá directamente en los clientes e inversionistas. Es por ello que tanto para el BCP como para el BBVA la seguridad es crítica; están conscientes de que el nombre del banco es su activo más valioso.

Según lo que indican los diferentes segmentos, estos, tienen conocimiento de la importancia de prevenir y garantizar la seguridad de los clientes es así que continuamente trabajan en cooperación y trabajo continuo con todas las áreas involucradas. Un ejemplo claro de esto es que el área de Imagen institucional ha tenido que reforzar e incrementar las capaciones y charlas sobre todo en el área de atención de reclamos y analistas de fraudes con el nombre de "Capacita-Te" en el caso del BBVA, instruyen a los empleados sobre la importancia de la recepción, entendimiento y tratamiento de un reclamo. Se realizan simulacros y exámenes a fin de garantizar que los empleados puedan reaccionar de forma rápida y efectiva en cuanto estén frente a un reclamo por algún tipo de fraude de modo que los clientes no se sigan llevando una mala impresión de su institución.

> (…) Uhmm… A pesar de que las pérdidas económicas que conllevan estos delitos, muchas veces no son asumidas por el banco, si no por un seguro; sabemos cómo esto afecta la imagen de nuestra institución y por ello estamos en constante alerta, capacitando y adquiriendo nueva tecnología que nos ayude a contrarrestar este fenómeno. **(Segmento 4: Subgerente de Prevención del Fraude BBVA)**

> (…) Estamos conscientes de lo vital que es la reputación para nosotros, la banca se basa en la confianza es por ello que hacemos lo posible para

> recuperar la imagen y la confianza de nuestros clientes que vamos perdiendo debido a este tipo de ataques. **(Segmento 1: Gerente de Seguridad BCP)**
>
> **(…)** Uno de los principales factores que se miden al evaluar la calidad de un banco es la satisfacción de nuestros clientes, porque sabemos que esto impacta directamente en nuestra imagen por ello es que hemos incrementado la frecuencia con de las encuestas de satisfacción al cliente. Necesitamos tener información actualizada respecto cuál es la percepción de ellos hacia nuestro banco. **(Segmento 4: Subgerente Adjunto de Prevención del Fraude BCP)**
>
> (…) Constantemente hacemos campañas de prevención, difusión y contamos con planes de contingencia entre los trabajadores del banco, por ejemplo, respecto a cómo actuar en casos de un ataque de grandes dimensiones; por otro lado, están las campañas de prevención que se hacen en coordinación con el área de Marketing tanto para los clientes como para el personal del banco**. Por ejemplo (Segmento 4: Subgerente de Prevención del Fraude BBVA)**

Según lo que nos indican, estas campañas incluyen la implementación de cursos virtuales a los asociados, carteles y afiches que son pegados en todas las oficinas del banco como ejemplo el programa semestral "Mes de la prevención contra el fraude" en el cual indican las medidas que se van implementar tanto para los empleados, como para los clientes de modo que ese mes puedan reducir los reclamos por este tipo de delitos.

Así mismo, podemos indicar también que el impacto negativo a la imagen y reputación de ambas instituciones es claramente percibido y reconocido por los trabajadores, principalmente los que trabajan en el área de prevención de riesgos o reclamos. Ellos, más que nadie conoce la problemática desde cerca, ya que son los que reciben las quejas de los clientes a través de los distintos canales. Los analistas de fraude consideran que a pesar de que se esfuerzan constantemente luchar contra este mal, consideran que cuando un cliente pasa por un evento como un robo de datos o clonación, tienen la percepción de que el banco es inseguro y no le ofrece las garantías necesarias para su permanencia en esa institución.

> (…) Los fraudes, nos afectan bastante en nuestra imagen como institución bancaria, muchas veces hay reclamos reiterativos y los clientes nos indican que, si no le solucionamos el problema, retirarán todo su dinero y se irán a otro banco. Siempre se quejan de que nos tomamos mucho tiempo en solucionar su reclamo. **(Analista de Fraude BBVA).**

> (…) En casos de operaciones no reconocidas lo que más les afecta a los clientes es el tiempo de devolución de su dinero, ellos sienten que, para el banco, esto no es urgente. (**Analista de Fraude BCP)**

> (…) uhmm. Los reclamos que ingresan, no solo se quedan allí, nos afectan por todos lados, muchas veces nuestros clientes han utilizado las redes sociales para contar la mala experiencia que han tenido con el banco. . (**Analista de Fraude BCP)**

Por otro lado, cabe destacar que, si bien es cierto existe una clara intensión de los bancos y de sus empleados por hacer frente y contrarrestar estos ataques, los clientes y proveedores tienen su propia percepción respecto a la importancia y/o interés que el banco muestra hacia la lucha frontal contra este tipo de delitos ya que consideran que la seguridad que le ofrecen las entidades no es suficiente y además que los tiempos de demora en el tratamiento de un reclamo es demasiado, ya que consideran que cuando ocurren estos hechos el banco es el principal responsable de ello por lo que es el banco quien debe dar una solución inmediata y no esperar hasta 30 días (en algunos casos, para resolver un reclamo)

> (…) A pesar de que sigo con este banco, tengo una mala percepción de este, hace meses tuve un consumo no reconocido realizado en una tienda de EEUU, y a pesar de que les demostré que yo me encontraba en Lima en aquellas fechas, igual se demoraron demasiado en resolver mi caso. **(Cliente Jorge Rodriguez- BEX BCP)**

> (…) A pesar de que, en los últimos años, los bancos van adquiriendo más sistemas de seguridad y protección para salvaguardar a sus clientes, este todavía no es suficiente. Nosotros, como empresa se seguridad, siempre estamos en constante innovación con nuevas tecnologías; sin embargo, es muy difícil lograr la venta de estos nuevos productos porque algunos clientes (como los bancos) no los consideran necesarios; sin embargo, considero que no es así; cada día hay más casos de todo tipo de fraudes y por ende más clientes insatisfechos, dispuestos a moverse a otro banco donde les brinden mayor seguridad. **(Proveedor de seguridad – Empresa RSA)**

> (…) Yo tuve que cambiarme de banco, en dos oportunidades: del primer banco me salí porque era un banco pequeño y no cubría mis necesidades; del segundo banco, que se supone que es un banco grande y de mucho prestigio, tuve que sacar todo mi dinero porque me clonaron la tarjeta en dos oportunidades**. (Cliente Diandra Curich BBVA)**

> (…) Tengo 3 años en el banco y considero que las medidas de seguridad del banco son muy pocas. Cuando me robaron mis datos bancarios, el correo que me llegó era completamente igual al del banco y lo peor de todo

> fue que se demoraron mucho en devolverme el dinero y solucionar el problema. **(Cliente Sheyla Aliaga BBVA)**
>
> (…) A parte del BCP tengo cuentas en otros bancos y la verdad no me siento seguro con ninguno de ellos. Te ofrecen miles de seguros lo cual te hace pensar que ellos mismo no están seguros de lo que ofrecen como banco. **(Cliente Patricia Sagástegui- BCP)**
>
> (…) En los últimos 3 años ya he comprado como 4 seguros…imagínate! Fueron dos veces las que me vaciaron mi tarjeta, pero como tenía el seguro me devolvieron todo mi dinero; aun así, pienso que el banco no se hace responsable ni tampoco toma las medidas necesarias. Al final le tiran el problema al cliente vendiéndole infinidad de seguros. **(Cliente Ángel Luna – Enalta BCP)**
>
> **(**…) La verdad es que no me siento completamente satisfecha con el servicio que me da mi banco actualmente. Pero no me queda de otra porque en comparación con otros bancos, es el mal menor. En el banco anterior en el que estaba clonaron mi tarjeta de crédito e hicieron compras en Ripley por más de 10 mil soles y el banco jamás se hizo cargo del problema porque supuestamente no tenía seguro. (**Cliente Gianninina Rodriguez – Masa BCP)**

Finalmente, tomando como referencia algunas entrevistas realizadas a los gerentes de cada banco, podemos indicar que, de alguna u otra manera, ellos también aceptan las deficiencias y falencias en cuanto a lucha contra los delitos informáticos. Esto se pude corroborar con lo expuesto por el Gerente de Seguridad del BCP.

> (…) Sabemos que todavía nos falta mucho por mejorar y que eso nos está causando impacto principalmente en la perdida de algunos clientes potenciales, sin embargo, día a día estamos haciendo lo posible por mejorar este panorama. **(Sub Gerente de Seguridad - BCP).**
>
> (…) Considero que quizá no encontremos solución a este problema, porque mientras la tecnología siga avanzando, estos tipos de delitos también se irán reinventando y seguirán afectándonos en todos los aspectos. Sin embargo, nosotros también estaremos mejorando cada vez más a pesar que todavía tenemos ciertas limitaciones. **(Gerente de Seguridad de la Información-BBVA)**

Categoría 3 – Presupuestos y gastos relacionados

En esta categoría se analizará principalmente como es que el incremento de los delitos informáticos afecta directa o indirectamente en los presupuestos y gastos de las entidades financieras como son el BBVA el BCP.

3.3 ¿Cuáles son las variaciones en el incremento de presupuesto de gastos relacionados a tecnología de la información en el sistema financiero de los principales bancos de Lima como son el BCP Y BBVA?

Todas las categorías antes analizadas, nos llevan de forma directa o in directa a la pérdida de dinero de las entidades bancarias, ya sea en mayor en menor medida. Cabe destacar que el impacto de la pérdida de dinero va más allá de una pérdida inmediata, esta también se refleja en el mediano y largo plazo. Como ya dijimos anteriormente, a pesar de que muchas veces, los bancos no asumen las devoluciones de dinero por fraude, si no, las aseguradoras; a largo plazo estos van perdiendo su principal fuente de ingresos, los clientes.

> (…) Ufff.. Yo siento que cuando perdemos a un cliente, perdemos a 100 más. Como todos sabemos, siempre es más fácil la difusión de una mala experiencia a través del boca a boca o en la mayoría de los casos (hoy en día) a través de las redes sociales. Esto con el tiempo trae consigo pérdidas económicas, ¡obviamente! **(Analista de Fraude BBVA)**

> (…) Creo que, de alguna u otra manera, todos los días perdemos la confianza de nuestros clientes. Ellos se ofuscan bastante sobre todo en cuanto a los tiempos de resoluciones de sus reclamos. A pesar de que hacemos todo lo posible por que estén contentos, se nota su malestar y descontento hacia el banco. **(Analista de Fraude BCP)**

> (…) Uhmm a veces es un poco difícil trabajar en esta área, siempre vamos a tener clientes insatisfechos, más ahora en los últimos años que los fraudes han aumentado. **(Analista de Fraude BBVA)**

Por otro lado, hay que indicar que la pérdida de dinero y aumento de costos y gastos no solamente se da por la pérdida de clientes, sino también porque los bancos están invirtiendo en infraestructura y aplicaciones tecnológicas que cuenten con las medidas de protección adecuadas. Un ejemplo de ello no indica el sub gerente de Fraude del BCP.

> (…) A diferencia de otras áreas, todos los años se incrementa un porcentaje considerable al área de tecnología de la información, ya que debido a la vulnerabilidad cada vez es más difícil mantener actualizados nuestros sistemas de seguridad informáticos. **(Segmento 4: Subgerente Adjunto de Prevención del Fraude BCP)**

> (…) Nuestras medidas de control van cambiado, por ende, aumenta el presupuesto del área, El gasto realizamos por monitorear nuestros sistemas es por cada usuario; A veces reducimos costos en monitorear banca por internet, pero tenemos que aumentar el costo de la seguridad de nuestros cajeros o en el aplicativo móvil. El presupuesto siempre va a aumentando porque tenemos que ir cubriendo nuevos puntos que se identifican año a año. **(Sub Gerente de Control Operativo y Negocio BBVA)**

Según lo indicado por el gerente de tecnología de la información del BCP cada año se va incrementando el presupuesto destinado a los gastos de ciber seguridad. Por ejemplo, hace unos 4 años, estos solo destinaban el 2% de su presupuesto a la seguridad; sin embargo, hoy en día destinan entre el 7 u 8 % de su presupuesto.

Otro factor a destacar es que los incrementos en los gastos debido a delitos informáticos no solamente se dan por la adquisición de nueva tecnología sino también por la implementación de diferentes medidas que de algún u otro modo ayudan a prevenir y frenar este mal; por ejemplo. Para la implementación de talleres y capacitaciones que ya han sido anteriormente descritas; tanto el área de marketing como el área de imagen institucional vienen destinando un presupuesto aparte, dinero que antes no estaba considerado dentro de su presupuesto.

> (…) No solamente aumenta el presupuesto en nuestra área, sino también en áreas como Marketing (debido a las campañas de concientización), operaciones (implementación de nuevos procesos) y recursos humanos (Nuevo personal especializado en algún nuevo sistema contra fraudes) **(Segmento 3: Subgerente Adj. De Monitoreo Trasancional BBVA).**

> (…) En los últimos años, debido a las altas incidencias de reclamos. A modo de recuperar e reforzar la imagen de nuestra institución; en coordinación con el área de Marketing hemos lanzado ciertos proyectos de talleres capacitaciones los cuales nos ha generado un gasto adicional a nuestro presupuesto. **(Dep. de Imagen insitucional del BCP)**

Finalmente, un punto importante que no queremos dejar de lado son los gastos que se dan por la compra, implementación y capacitación al adquirir nuevos sistemas de y productos de seguridad. Según nos indica el especialista en seguridad de RSA, cuando venden algún producto al banco, el precio de este no incluye las capacitaciones y asesorías permanentes. Este es un costo a parte; además hay que considerar los gastos en la fabricación de nuevas instalaciones para la instalación de maquinarias. Habilitación de nuevos almacenes, por ejemplo, en el caso del almacenaje y distribución de los token.

(…) Es obvio que los procesos operacionales han sido modificados y hasta a veces se ha creado nuevos procesos debido al incremento de los delitos informáticos; cada vez que nosotros como proveedores de seguridad implementamos un nuevo sistema de seguridad hay que capacitar personas, modificar, crear nuevos procedimientos y hasta implementar nuevos ambientes lo que implica también costos y gastos. **(Segmento 6: Proveedor de sistemas de seguridad).**

CAPÍTULO IV. DISCUSIÓN DE RESULTADOS

4.1 Hallazgos

- Se identificó que a nivel país, no existe información suficiente, datos actuales y tampoco estudios estadísticos respecto a los delitos informáticos, como si los hay en otros países de nuestra región. A pesar que, en muchas de las investigaciones realizadas por empresas de seguridad extranjeras, muestran al Perú como uno de los principales países más vulnerables respecto a este tipo de delitos.
- Se observa que la prevención contra el fraude o delito informático, no solo se da en el área de seguridad o de prevención del fraude. Si no que en los últimos años se ha expandido a todas las áreas creando una cultura de alerta. Cada integrante muestra responsabilidad y compromiso hacia su entidad y constantemente se les brinda capacitación y cursos a todos los trabajadores, ya sea virtual o presencial.
- Se identificó que la percepción del cliente respecto a ambos bancos sigue siendo negativa, a pesar de los esfuerzos que realizan para contrarrestar este tipo de delitos, todavía no es suficiente. Esta percepción también lo corroboraron los mismos trabajadores de ambas entidades, ya que son los que reciben los reclamos.

4.2 Barreras

Tuvimos dos escenarios, en el caso del BCP no tuvimos inconvenientes, solo demoras por temas de horarios, todos fueron muy amables al entrevistarlos, ya sea presencialmente o vía call conference.

Sin embargo, en el caso del BBVA nos fue difícil llegar a los subgerentes de las áreas de seguridad de la información y de fraude, ya que no los podíamos contactar telefónicamente, lo que nos retrasó bastante en esas dos entrevistas, hasta que pudimos conseguir el contacto que nos referenciara con estas personas, solo uno de ellos no nos recibió personalmente y la otra persona aceptó brindarnos la entrevista por teléfono y luego enviarnos por email completo.

4.3 Brechas

No hemos tenido brechas en nuestra investigación.

CAPITULO V. CONCLUSIONES

1 Se pudo validar la hipótesis inicial respecto a los cambios y creación de nuevos procesos operacionales debido al incremento de los delitos informáticos así también el incremento en la asignación de presupuesto en tecnología de la información destinada a ciberseguridad, la pérdida de credibilidad y desgaste en la imagen de los principales bancos del Perú como son el BBVA Banco Continental y BCP de Lima Metropolitana en los últimos 5 años.

2 También se identificó que, pese a que se reconoce un incremento de estos delitos en ambos bancos, todavía no hay una asignación de un presupuesto considerable para ciber seguridad. Si bien es cierto, se considera un crecimiento anual; este todavía no es suficiente respecto a otros bancos de otros países.

3 En las entrevistas se identificó que, en ambas entidades financieras, coinciden con que el delito más frecuente es el Phishing, el cual afecta en un 70%, tanto a los clientes como a los bancos, según indica el Sub gerente de prevención del fraude. Así mismo, el segundo delito más frecuente entre los entrevistados es la clonación de tarjetas.

4 En cuanto a la imagen de ambos bancos, respecto a los clientes que se entrevistaron, se pudo determinar que la mayoría muestra su descontento hacia el banco debido a las demoras en la resolución de sus reclamos. A pesar de estar en constante actualización e implementación de sistemas de seguridad y tener un proceso de contingencia ante un fraude de mayor magnitud, vienen pasando por siniestros pequeños que les afecta desfavorablemente principalmente en la imagen institucional.

RECOMENDACIONES

1 Se recomienda a los futuros profesionales seguir investigando sobre este fenómeno que año tras año viene atacando a todos los sectores y niveles de nuestra sociedad, ya que hoy en día, los estudios e investigaciones respecto a este tema son escasos en nuestro país. Esto ayudara a seguir aportando información actualizada y valiosa a toda la comunidad estudiantil y a los sectores interesados.

2 A las entidades correspondientes se les recomienda realizar más estudios e investigaciones respecto a los delitos informáticos, de modo que puedan tomar las acciones necesarias para seguir implementando métodos y sistemas de seguridad informática actuales para así poder contrarrestar y evitar las consecuencias nefastas de este tipo de acciones ilegales.

3 Se sugiere a ambos bancos seguir incrementando sus esfuerzos en combatir este fenómeno, ya que, a pesar de los esfuerzos realizados, los clientes todavía tienen una mala percepción del banco respecto a la seguridad que les brindan.

4 A los futuros investigadores y profesionales sugerimos realizar estudios e investigaciones respecto a la falta de una política de defensa cibernética en nuestro país ya que el crecimiento continuo de estos ataques ha ido más allá de nuestros códigos penales establecidos; sin embargo, las autoridades y el gobierno no tienen, todavía, un real interés y conocimiento profundo de este problema, esto hace que nuestro país sea un país potencialmente expuesto a este fenómeno.

BIBLIOGRAFÍA

Alan D. Smith, (2004) "Cybercriminal impacts on online business and consumer confidence", Online Information Review, Vol. 28 Issue: 3, pp.224-234.

Anderson, R. et. al, (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* pp. 265-300). Springer, Berlin, Heidelberg.

ASBANC (2013). Memoria Anual 2013 de la Asociación de Bancos. Recuperado de http://www.asbanc.com.pe/Publicaciones/MemoriaAnualASBANC2013.pdf

ASBANC (2016). La economía y el sistema financiero en el 2016. Recuperado de http://www.asbanc.com.pe/Publicaciones/MA-asbanc-2016.pdf#page=32

BBC (2016, Setiembre 6). "12 ataques por segundo": cuáles son los países de América Latina más amenazados por "malware". Recuperado de http://www.bbc.com/mundo/noticias-37286420

BCP (2017). Informe de Sostenibilidad 2016. Recuperado de https://www.bcp.com.bo/Content/descargas/MemoriaRSE/memoria_rse_2016.pdf

Beekman, G. (1995). Computación & informatica hoy. Una Mirada a la teconología del mañana. México.

Calderon-Sequeiros, C. (2016). Vacíos Legales que imposibilitan a la sanción de los delitos informáticos en el nuevo código penal peruano-2015.

Castro P. y Sanchez-Garzón, R. E. (2006). Modelo de mejoramiento en la calidad del servicio al cliente para el banco Davivienda desde la perspectiva de quejas y reclamos de los clientes 2006.

Deloitte. (2015). El futuro de la banca móvil en América Latina Perspectivas desde Argentina, Brasil y México. Recuperado de https://www2.deloitte.com/content/dam/Deloitte/py/Documents/about-deloitte/Futuro_banca_movil2012.pdf

Deloitte. (2016). La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. Recuperado de https://www2.deloitte.com/

Dueñas C., M. (2015). Fraude electrónico crece y cambia de cara tan rápido como la tecnología. Bogotá. Recuperado de internet el 05/08/2015 en http://colombiainn.com.co/fraude-electronico-crece-y-cambia-de-cara-tan-rapido-como-latecnologia/

ESET. (2017). ESET Security Report Latinoamérica 2017. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Gestión, R. (2017, Agosto 10). Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017. Retrieved from https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411

Gestión (2017). Indecopi: 45 de cada 100 reclamos son contra entidades financieras Recuperado de: https://gestion.pe/tu-dinero/indecopi-45-100-reclamos-son-entidades-financieras-134556

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Grant Thorton. (2017, Mayo 12). 3 de 10 e mpresas españolas sufrieron ciberataques en 2016. Obtenido de https://www.grantthornton.es/

ITNow. (2017, Junio 24). Just a moment.Las 15 principales estadísticas de 2017 para IT. Obtenido de https://revistaitnow.com/las-15-principales-estadisticas-2017/

Olenski,S. (2016, August 4). The Effect Of Cyber Crime On Online Shopping. Recuperado de https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/#69a51c522b87

Kellerman T. et al (2015) Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. Recupedado de: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Orts, E & Roig, M (2001). Delitos informáticos y delitos communes cometidos a través de la informática. Valencia

PERÚ21, R. (2017, Enero 24). Aumentan ciberataques en el Perú: ¿Por qué pensamos que nunca nos pasará a nosotros? Recuperado de https://peru21.pe/cheka/tecnologia/aumentan-ciberataques-peru-pensamos-pasara-62934

PWC. (2014, Noviembre). Delitos económicos: Una amenaza a los negocios. Obtenido de https://www.pwc.pe/es/publicaciones/assets/delitos-economicos-2014.pdf

PWC. (2016, Diciembre, 12). Hacia una nueva ética en los negocios. Delito económicos einformáticos.Recuperadodehttps://www.pwc.com.ar/es/publicaciones/assets/encuesta-delitos-economicos-2016.pdf

Price Waterhouse Coopers (PWC). (2016). Encuesta global sobre delitos económicos. Recuperado de https://www.pwc.com.ar/es/publicaciones/assets/encuesta-delitos-economicos-2016.pdf

Rincón-Castañeda, et. al, (2016). *Diagnóstico actual del ciberdelito contra los usuarios de la banca en línea en el sector bancario colombiano* (Bachelor's thesis, Instituto Tecnologico Metropolitano).

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. *Journal of Marketing Theory and Practice*, *10*(2), 29-37.

Sajón, Edgardo (2018). Encuesta Global sobre Delitos Econòmicos 2018. Recuperado de: http://www.pwc.com.ar/es/publicaciones/assets/encu esta-global-sobre-delitos-economicos-argentina-201 8.pdf.

Sanmartín, Álvaro, Sanmartín (2017). El impacto del cibercrimen en el mundo. Recuperado de https://www.grantthornton.es/globalassets/___spain___/insights/el-impacto-del-cibercrimen-en-el-mundo.pdf

Smith, Katherine & Smith, Murphy & Smith, Jacob. (2010). Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value. Academy of Marketing Studies Journal. 15.

Tellez, J. (1996). Los delitos informaticos. Situación en Méxio, Informática y derecho Nº 9, 10 y 11. Centro Regional de Extermadura, Mérida.

Temperini, M. G. I. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. En *1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*.

Vizcardo, S. J. H (2014). Tipificación De Los Delitos Informáticos Patrimoniales En La Nueva Ley De Delitos Informáticos N° 30096 *alma Máter Segunda Época*, (1), 69-80.

Villavicencio, F. (2014) Delitos informáticos. Cibercrimen. Revista IUS ET Veritas. Diciembre 2014.

World Economic Forum. (2017, January 11). The Global Risks Report 2017. Obtenido de https://www.weforum.org/reports/the-global-risks-report-2017

ANEXOS

ANEXO 1: GUÍA DE PREGUNTAS

SEGMENTO 1: Gerente de seguridad

1 Procesos operativos del sistema financiero

¿Cuáles son los procesos más usados dentro del banco a fin de minimizar los ciber delitos?

A lo largo de estos últimos 3 años ¿han sido modificados o han aumentado estos procesos?

2 Imagen y reputación de la entidad financiera

¿Cuáles son los factores que más impactan en la imagen y reputación del banco cuando se ven expuestos a un ciber delito de gran magnitud?

¿Qué tanto les afecta a ustedes como banco cuando un cliente publica en la red social (Facebook, Twitter, etc.) alguna queja o reclamo por fraude?

3 Presupuesto de gastos en relación a la ciber seguridad

Actualmente, ¿Cuentan con un presupuesto destinado solo para ciber seguridad?

¿Considera que, en los últimos 5 años, ha venido incrementándose el presupuesto destinado para la seguridad de la información?

SEGMENTO 2: Sub Gerente de Control de la Operativa y Negocio – Engeniering

4 Procesos operativos del sistema financiero

¿Considera usted que en los últimos 5 años ha habido un aumento o reducción de los fraudes o delitos informáticos hacia los bancos?

En los últimos años, ¿Han realizado algún tipo de cambio significativo, ya sea en proceso o cantidad de personas, debido a los fraudes o delitos informáticos?

5 Imagen y reputación de la entidad financiera

¿Según su experiencia en banca, de qué manera afecta más a los bancos, este tipo de delitos? ¿En imagen, gastos?

¿Considera usted que los delitos informáticos y fraudes suponen un peligro potencial para el banco?

6 Presupuesto de gastos en relación con la ciber-seguridad

En los últimos 5 años, ¿Se ha incrementado el presupuesto para la seguridad de la información a fin de minimizar los delitos informáticos?

SEGMENTO 3: Subgerente Adjunto de Monitoreo Transaccional

7 Procesos operativos del sistema financiero

¿Cuáles son los procesos operativos que se realizan dentro del banco con el fin de evitar delitos informáticos?

¿Cuáles son las medidas de seguridad que se tienen en las operaciones realizadas a través de los canales digitales del banco?

¿Existe manera alguna de poder bloquear una operación inusual o sospechosa?

8 Imagen y reputación de la entidad financiera

En el área de monitoreo transaccional, ¿Cuentan con algún plan o medida ante una pérdida a fin de cuidar la imagen del banco?

9 Presupuesto de gastos en relación con la ciber seguridad

¿El presupuesto con el que cuentan para sistemas de monitoreo o seguridad, se ha venido incrementando en los últimos años?

SEGMENTO 4: Subgerente Adjunto de Prevención del Fraude

10 Procesos operativos del sistema financiero

Basándose en su experiencia, ¿considera que en los últimos 5 años ha habido un aumento o reducción de los fraudes o delitos informáticos hacia los bancos?

¿Cuáles son los delitos informáticos o los fraudes más frecuentes a los cuales se enfrenta el banco?

¿Considera usted que los delitos informáticos y fraudes suponen un peligro potencial para el banco?

11 Imagen y reputación de la entidad financiera

¿Cree usted que se le está dando la debida importancia al problema que se viene dando debido a los delitos informáticos, sobre todo al dañar la imagen del banco?

12 Presupuesto de gastos en relación con la ciber-seguridad

¿Según su experiencia en banca, de qué manera afecta a los bancos, este tipo de delitos? (Imagen, costos, redefinición de procesos)

¿En los últimos años, han realizado algún tipo de cambio significativo (procesos, personas, gastos) debido a los fraudes o delitos informáticos?

SEGMENTO 5: Analista de Reclamos

13 Procesos operativos del sistema financiero

¿Cuántos reclamos por fraude digital atienden en un día normal?

¿Cuál es el procedimiento que tienen para atender un reclamo por fraude realizado con una tarjeta VISA?

¿Cuál es el tiempo de atención para dichos reclamos?

14 Imagen y reputación de la entidad financiera

Ustedes que tienen contacto con el cliente, ¿Cuáles crees que son los factores que más impactan en la imagen que se lleva el cliente respecto al banco?

¿Cuentan con capacitaciones o actualizaciones sobre las medidas de seguridad que toma VISA y el banco en sinergia?

15 Presupuesto de gastos en relación con la ciber seguridad

¿Qué porcentaje aproximadamente viene asumiendo el banco, sobre los reclamos en los que el cliente se ve afectado monetariamente?

¿Cuáles son los niveles de autonomía con los que cuenta los analistas para realizar devoluciones al cliente, una vez validado el reclamo?

SEGMENTO 6: Proveedor de Sistema de Seguridad

16 Procesos operativos del sistema financiero

¿Cuál es el servicio que brindan ustedes como empresa de seguridad digital?

¿Quiénes son sus principales clientes?

¿Cuáles son los principales productos o sistemas de seguridad que solicitan los bancos?

¿Cuáles son los principales delitos informáticos a los cuales se enfrentan los bancos?

17 Imagen y reputación de la entidad financiera

Basándonos en las propuestas que les presentan a los bancos, ¿Es uno de los puntos más fuertes a favor de ustedes, el que se vea afectada la reputación del banco?

18 Presupuesto de gastos en relación con la ciber seguridad

¿Se ha incrementado la demanda de los servicios de seguridad?

¿Los bancos están dispuestos a pagar un poco más a fin de poder proteger sus servicios y medios transaccionales?

SEGMENTO 7: Clientes

19 Procesos operativos del sistema financiero

Actualmente, ¿Qué productos mantienes con el banco?

¿A qué segmento pertenece?

¿Ha sido víctima de fraude, robo o clonación?

20 Imagen y reputación de la entidad financiera

Basándonos en la experiencia que ha vivido, ¿Cree usted que el banco está tomando las medidas necesarias para prevenir estos ciber delitos?

¿En algún momento ha utilizado la red social del banco para elevar un reclamo o queja que ha tenido por fraude o clonación?

¿Dejaría de ser cliente del banco o se trasladaría a otra entidad financiera, en caso el banco no asuma una operación que usted no reconoce?

21 Presupuesto de gastos en relación con la ciber seguridad

¿Actualmente paga un seguro de protección de tarjeta?

¿Está de acuerdo en pagar por la renovación del token o tarjeta de coordenadas el cuál le brinda seguridad a fin de confirmar sus operaciones?

ANEXO 2: GLOSARIO DE TERMINOS

1. Browser (Buscador): El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
2. Cookie: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de anti-cookie software que automáticamente borran esa información entre visitas a su sitio.
3. TIC: Tecnología de la Información y Comunicaciones
4. Malware: es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares podemos encontrar términos como, por ejemplo, Virus, Troyanos, Gusanos (Worm), keyloggers, Botnets
5. Phising/Spoofing: Significa acceder ilegalmente un ordenador y enviar múltiples correos electrónicos; volver a enviar varios mensajes de correo electrónico comercial con la intención de engañar a los destinatarios; o falsificar información del encabezado en varios mensajes de correo electrónico.
6. Extorsión: Es el uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.
7. Hacking: Es el hacking es acceder de forma ilegal a datos almacenados en un ordenador o servidor. El último caso sonado de hacking fue el robo de datos de los clientes de Ashley Madison.
8. Fraude: Es la elaboración de cualquier plan para defraudar, o para la obtención de dinero o bienes mediante pretextos falsos o fraudulentos, usando Internet con el fin de ejecutar el plan.
9. Ciberbulling: Es el uso de Internet para molestar, abusar, amenazar o acosar a la persona, a menudo de forma anónima. Los casos de ciberbulling parecen haber ido en aumento en los últimos años, con trágicas consecuencias en ocasiones.
10. Malware: Es también conocido como software malicioso (virus en general, troyanos, spyware, etc.). Son programas informáticos que, una vez instalados y ejecutados en los equipos, puede dar el control parcial o total de estos a los criminales lo que les permite acceder fácilmente a cualquier información sensible o dañar/robar datos.
11. Ransomware: Es cifrar los archivos de un ordenador para impedir que el usuario tenga acceso a ellos. Una vez conseguido, lo más habitual es que aparezca un mensaje en la pantalla exigiendo el pago de unos 300 dólares en Bitcoins en un plazo de entre 48 y 72 horas. A cambio, el criminal promete entregar al usuario la clave que le permitirá desbloquear su dispositivo.