UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN ADMINISTRACIÓN FINANCIERA

INCIDENCIA FINANCIERA POR EL RIESGO OPERATIVO DE PHISHING EN TRANSACCIONES ELECTRÓNICAS EN UNA INSTITUCIÓN BANCARIA DEL SISTEMA FINANCIERO GUATEMALTECO

LICENCIADO JORGE FERNANDO MO CAAL

Guatemala, marzo de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN ADMINISTRACIÓN FINANCIERA

INCIDENCIA FINANCIERA POR EL RIESGO OPERATIVO DE PHISHING EN TRANSACCIONES ELECTRÓNICAS EN UNA INSTITUCIÓN BANCARIA DEL SISTEMA FINANCIERO GUATEMALTECO

Informe Final de Trabajo Profesional de Graduación para optar al Grado de Maestro en Artes, con base en el "Instructivo para Elaborar el Trabajo Profesional de Graduación para Optar al Grado Académico de Maestro en Artes", aprobado por la Honorable Junta Directiva de la Facultad de Ciencias Económicas, el 15 de octubre de 2015, según Numeral 7.8 Punto SÉPTIMO del Acta No. 26-2015 y ratificado por el Consejo Directivo del Sistema de Estudios de Postgrado de la Universidad de San Carlos de Guatemala, según Punto 4.2, sub-incisos 4.2.1 y 4.2.2 del Acta 14-2018 de fecha 14 de agosto de 2018.

DOCENTE: LICDA. SILVIA MARISOL CRUZ BARCO

AUTOR: **LICENCIADO JORGE FERNANDO MO CAAL**

Guatemala, marzo de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
HONORABLE JUNTA DIRECTIVA

Decano:	Lic. Luis Antonio Suárez Roldán
Secretario:	Lic. Carlos Roberto Cabrera Morales
Vocal Primero:	Lic. Carlos Alberto Hernández Gálvez
Vocal Segundo:	MSc. Byron Giovani Mejía Victorio
Vocal Tercero:	Vacante
Vocal Cuarto:	P.C. Marlon Geovani Aquino Abdalla
Vocal Quinto:	P.C. Carlos Roberto Turcios Pérez

TRIBUNAL QUE PRACTICÓ EL
TRABAJO PROFESIONAL DE GRADUACIÓN

Coordinador:	Dr. Sergio Raúl Mollinedo Ramírez
Evaluador:	MSc. Victor Manuel López Fernández
Evaluador:	MSc. Juan Carlos González Meneses

ACTA/EP No. 03662

ACTA No. MAF-JN-B-012-2021

De acuerdo al estado de emergencia nacional decretado por el Gobierno de la República de Guatemala y a las resoluciones del Consejo Superior Universitario, que obligaron a la suspensión de actividades académicas y administrativas presenciales en el campus central de la Universidad, ante tal situación la Escuela de Estudios de Postgrado de la Facultad de Ciencias Económicas, debió incorporar tecnología virtual para atender la demanda de necesidades del sector estudiantil, en esta oportunidad nos reunimos de forma virtual los infrascritos miembros del Jurado Examinador, 17 de Abril de 2,021, a las 12:00 horas para practicar la PRESENTACIÓN DEL TRABAJO PROFESIONAL DE GRADUACIÓN del Licenciado Jorge Fernando Mo Caal, carné No. 200812887, estudiante de la Maestría en Administración Financiera de la Escuela de Estudios de Postgrado, como requisito para optar al grado de Maestro en Artes. El examen se realizó de acuerdo con el Instructivo para Elaborar el Trabajo Profesional de Graduación para optar al grado académico de Maestro en Artes, aprobado por la Junta Directiva de la Facultad de Ciencias Económicas, el 15 de octubre de 2015, según Numeral 7.8 Punto SÉPTIMO del Acta No. 26-2015 y ratificado por el Consejo Directivo del Sistema de Estudios de Postgrado –SEP- de la Universidad de San Carlos de Guatemala, según Punto 4.2, subincisos 4.2.1 y 4.2.2 del Acta 14-2018 de fecha 14 de agosto de 2018.----------

Cada examinador evaluó de manera oral los elementos técnico-formales y de contenido científico profesional del informe final presentado por el sustentante, denominado "Incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco", dejando constancia de lo actuado en las hojas de factores de evaluación proporcionadas por la Escuela. El examen fue Aprobado con una nota promedio de 73 puntos, obtenida de las calificaciones asignadas por cada integrante del jurado examinador. El Tribunal hace las siguientes recomendaciones: Que el sustentante incorpore las enmiendas señaladas dentro de los 5 días hábiles contados del 19 al 23 de Abril 2021. ----------

En fe de lo cual firmamos la presente acta en la Ciudad de Guatemala, a los 17 días del mes de Abril del año dos mil veintiuno.

Dr. Sergio Raúl Mollineda Ramírez
Coordinador

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA FACULTAD DE CIENCIAS ECONÓMICAS ESCUELA DE POSTGRADO

MSc. Víctor Manuel López Fernández
Evaluador

MSc. Juan Carlos González Meneses
Evaluador

Lic. Jorge Fernando Mo Caal
Postulante

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO

ADENDUM

El infrascrito Coordinador de la Terna Evaluadora CERTIFICA que el estudiante Jorge Fernando Mo Caal, incorporó los cambios y enmiendas sugeridas por cada miembro de la terna evaluadora.

Guatemala, 26 de Abril de 2021.

(f)

Ph. D. Sergio Raúl Mollinedo Ramírez
Coordinador de la Terna Evaluadora

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONÓMICAS
Edificio "s-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

J.D-TG. No. 0744-2021
Guatemala, 17 de septiembre del 2021

Estudiante
Jorge Fernando Mo Caal
Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala

Estudiante:

Para su conocimiento y efectos le transcribo el Punto Quinto, inciso 5.1, subinciso 5.1.1 del Acta 21-2021, de la sesión celebrada por Junta Directiva el 13 de septiembre de 2021, que en su parte conducente dice:

"QUINTO: ASUNTOS ESTUDIANTILES

5.1 Graduaciones
5.1.1 Elaboración y Examen de Tesis y/o Trabajo Profesional de Graduación

Se tienen a la vista las providencias de las Escuelas de Economía, Administración de Empresas y Estudios de Postgrado; en las que se informa que los estudiantes que se indican a continuación, aprobaron el Examen de Tesis y/o Trabajo Profesional de Graduación, por lo que se trasladan las Actas de los Jurados Examinadores y los expedientes académicos.

Junta Directiva acuerda: 1º. Aprobar las Actas de los Jurados Examinadores. 2º. Autorizar la impresión de tesis, Trabajos Profesionales de Graduación y la graduación a los estudiantes siguientes:

Solicitudes de Impresión, Maestría en Artes
TPG, Jornada Normal 2021

Maestría en Administración Financiera

	Nombre	Registro Académico	Trabajo Profesional de Graduación
Ref. MAF-JN-B-12-2021	Jorge Fernando Mo Caal	200812887	INCIDENCIA FINANCIERA POR EL RIESGO OPERATIVO DE PHISHING EN TRANSACCIONES ELECTRÓNICAS EN UNA INSTITUCIÓN BANCARIA DEL SISTEMA FINANCIERO GUATEMALTECO

3º. Manifestar a los estudiantes que se les fija un plazo de seis meses para su graduación".

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
SECRETARIA
GUATEMALA

m.ch

Agradecimientos

A DIOS: Por darme el privilegio de la vida y bendecirme con la oportunidad de culminar con éxito esta meta.

A MI MAMÁ: Teresa Caal, por estar siempre a mi lado, le agradezco por su amor, dedicación, regaños y apoyo que me ha brindado durante toda mi vida para ella todo mí amor.

A MI PADRE: Fernando Mó, (Q.E.P.D.), a quien agradezco por su amor incondicional y por enseñarme que, con trabajo, esfuerzo y confianza en Dios, es posible alcanzar cada uno de nuestros sueños.

A MIS HERMANOS: Maynor Rene Mo Caal, por ser un apoyo moral y ejemplo a seguir, Miguel Fernando Mo Caal, (Q.E.P.D.), a quien extraño y siempre estaré agradecido por haber sido parte de mi vida, gracias por estar a mi lado y ser mis amigos.

A MI FAMILIA: Con aprecio y cariño a toda mi familia.

A MIS AMIGOS: A todos mis queridos amigos porque son el aliento que me motiva a superarme cada día:

A LA ESCUELA DE ESTUDIOS DE POSTGRADO: A través de la Facultad de Ciencias Económicas, por haberme permitido formar parte de la facultad y culminar esta meta.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Por todos los conocimientos adquiridos, que contribuyen a mi desarrollo como profesional.

CONTENIDO

Resumen

El sistema financiero guatemalteco tiene dos segmentos, el primero lo constituye el sector financiero formal y el segundo lo conforman el sector financiero informal. El sector financiero formal está conformado por instituciones cuya autorización es de carácter estatal, sujetas a la supervisión de la Superintendencia de Bancos.

El sistema financiero en Guatemala ha sufrido una serie de cambios, derivado de un incremento acelerado de empresas en la industria, lo que ha repercutido en el desarrollo de un mercado competitivo, las instituciones bancarias han representado un papel importante, debido a que por medio de estas se ha fomentado el desarrollo económico mediante, inversión y financiamiento.

El sector bancario es una de las áreas comerciales más dinámicas, debido a su amplio campo de servicios, lo que representa grandes ventajas competitivas, lo cual influye en el desarrollo económico a nivel nacional.

Actualmente en Guatemala, el sector bancario ha tenido un desempeño considerable ya que los bancos actualmente utilizan herramientas tecnológicas, que han evidenciado una nueva modalidad para brindar distintos servicios y enfocar los productos financieros a una nueva generación, no solo en aspectos de publicidad o marketing sino también en operaciones que normalmente se realizarían en una agencia bancaria.

Para el desarrollo del trabajo profesional de graduación se estableció un enfoque financiero, se realizó con base en la utilización del método científico, incluyendo la evaluación previa del sector financiero en Guatemala; específicamente el sector bancario por medio de la unidad de análisis.

Se evalúa el caso particular de la entidad bancaria BANLLASE, S. A., del cual se logra identificar mediante la evaluación de riesgo operativo, ataques de hackers. Derivado a

esto, se realizó una investigación de campo donde se obtuvieron los datos que demuestran la utilización de phishing en transacciones electrónicas.

BANLLASE, S. A. es una de las entidades bancarias que ha tratado de innovar por lo que ha implementado una plataforma para realizar transferencias electrónicas entre cuentas del mismo banco, otros bancos, pago de servicios e incluso pago por medio de convenios, pero por medio de phishing personas mal intencionadas han vulnerado las medidas de seguridad con las que contaba la entidad, lo que para el año 2019 repercutió financieramente y en la imagen de la entidad.

Se realizó el análisis de los estados financieros: estado de resultados, notas de ingresos y gastos extraordinarios, además la conciliación entre la utilidad contable y la renta imponible, del periodo contable 01 de enero al 31 de diciembre 2019.

Como parte del aporte del trabajo profesional de graduación se elaboró una evaluación y valoración del riesgo para BANLLASE, S. A., identificando la pérdida que puede sufrir en condiciones normales en un intervalo de tiempo con un cierto nivel de confianza para lo cual se evaluó el nivel de la probabilidad, la valoración del impacto y el riesgo inherente, lo que se reflejó en el mapa de calor, tanto del total de casos y se especificó el caso más representativo de la cuentahabiente la señora Damaris Ruano.

En conclusión, el resultado del análisis realizado demostró que ante la implementación de proyectos innovadores en Guatemala es necesario evaluar todo el riesgo que puedan afectar a la entidad bancaria, establecer políticas de divulgación y prevención ante ataques cibernéticos y documentar cualquier tipo de reclamo, beneficiando a la administración financiera, permitiendo identificar las necesidades idóneas para el banco BANLLASE y así obtener el adecuado rendimiento financiero.

Se determinó que el impacto financiero de ataques de phishing por medio de transacciones electrónicas ascendió a la cantidad de Q.2,260,600 durante el periodo

comprendido del 01 de enero al 31 de diciembre de 2019 representando un 75% del total de gastos no deducibles.

Siendo las transferencias móviles a terceros el monto más representativo del total de casos reportados en el año 2019 con Q.1,763,900 equivalente a un 78%.

Introducción

Derivado al desarrollo económico financiero, en Guatemala se ha implementado la utilización de tecnologías para el desarrollo constante hacia el servicio y satisfacción de los clientes. La unidad de estudio en el presente trabajo profesional de graduación es un banco denominado BANLLASE, S. A. del sector bancario, y el objeto de estudio es la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco.

El problema de interés al que se ha enfrentado el sector del sistema financiero bancario nacional, se refiere al riesgo operativo de phishing en transacciones electrónicas realizadas por hackers, debido a la usurpación de identidades de clientes de instituciones en plataformas digitales, mediante infiltración en correos falsos, se ha generado una nueva modalidad de robos que pueden ascender a varios miles de quetzales, lo que repercute a la entidad bancaria de forma financiera y además perjudica su reputación, debido a que se vulnera la seguridad, así como también se puede enfrentar a litigios y deserción de clientes inconformes ante tales estafas.

La propuesta de solución que se ha planteado, consiste en mecanismos e instrumentos que puedan prevenir y mitigar los ataques de phishing en transacciones electrónicas en la entidad bancaria objeto de estudio, implementando políticas administrativas, para mitigar el robo de información de clientes.

La justificación del presente trabajo profesional de graduación, demuestra la importancia que tiene el sector del sistema financiero bancario; además, existe la necesidad derivado a las nuevas tecnologías, los riesgos de robo de identidad a clientes de instituciones financieras se han incrementado, este tema es conocido mundialmente pero en el sistema bancario nacional se tiene una regulación limitada, siendo las instituciones financieras y sus usuarios los mayores perjudicados antes estos ataques, por tal razón se intenta concientizar e indicar las medidas preventivas a tomar ante estos casos de robo de identidad.

El objetivo general se relaciona en forma directa con la definición del problema, determinar el impacto financiero que repercute por defraudación mediante phishing y así proponer la implementación de mecanismos e instrumentos que puedan ayudar a resolver los ataques de phishing en transacciones electrónicas en una entidad bancaria del sistema financiero de Guatemala.

Los objetivos específicos, del trabajo profesional de graduación, son los siguientes:

Cuantificar el impacto financiero del riesgo tecnológico por robo de información a clientes de una institución bancaria y así elaborar estrategias de contingencia ante estos casos de phishing.

Reducir los gastos no deducibles por incidentes de phishing con base a procesos y políticas administrativas que contengan instrucciones detalladas para el manejo de este, además de proponer tácticas de información para clientes con base en la forma de actuar de hackers que utilizan el phishing e informar las consecuencias de no tener los estándares mínimos de ciberseguridad.

Estos objetivos planteados se pretenden cumplir con base en la propuesta de políticas preventivas, para mitigar el robo de información de clientes de una institución bancaria, así como procesos adecuados ante la forma de proceder en los reclamos de robo por medio de phishing, con base a investigación de los sistemas y canales electrónicos, así como de hechos históricos para comprobar que se tenga la certeza que no sea una estafa elaborada.

El presente trabajo profesional de graduación consta de cuatro capítulos: El capítulo uno, Antecedentes, expone el marco referencial teórico y empírico del plan de trabajo; el capítulo dos, el marco teórico en el cual se desarrolla la teoría, conceptos, definiciones y categorías científicas que contribuyen a la solución del problema abordado en el trabajo profesional de graduación; el capítulo tres contiene la Metodología, técnicas e instrumentos que guían al trabajo profesional de graduación.

El capítulo cuatro describe la discusión de resultados, el cual contiene la información recabada durante la investigación, además presenta la situación financiera de la entidad, así como la evaluación de riesgo e impacto del banco objeto de análisis.

El trabajo profesional de graduación se complementa con conclusiones, recomendaciones, bibliografía que lista los documentos que fueron consultados y anexos que complementan el trabajo profesional de graduación.

1. Antecedentes

Los Antecedentes, constituyen el origen del trabajo profesional de graduación. Exponen el marco referencial teórico y empírico de la investigación relacionada con la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco.

1.1. Sistema Financiero Guatemalteco

El sistema financiero de Guatemala comprende al conjunto de instituciones públicas y privadas que participan en el proceso de intermediación financiera, su función básica es la movilización de recursos financieros de aquellas unidades de ahorrantes a unidades que requieren recursos adicionales usuarios de crédito, en un ámbito de seguridad razonable (Palma, 2001, p.23).

En toda economía de un país, el Sistema Financiero es prácticamente la columna vertebral, la eficiencia y competitividad del Sistema Financiero deben ser objetivos fundamentales de la política económica de Guatemala y para el buen funcionamiento del crecimiento de la economía.

La función principal del sistema financiero en un país es la creación, intercambio, transferencia de activos y pasivos financieros, que producen servicios demandados por la población.

Conforme al Decreto 19-2002 del Congreso de la República de Guatemala Ley de Bancos y Grupos Financieros (2002), artículo 5 (Régimen Legal), indica: los bancos, las sociedades financieras, los bancos de ahorro y préstamo para la vivienda familiar, los grupos financieros, y las empresas que conforman a estos últimos, y las oficinas de representación de bancos extranjeros se regirán, en su orden, por sus leyes específicas, por esta ley, por las disposiciones emitidas por la Junta Monetaria y, en lo que le fuere aplicable, por la Ley Orgánica del Banco de

> Guatemala, la Ley Monetaria y la Ley de Supervisión Financiera, y demás legislación guatemalteca. (p.3)

Decreto No. 19-2002 del Congreso de la República Ley de Bancos y Grupos Financieros:

> De acuerdo a la nueva legislación los grupos financieros que se conforman, por medio de empresa controladora, estarán integrados por ésta y por dos o más de las empresas siguientes: bancos, sociedades financieras, casas de cambio, almacenes generales de depósito, compañías aseguradoras, compañías afianzadoras, empresas especializadas en emisión y/o administración de tarjetas de crédito, empresas de arrendamiento financiero, empresas de factoraje, casas de bolsa, entidades fuera de plaza o entidades off shore y otras que califique la Junta Monetaria. (p.11)

Cuando el control común lo tenga la empresa responsable, los grupos financieros estarán integrados por ésta y por una o más de las empresas mencionadas anteriormente.

Corresponde a la Junta Monetaria autorizar la conformación de grupos financieros, previo dictamen de la Superintendencia de Bancos. Todas y cada una de las empresas integrantes de los grupos financieros estarán sujetas a supervisión consolidada por parte de la Superintendencia de Bancos (SIB, 2020, p.4).

La Junta Monetaria integrada conforme a la Constitución Política de la República de Guatemala, ejerce la dirección suprema del Banco de Guatemala.

La Superintendencia de Bancos es un órgano de banca central, eminentemente técnico, que actúa bajo la dirección general de la Junta Monetaria y ejerce la vigilancia e inspección del Banco de Guatemala, bancos, sociedades financieras, entidades de seguros, afianzadoras, almacenes generales de depósito, casas de cambio, grupos financieros y empresas controladoras de grupos financieros y las demás entidades que otras leyes dispongan (SIB, 2020, p.6).

1.2. Antecedentes del Sector Bancario

Banco se definen como aquellas instituciones que realizan operaciones de banca, es decir, es prestatario y prestamista de crédito; recibe y concentra en forma de depósitos los capitales captados para ponerlos a disposición de quienes puedan hacerlos fructificar (Osorio, 2000, s.p).

Las instituciones bancarias se pueden clasificar de diferentes formas, entre éstas se pueden mencionar las siguientes.

Según el origen del capital:

- Bancos públicos, el capital es aportado por el Estado.
- Bancos privados, el capital es aportado por accionistas particulares.
- Bancos mixtos, su capital se forma con aportes privados y oficiales.

Según el tipo de operación:

- Bancos corrientes o universales, son los más comunes con que opera el público en general. Sus operaciones habituales incluyen depósitos monetarios, de ahorro, préstamos, cobranzas, pagos y cobranzas por cuentas de terceros, custodia de títulos y valores, alquileres de cajas de seguridad, financiación, otros.
- Bancos especializados: tienen una finalidad crediticia específica. Bancos de emisión: a la fecha se preservan como bancos oficiales (Palma, 2001, p.15).

Para efecto el Decreto No. 19-2002 del Congreso de la República Ley de Bancos y Grupos Financieros, establece en su artículo numero dos: que la denominación de banco, comprende a los bancos constituidos en el país y a las sucursales de bancos extranjeros establecidos en el mismo (p.3).

El diccionario de términos bancarios Ciencias Jurídicas Políticas y Sociales, define al Banco como: establecimiento público o privado autorizado para ejercer la actividad económica que genéricamente consiste en la intermediación financiera de depósitos, es

decir, la obtención de depósito o pasivo para destinarlos a fines de préstamos (Osorio, 2000, s.p).

Las entidades bancarias se organizan como sociedades anónimas. De conformidad con el Decreto del Congreso Número 2-70 del Código de Comercio en el artículo 86, la sociedad anónima es la que tiene el capital dividido y representado por acciones. La responsabilidad de cada accionista está limitada al pago de las acciones que hubiere suscrito (p.18).

Los bancos autorizados conforme a la Ley de Bancos y Grupos Financieros podrán efectuar las operaciones en moneda nacional o extranjera y prestar los servicios siguientes:

Operaciones pasivas

- Recibir depósitos monetarios
- Recibir depósitos a plazo
- Recibir depósitos de ahorro
- Crear y negociar bonos y/o pagarés, previa autorización de la Junta Monetaria
- Obtener financiamiento del Banco de Guatemala, conforme la ley orgánica de éste
- Obtener créditos de bancos nacionales y extranjeros
- Crear y negociar obligaciones convertibles
- Crear y negociar obligaciones subordinadas
- Realizar operaciones de reporto como reportado.

Operaciones activas

- Otorgar crédito
- Realizar descuento de documentos
- Otorgar financiamientos en operaciones de cartas de crédito
- Conceder anticipos para exportación
- Emitir y operar tarjeta de crédito
- Realizar arrendamiento financiero

- Realizar factoraje
- Invertir en títulos valores emitidos y/o garantizados por el Estado, por los bancos autorizados de conformidad con la Ley de Bancos y Grupos Financieros o por entidades privadas.
- En el caso de la inversión en títulos valores emitidos por entidades privadas, se requerirá aprobación previa de la Junta Monetaria;
- Adquirir y conservar la propiedad de bienes inmuebles o muebles, siempre que sean para su uso;
- Constituir depósitos en otros bancos del país y en bancos extranjeros; y,
- Realizar operaciones de reporto como reportador.

Operaciones de confianza:

- Cobrar y pagar por cuenta ajena
- Recibir depósitos con opción de inversiones financieras
- Comprar y vender títulos valores por cuenta ajena; y,
- Servir de agente financiero, encargándose del servicio de la deuda, pago de intereses, comisiones y amortizaciones.

Pasivos contingentes:

- Otorgar garantías
- Prestar avales
- Otorgar fianzas; y
- Emitir o confirmar cartas de crédito.

Servicios:

- Actuar como fiduciario
- Comprar y vender moneda extranjera tanto en efectivo como en documentos
- Apertura de cartas de crédito
- Efectuar operaciones de cobranza
- Realizar transferencia de fondos; y

- Arrendar cajillas de seguridad (pp,15.17).

De conformidad con el Decreto 19-2002 Ley de Bancos y Grupos Financieros (2002) denominación al Banco como: establecimiento público o privado autorizado para ejercer la actividad económica que genéricamente consiste en la intermediación financiera de depósitos, es decir, la obtención de depósito o pasivo para destinarlos a fines de préstamos. Las entidades bancarias se organizan como sociedades anónimas. (p.32)

El sistema financiero en Guatemala ha tenido una serie de cambios, debido a un incremento acelerado de las empresas en la industria, lo que ha provocado el desarrollo de un mercado más competitivo, las instituciones bancarias han representado un papel importante, debido a que por medio de estas se ha fomentado el desarrollo económico mediante, inversión y financiamiento (Palma, 2001, 16).

El sistema financiero guatemalteco tiene dos segmentos, el primero lo constituye el sector financiero formal y el segundo lo conforman el sector financiero informal. El sector financiero formal está conformado por instituciones cuya autorización es de carácter estatal, sujetas a la supervisión de la Superintendencia de Bancos.

La Superintendencia de Bancos, SIB (2020) informa al público que los bancos legalmente autorizados para operar en el país, al 31 de marzo de 2020 y que se encuentran bajo su vigilancia e inspección, son los siguientes:

1. El Crédito Hipotecario Nacional de Guatemala
2. Banco Inmobiliario, S. A.
3. Banco de los Trabajadores
4. Banco Industrial, S. A.
5. Banco de Desarrollo Rural, S. A.
6. Banco Internacional, S. A.
7. Citibank, N.A., Sucursal Guatemala
8. Vivibanco, S. A.

9. Banco Ficohsa Guatemala, S. A.
10. Banco Promerica, S. A.
11. Banco de Antigua, S. A.
12. Banco de América Central, S. A.
13. Banco Agromercantil De Guatemala, S. A.
14. Banco G&T Continental, S. A.
15. Banco Azteca de Guatemala, S. A.
16. Banco INV, S. A.

Siendo estas instituciones susceptibles a defraudación, por el modelo de negocio presentado, ya que esta actividad involucra el uso de transacciones de dinero, por lo que se pretende evaluar la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco. (s.p)

Según información del sistema bancario guatemalteco, el informe del Superintendente de Bancos ante la honorable Junta Monetaria (2020) indica, que al 31 de marzo 2020 los activos totales de los bancos ascienden a Q361,959 millones, registrando un crecimiento interanual de 9.1% debido principalmente al incremento de la cartera de créditos bruta en Q13,080 millones (7.3%) y de las inversiones por Q10,737 millones (11.3%) que totalizados conforman más del 82% del total del activo de los bancos. (p. 5)

Los pasivos se situaron en Q327,362 millones, lo que representó un incremento interanual de 9.2%, explicado por el aumento de los depósitos monetarios en Q9,027 millones (10.3%), los de ahorro en Q7,759 millones (14.5%) y los a plazo en Q7,622 millones (7.4%); por su parte, los créditos obtenidos aumentaron en Q4,575 millones (11.4%) (SIB, 2020, p.5).

Las utilidades antes de impuesto, a marzo de 2020, alcanzaron Q1,524 millones, mayores en 12.6% a las obtenidas a marzo de 2019. En ese período se observa un aumento en el margen de intermediación por Q484 millones (12.5%) (SIB, 2020, p.6).

La Superintendencia de Bancos (2020), al 31 de diciembre de 2019, el sistema bancario de Guatemala está integrado por 16 entidades que de manera conjunta consolidan Q. 349,684.2 millones en activos (US$46,438.8 millones), posicionándose como el segundo sistema financiero más grande de la región centroamericana, sólo por detrás de Costa Rica (con US$48,577 millones) (s.p).

Es importante señalar que este informe incluye únicamente los bancos comerciales, no así entidades fuera de la plaza (offshore). Un factor común en los sistemas financieros de la región, es la alta concentración en los bancos de mayor tamaño.

Guatemala no es la excepción, haciendo notar que las cuatro entidades más grandes de la plaza bancaria concentran el 73.0% del total de activos del sector (SIB, 2020, p.6).

En años recientes, la inestabilidad política y el ritmo de crecimiento de la economía (3.5% en 2019) han limitado la expansión del crédito bancario en Guatemala.

En ese contexto, al cierre de 2019, la cartera de préstamos muestra un crecimiento anual del 5.1% (6.7% en 2018). Los destinos económicos que más aportaron al aumento descrito fueron consumo, comercio, construcción y servicios comunales, sociales y personales; con participaciones del 8.6%, 7.9%,10.2% y 12.9%, respectivamente (SIB, 2020, p.9).

1.3. Antecedentes de phishing en Guatemala

El término phishing apareció por primera vez en enero de 1996, en el grupo de noticias de hackers alt.2600, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker "2600 Magazine".

El término 'phishing' fue adoptado por quienes intentaban "pescar" cuentas de miembros de America On line (AOL). Para poder engañar a la víctima de modo que diera

información confidencial, el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura".

Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales, incluyendo el spam. Tanto el phishing como el warezing en AOL requerían generalmente el uso de programas escritos por crackers, como el AOLHell. (Valdés, 2006, s.p)

Guatemala es el segundo país más vulnerable a ataques por internet. Según el informe del 2016 sobre ciberseguridad del Banco Interamericano de Desarrollo y otros organismos, se calcula que el cibercrimen le cuesta al mundo hasta US$575 mil millones al año. En América Latina y el Caribe constituye alrededor de US$90 mil millones anuales.

Según el ESET Security Report 2016, una encuesta reveló que las empresas que se vieron más afectadas por códigos maliciosos son las de Nicaragua, que ocupa el primer lugar, con el 58.3% de las respuestas afirmativas; luego, Guatemala, con el 55.8%, y Ecuador, con 51.9%. Los países más afectados por casos de phishing son Ecuador (24%), Perú (22%) y Guatemala (20%).

Por lo general son individuos clientes de instituciones financieras y servicios de pago en línea los blancos de los ataques de phishing. No existe una política de divulgación y aparte de ciertas instituciones financieras, el sector privado rara vez informa al gobierno de eventos cibernéticos. Sin embargo, el sector privado tiene su propia entidad de respuesta a incidentes, el CERT Cyberseg.

La tecnología es parte de la vida cotidiana del guatemalteco. Un estudio de la empresa iLifebelt detalla que Guatemala presenta la mayor cantidad de perfiles electrónicos en Centroamérica y el Caribe, alcanzando más de 5.3 millones de usuarios.

Uno de los Ciberdelitos de mayor expansión en el país es el robo de identidad por internet, las estafas electrónicas, no siempre se denuncian, pues indica “los delincuentes se basan en el anonimato de ciertos portales o sitios de envío de mensajes de texto para cometer las fechorías y las fuerzas de seguridad, muchas veces no toman por falta de ley al respecto, un ciber ataque como un delito en contra de la vida de un cibernauta”. (Leonett, 2018, s.p)

Las instituciones bancarias privadas son vulnerables a este tipo de ataques, pues este tipo de delito les es de total desconocimiento, tanto de empresas privadas como del sistema judicial.

2. Marco Teórico

El Marco Teórico contiene la exposición, análisis de las teorías y enfoques conceptuales utilizados para fundamentar la investigación relacionada con la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco.

2.1 Sistema financiero de Guatemala

El sistema financiero guatemalteco ha adoptado en la práctica un esquema de Grupos Financieros, de hecho, cada uno de estos reúne en su seno un conjunto de intermediarios financieros (empresas auxiliares) con especializaciones distintas (SIB, 2020, s.p).

Por tanto, los grupos financieros operan proveyendo un conjunto diversificado de servicios financieros.

El sector financiero de acuerdo al Decreto No. 19-2002 del Congreso de la República Ley de Bancos y Grupos Financieros (2002), establece que: está integrado por instituciones legalmente constituidas, autorizadas por la Junta Monetaria y fiscalizadas por la Superintendencia de Bancos, se integra por:

- Banco de Guatemala
- Superintendencia de Bancos
- Bancos del Sistema
- Sociedades Financieras
- Casas de Cambio
- Auxiliares de Crédito (Almacenes Generales de Depósito, Compañías Aseguradoras, Compañías Afianzadoras, Empresas Especializadas en emisión de tarjeta de crédito y/o administración, Casas de Bolsa, Entidades Off Shore) (BANGUAT, 2019, s.p).

Para resumir, el sistema financiero lo forman:

- Las instituciones (autoridades monetarias y financieras entre ellas).
- Activos financieros que se generan.
- Los mercados en que operan.

De tal forma que los activos que se generan son comprados y vendidos por este conjunto de instituciones e intermediarios en los mercados financieros. Los intermediarios financieros son un conjunto de instituciones especializadas en la mediación entre ahorradores e inversores, mediante la compraventa de activos en los mercados financieros (BANGUAT, 2019, s.p).

Existen dos tipos de intermediarios financieros:

Los bancarios, que además de una función de mediación pueden generar recursos financieros que son aceptados como medio de pago. Dentro de este grupo está el Banco de Guatemala, la Banca Privada y las Sociedades Financieras y las entidades fuera de plaza autorizadas para funcionar en territorio guatemalteco (SIB, 2020, s.p).

Los no bancarios, que se diferencian de los anteriores en que no pueden emitir recursos financieros, es decir, sus pasivos no pueden ser dinero. Dentro de este grupo se encuentran entre otros las instituciones aseguradoras, tarjetas de crédito, leasing, otros (SIB, 2020, s.p).

2.1.1 El sistema bancario guatemalteco

El sistema bancario se define como el conjunto de instituciones cuyo objetivo es canalizar el excedente que generan las unidades de gasto con superávit para encauzarlos hacia las unidades que tienen déficit, la transformación de los activos financieros emitidos por las unidades inversoras en activos financieros indirectos, más acordes con las demandas de los ahorradores, es en lo que consiste la canalización (Osorio, 2000, s.p).

Esto se realiza principalmente por la no coincidencia entre unidades con déficit y unidades con superávit, es decir, ahorrador e inversor. Del mismo modo que los deseos de los inversores y ahorradores son distintos, los intermediarios han de transformar estos activos para que sean más aptos a los últimos (SIB, 2020, s.p).

La Superintendencia de Bancos (2020), Los indicadores de calidad de cartera del sistema bancario guatemalteco son adecuados. El índice de mora exhibe un valor del 2.20%, similar al registrado en el año previo (2.18%). Al comparar con la mora de los sistemas financieros centroamericanos, Guatemala se ubica en la segunda mejor posición, sólo por debajo de El Salvador (con un indicador del 1.8%). (s,p)

El resto de los países presentan índices de créditos vencidos más elevados: Honduras (2.5%), Costa Rica (2.6%) y Nicaragua (3.0%). Un aspecto a considerar es la concentración por deudores que reflejan algunos bancos en ciertos sectores (azúcar, energía, entre otros); determinando exposiciones relevantes en algunos deudores que podrían sensibilizar la calidad de la cartera, en caso estos sectores experimenten estrés en sus flujos de efectivo (López, 2020, p.2).

Por su parte, las reservas de saneamiento de cartera vencida registran una cobertura del 135.9% al cierre de 2019, superior al promedio de los últimos cuatro años (128%). Al compararla con los sistemas de la región, la cobertura de reservas se ubica en un nivel medio, superior a los niveles de Honduras (122.8%) y El Salvador (128.5%) (SIB, 2020, s.p).

En otro aspecto, las inversiones de la banca se concentran altamente en el soberano (60% del portafolio a septiembre de 2019) y en Banco Central (22%); haciendo notar la fuerte correlación que existe entre la calidad crediticia de las inversiones y las finanzas públicas (SIB, 2020, s.p).

La plaza bancaria en Guatemala, en general, presenta una estructura de fondeo estable y diversificado. Históricamente, las fuentes de financiamiento de la banca guatemalteca

se fundamentan en los depósitos a plazo, captaciones a la vista y préstamos de entidades financieras del exterior (SIB, 2020, s.p).

La evolución de los pasivos de intermediación al cierre de 2019 ha estado determinada de manera conjunta por la mayor captación de depósitos, principalmente operaciones a plazo, el pago de los créditos obtenidos con instituciones financieras (nacionales y extranjeras) y la ampliación en el saldo de las obligaciones financieras (SIB, 2020, s.p).

López (2020), indica: “en términos de liquidez, la posición de la banca guatemalteca es favorable, destacando el importante papel que tiene el creciente flujo de remesas internacionales hacia Guatemala. Por otra parte, la participación combinada de las disponibilidades e inversiones financieras sobre los activos totales exhibe una tendencia creciente en los últimos años, siendo del 42.4% a diciembre 2019 (41.2% en 2018 y 40.6% en 2017).” (p.7)

López (2020), indica: “La cobertura de los activos líquidos sobre los depósitos totales pasó a 39.1% desde 40.2% en el lapso de un año. De comparar con otros países centroamericanos, este indicador es superior al de Honduras (37.8%), pero Costa Rica (48.6%), Nicaragua (45.6%) y El Salvador (41.5%) exhiben una mayor cobertura”. La banca guatemalteca registra un prudencial calce de operaciones en moneda extranjera. La posición larga en divisas (dólar estadounidense) representa el 11.6% del patrimonio computable a diciembre de 2019, sobre un límite regulatorio del 40%.” (p.10)

Los niveles de solvencia de la banca de Guatemala han sido adecuados para soportar pérdidas inesperadas y el crecimiento experimentado; haciendo notar que estos son inferiores a los mostrados por otros países de la región (SIB, 2020, s.p).

Cabe señalar, que la solvencia del sistema presenta mejoras graduales desde el año 2017. En ese sentido, el indicador de solidez (patrimonio / activos) se ubica en 9.8%

(9.5% en 2018), mientras que su adecuación de capital se presenta en niveles del 15.5% a diciembre 2019 (López, 2020, p.11).

Finalmente, el sistema bancario de Guatemala presenta los mejores indicadores de rentabilidad de la región, mostrando una recuperación al cierre de 2019. El mayor desempeño es el resultado de gastos operativos controlados y la ampliación de la utilidad financiera (SIB, 2020, s.p).

De esta manera, el sistema financiero cerró 2019 con una utilidad neta global de Q. 5,135 millones, registrando un notable incremento de 18.7% con respecto a 2018. Por su parte, el ROA y ROE se ubican en 1.6% y 16.3%, respectivamente (SIB, 2020, s.p).

La actividad económica de Guatemala ha aumentado su ritmo de crecimiento desde 2016. Al cierre de 2019, el Producto Interno Bruto (PIB) de la nación se expandió en 3.5% (3.1% en 2018), de acuerdo a cifras preliminares del Banco de Guatemala (BANGUAT, 2019, s.p).

Si bien se han materializado tensiones políticas desde 2015 y la reciente elección presidencial de agosto de 2019 generó incertidumbre en la actividad económica (comportamiento natural en procesos electorales), la economía registra favorables niveles de expansión (BANGUAT, 2019, s.p).

Los principales motores del crecimiento han sido el comercio, la industria manufacturera, el sector construcción y el consumo, estimulado por las remesas. Por el contrario, limitadores de la expansión económica se presentan en el sentido de la corrupción, el bajo nivel de inversión extranjera directa, las limitantes provenientes de los ingresos fiscales y el deterioro del sector externo, entre otros. (SIB, 2020, s.p).

La Superintendencia de Bancos (2020) indica: “la proyección de crecimiento para la economía guatemalteca es del 3.6% para el año 2020. Los riesgos en el sector externo están vinculados con la disminución del crecimiento económico mundial,

> principalmente el de aquellos países que mantienen relaciones comerciales con Guatemala; una evolución desfavorable en las disputas comerciales en curso; las deportaciones a gran escala de migrantes no documentados provenientes de los Estados Unidos y el deterioro en los términos de intercambio, afectando la balanza comercial. El fortalecimiento de las instituciones y la gobernabilidad; así como una mayor recaudación fiscal son los principales desafíos que enfrenta la nación.” (s.p)

Al cierre de 2019, Guatemala exhibe un crecimiento histórico en el importe de remesas recibidas, 13.1% en relación a 2018 de acuerdo con Banguat (2019), indicando:

> “similar a la dinámica observada en otros países de la región centroamericana. Dicho crecimiento está relacionado con el dinamismo del mercado laboral en Estados Unidos, así como medidas cautelares tomadas por la población emigrante guatemalteca ante las políticas anti migratorias y redadas en el país del norte. Cabe resaltar que el volumen de remesas representa un 13.8% del PIB (11.0% en 2018)”. (s.p)

En términos de la balanza comercial, a diciembre 2019, las exportaciones crecieron anualmente en 2.0%. Los productos con mayor aportación al monto exportado fueron las prendas de vestir, el banano, el azúcar, el café y el cardamomo, siendo los principales destinos Estados Unidos, Centroamérica y la Eurozona, en ese orden (BANGUAT, 2019, s.p).

En lo que respecta a las importaciones de bienes, el incremento fue de 1.1%, derivado principalmente por los bienes de consumo no duraderos y los bienes de capital para la industria. (BANGUAT, 2019, s.p).

Las importaciones provienen principalmente de Estados Unidos, Centroamérica, China y la Eurozona. Por su parte, la inflación se mantuvo en los rangos establecidos como meta por Banguat (3-5%), ubicándose en 3.41% al cierre de 2019 (2.31% en 2018). (BANGUAT, 2019, s.p).

Durante 2019, el promedio del tipo de cambio de la moneda local por el dólar estadounidense sufrió una depreciación del 2.4%, ante deterioros en los términos de intercambio. Por su parte, Banguat realizó medidas en términos de políticas monetarias para moderar la depreciación cambiaria. Vale decir que hasta el año 2017, la moneda local venía apreciándose frente al dólar desde 2013. (BANGUAT, 2019, s.p).

2.2 Marco constitucional y legal regulatorio

Las consideraciones de la banca guatemalteca en el Marco Constitucional y Legal que regula la banca en Guatemala son de importancia derivado que, en la Constitución de la República de Guatemala, así como en las Leyes Bancarias se encuentran lineamientos e indicaciones desde la apertura hasta el movimiento de las operaciones de las que se debe cumplir en la constitución de un Banco y de sus operaciones.

En la Constitución Política de la República de Guatemala (1986) en su artículo 132, indica: Es potestad exclusiva del Estado, emitir y regular la moneda, formular y realizar las políticas que tiendan a crear y mantener condiciones cambiarias y crediticias favorables al desarrollo ordenado de la economía nacional. Las actividades monetarias, bancarias y financieras, estarán organizadas bajo el sistema de banca central, el cual ejerce vigilancia sobre todo lo relativo a la circulación de dinero y a la deuda pública, dirigirá este sistema, la Junta Monetaria, de la que depende el Banco de Guatemala, entidad autónoma con patrimonio propio, que se regirá por su Ley Orgánica y Ley Monetaria. (p.27)

La Superintendencia de Bancos (2020), organizada conforme a la ley, es el órgano que ejercerá la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y las demás que la ley disponga (s.p).

El artículo 133 de la Constitución Política de la Republica indica: “La Junta Monetaria tendrá a su cargo la determinación de la política monetaria, cambiaria y crediticia del país

y velará por la liquidez y solvencia del sistema bancario nacional, asegurando la estabilidad y el fortalecimiento del ahorro nacional.” (p.28).

2.2.1 Clasificación del Sistema Financiero

Por su regulación el Sistema Financiero guatemalteco se divide en:

- Regulado o Formal
- No Regulado o informal

Está integrado por instituciones legalmente constituidas, autorizadas por la Junta Monetaria y fiscalizadas por la Superintendencia de Bancos. Se integra por el Banco Central (Banco de Guatemala), los bancos del sistema, las sociedades financieras, las casas de cambio y los auxiliares de crédito (almacenes generales de depósito, seguros y fianzas) (BANGUAT, 2019, s.p).

2.2.1.1 Junta Monetaria

Conforme lo establecido en el artículo 132 de la Constitución Política de la República de Guatemala, la Junta Monetaria se integra con los siguientes miembros:

a) “El Presidente, quien también lo será del Banco de Guatemala, y es nombrado por el presidente de la República y por un período establecido en la Ley;
b) Los Ministros de Finanzas Públicas, Economía y Agricultura, Ganadería y Alimentación;
c) Un miembro electo por el Congreso de la República;
d) Un miembro electo por las asociaciones empresariales de comercio, industria y agricultura;
e) Un miembro electo por los presidentes de los consejos de administración o juntas directivas de los bancos privados nacionales; y,
f) Un miembro electo por el Consejo Superior de la Universidad de San Carlos de Guatemala.

Todos los miembros de la Junta Monetaria tienen suplentes, salvo el presidente, a quien lo sustituye el vicepresidente y los Ministros de Estado, que son sustituidos por su respectivo viceministro". (p. 27)

2.2.2 Reglamentos y normas

Según el Decreto No. 19-2002 del Congreso de la República Ley de Bancos y Grupos Financieros, Artículo 55 establece:

La norma con la administración de riesgos y establece que los bancos y las empresas que integran grupos financieros, deberán contar con procesos integrales que incluyan, según el caso, la administración de riesgos de crédito, de mercado, de tasas de interés, de liquidez, cambiario, de transferencia, operacional y otros a que estén expuestos, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos. (p. 22)

Resolución JM-56-2011 Reglamento para la Administración Integral de Riesgos. Este reglamento tiene por objeto regular los aspectos mínimos que deben observar las entidades, con relación a la administración integral de riesgos.

Otras normativas relacionadas con riesgos:

- Resolución JM-93-2005 Reglamento para la Administración del Riesgo de Crédito.
- Resolución JM-117-2009 Reglamento para la Administración del Riesgo de Liquidez.
- Resolución JM-134-2009 Reglamento para la Administración del Riesgo Cambiario Crediticio.
- Resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

2.2.3 Iniciativa de Ley contra la ciberdelincuencia

La ciberdelincuencia es un tema que ha adquirido importancia gubernamental a lo largo de los años; sin embargo, no se ha llegado a un acuerdo para consensuar la creación de

una ley. El problema es que sin una legislación sobre la delincuencia cibernética se vuelve complicado el procesamiento de los casos (Periódico Digital Centroamericano y del Caribe, 2015, s.p).

El primer intento se da en el 2017 con el proyecto de ley 5254, «Ley de ciberdelincuencia», el cual traía engarzado un peligrosísimo artículo que pretendía poner un bozal a casi cualquier persona que osara criticar a las autoridades (Valdizán. 2019, s.p).

El segundo intento se lleva a cabo en el 2018 con la iniciativa 5339, «Ley contra actos terroristas», La cual también traía un artículo similar, con la única diferencia de que pretendía llamar «terrorista cibernético» a prácticamente cualquier ciudadano que hiciera ejercicio a su derecho a la libre emisión del pensamiento en redes sociales (Valdizán. 2019, s.p).

Según analistas de la iniciativa de Ley de prevención y protección contra la ciberdelincuencia indican:

> Honestamente no pensé que lo harían una tercera vez, pero sin duda, en este país todos somos recurrentes… ¡O necios! La nueva iniciativa 5601 «Ley de prevención y protección contra la ciberdelincuencia», no solo atenta contra el hacking ético que es tan necesario para comprobar los sistemas de seguridad y prevenir ataques cibernéticos, sino que nuevamente pone en peligro la libre emisión del pensamiento, esta vez castigando el «acoso», el cual, a falta de una definición exacta, puede ser cualquier cosa. Especialmente si de criticar a las autoridades de turno se trata. (Valdizán. 2019, s.p).

2.2.4 Regulaciones internacionales

Se establece que el colapso que ocurrió en el año 1974 del Bankhaus Herstatt en Alemania y del Franklin National Bank en Estados Unidos exhortó a los gobernantes de

10 bancos centrales a crear el Comité de Basilea para Supervisión Bancaria (Hoyos, 2008, s.p).

Este acontecimiento se dio según investigación durante el año 1988 el Comité de Basilea, emitió el Acuerdo de Capital de Basilea, introduciendo un marco de trabajo que se convirtió en un estándar globalmente aceptado. La mayoría de países en el mundo, adoptaron las recomendaciones emitidas por el BIS en el acuerdo de 1988. Una revisión de este acuerdo de capital en el 2004, conocido como Basilea II, incluyó en sus estándares el riesgo operativo (Hoyos, 2008, s.p).

2.2.4.1 Basilea I

Con el nombre de Basilea I se conoce al acuerdo publicado en 1988, en Basilea, Suiza, por el Comité de Basilea, compuesto por los gobernadores de los bancos centrales de Alemania, Bélgica, Canadá, España, EE.UU., Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza. Se trataba de un conjunto de recomendaciones para establecer un capital mínimo que debía tener una entidad bancaria en función de los riesgos que afrontaba (Basilea I, 1968, s.p).

El primer acuerdo de capital de Basilea ha jugado un papel muy importante en el fortalecimiento de los sistemas bancarios. La repercusión de ese acuerdo, en cuanto al grado de homogeneización alcanzado en la regulación de los requerimientos de solvencia ha sido extraordinaria. Entró en vigor en más de 130 países. (Gonzales, 2012).

Bank for International Settlements, (1988), establece que:

> El Comité constituye un foro de debate para la resolución de problemas específicos de supervisión y coordina la distribución de las competencias supervisoras entre las autoridades nacionales, a fin de garantizar una supervisión eficaz de las actividades bancarias en todo el mundo. El propósito es mejorar las normas de supervisión, particularmente respecto a la solvencia, a fin de reforzar la solidez y estabilidad de la actividad bancaria a nivel internacional. (s.p)

La estructura de ponderación de riesgo se ha elaborado de la forma más simple posible; se utilizan únicamente cinco niveles de ponderación: 0, 10, 20, 50 y 100%. No obstante, pueden existir distintos juicios al decidir qué ponderación debe aplicarse a los diferentes tipos de activos para propósitos de valuar el mercado de instrumentos diferentes. El acuerdo establecía que el capital mínimo de la entidad bancaria debía ser el 8% del total de los activos de riesgo crédito, mercado y tipo de cambio sumados. (Ocaña, 2008, s.p)

2.2.4.2 Basilea II

El nuevo acuerdo no sólo perfecciona aspectos considerados en Basilea II (1999), sino que también incorpora nuevos elementos a ser tomados en cuenta, basándose en tres pilares que se refuerzan mutuamente: requerimientos de capital, acción de los organismos supervisores y disciplina del mercado. (s.p)

El primer pilar tiene como objetivo:

> Establecer los mecanismos para determinar los requerimientos mínimos de capital sobre la base de los riesgos de crédito, de mercado y operativo; este último no considerado en Basilea I. Mientras Basilea I ha sido diseñada para bancos con actividad internacional y para los entonces 10 países representados en el Comité de Basilea, más de 130 países lo han adoptado. Además, cuenta con el reconocimiento del Fondo Monetario Internacional y del Banco Mundial como buena práctica internacional. (Basilea II, 1999, s.p)

En lo que respecta al riesgo de crédito, el acuerdo propone tres alternativas para su determinación:

> El primero de ellos, en su mecánica, es similar con lo establecido en Basilea I (ponderación preestablecida según riesgo para los distintos tipos de activos), pero presenta mejoras que lo hace más sensible al riesgo e incorpora el uso de clasificaciones externas efectuadas por agencias especializadas. Los otros dos métodos (no considerados en Basilea I) se basan en mediciones internas realizadas por los propios bancos. El nuevo marco trata de ser más sensible al

> riesgo que el anterior, por lo que el Comité ha puesto más énfasis en el papel que juegan el examen del supervisor y la disciplina de mercado (Basilea II, 1999, s.p).

“La medición del riesgo de mercado no tiene variación en relación con Basilea I y su propósito es determinar las exigencias de capital producto de los riesgos de tasas de interés, tipo de cambio y precio de bienes transables” (Basilea II, 1999, s.p).

No obstante, lo anterior, es importante indicar que, en última instancia, es responsabilidad de la administración de los bancos la de manejar adecuadamente los riesgos a los que están expuestos y asegurar que el capital mantenido sea adecuado a su perfil de riesgo. Con el objetivo de lograr una mayor sensibilidad al riesgo, el Comité propone un enfoque estándar de las exigencias de capital por riesgo crediticio (Basilea II, 1999, s.p).

Para atender el objetivo de resaltar la importancia de las evaluaciones internas de los riesgos a los que se exponen los bancos, se propuso un nuevo marco fundamentado en la calificación interna del riesgo de crédito. Reconociendo más elementos en el cálculo del capital regulador del riesgo crediticio, tales como la solvencia del deudor, la estructura y concentración de préstamos a un prestatario o grupo de prestatarios (Basilea II, 1999, s.p).

El pilar I constituye el núcleo del acuerdo e incluye una serie de novedades con respecto al anterior: tiene en cuenta la calidad crediticia de los prestatarios (utilizando ratings externos o internos) y añade requisitos de capital por el riesgo operacional.

El riesgo operacional se calcula multiplicando los ingresos por un porcentaje que puede ir desde el 12% hasta el 18%. Existen 3 métodos alternativos para calcularlo dependiendo del grado de sofisticación de la entidad bancaria (Método del Indicador Básico, Método Estándar y Métodos de Medición Avanzada) (Basilea II, 1999, s.p).

Por último, la definición de capital regulatorio disponible permanece casi igual a la de Basilea I. Hay que advertir una objeción en este cálculo del riesgo: que se ignora los

efectos agravantes / mitigantes de la concentración / diversificación de riesgos (estructura de correlación probabilística entre las diversas exposiciones). Ésta es una de las principales diferencias entre capital regulatorio y Capital Económico (Basilea II, 1999, s.p).

El segundo pilar se centra:

> En las atribuciones y responsabilidades de los organismos reguladores para efecto de fiscalizar la correcta aplicación de los métodos de determinación del capital, en especial cuando ésta se base en mediciones internas de las instituciones financieras. (Basilea II, 1999, s.p)

Finalmente, el tercer pilar se refiere a:

> La necesidad de contar con mecanismos de divulgación de la información respecto a la metodología utilizada para la determinación de los riesgos, de manera que los agentes del mercado se encuentren debida y oportunamente informados. (Basilea II, 1999, s.p)

2.2.4.3 Basilea III

Derivado de la última crisis financiera derivada de las carteras de crédito subprime, se ha visto que no han sido suficientes los actuales requerimientos de capital, el cual se nombró como Basilea III. Más de un banco en los mercados emergentes está testeando en estos momentos si las muy recientes propuestas del Grupo de Gobernadores Supervisores del Comité de Basilea -sobre capacidad de absorción de pérdidas no esperadas- los dejarían fuera de juego (Trujillo, 2015, s.p).

Es que el Basilea III es duro para muchas instituciones financieras, pero muchísimo menos impactante que lo que se esperaba gracias a los esfuerzos de los lobbies bancarios. Para la mayoría de los mercados latino y centroamericanos los nuevos requerimientos para fortalecimiento patrimonial tienen algunos perfiles extraños ya que las regulaciones vigentes en éstos no exigen ratios patrimoniales de mayor acidez,

aunque sí desde hace años se han ajustado a las exigencias de mantener una relación de suficiencia patrimonial mayor o igual al mínimo de 8% ratificado por el Basilea II del 2004 (en Ecuador 9%, Guatemala y Costa Rica 10%, El Salvador 12%).

En los países desarrollados, no sólo se observa el estándar general de 8% como relación mínima entre patrimonio técnico (capital base, capital económico, fondo patrimonial, otros) y los activos ponderados por riesgos (RWA), sino también requerían el mantenimiento por parte de las instituciones de una proporción de 2% entre el valor de Acciones Comunes y los RWA. 48 (Basilea II, 2010, s.p).

Asimismo, exigían un coeficiente mínimo de 4% para el cociente entre el saldo del Tier 1 (en general, la sumatoria del capital pagado más reservas más utilidades retenidas y otras cuentas de alto poder absorbente) y los RWA. Las nuevas propuestas llevan dichos índices al 4.5% y 6% respectivamente, tratando así de incrementar la capacidad de la banca para hacer frente situaciones de estrés. Estas modificaciones debieron ser implementadas a partir del 2015, comenzándose con un período de transición y testeo a partir del 2018 (Caruana, 2019, s.p).

2.2.5 Otras regulaciones internacionales

Internacionalmente, el marco de trabajo de COBIT y todos los productos y publicaciones relacionados que emitió el ITGI, guía a las organizaciones en la implementación de un adecuado gobierno de TI que garantice el cumplimiento de los objetivos del negocio por medio del valor agregado que debe brindar la tecnología de información, la administración de los riesgos y recursos y la medición del desempeño (Sans, 2004, s.p).

Además, integra estándares internacionales generalmente aceptados como COSO, ITIL, ISO 9001, ISO 27002, AS/NZ 4360:8 2004, etc., que lo convierten en un marco de trabajo completo y alineado con las mejores prácticas relativas a la tecnología de información. El presente trabajo se orienta a buscar una solución, adoptando para ello las mejores

prácticas que el marco de trabajo de COBIT 4.1 puede aportar en ese tema (Sans, 2004, s.p).

2.2.6 Requisitos que deben cumplir los bancos

En el Acuerdo de Capital de 1988, se establece la primera definición internacionalmente aceptada del capital bancario, así como una medida mínima del mismo. El Comité de Basilea diseñó el Acuerdo de 1988 como una norma sencilla para que pudiera ser aplicada a muchos bancos en muchas jurisdicciones diferentes (Basilea II, 1999, s.p).

Según el Acuerdo, los bancos deben dividir sus riesgos en “clases” generales de tipos parecidos de prestatarios. Las exposiciones al mismo tipo de prestatarios como las exposiciones a prestatarios empresariales están sujetas al mismo requerimiento de capital, independientemente de las posibles diferencias que puedan existir en la solvencia y riesgo de cada prestatario individual. (Basilea II, 1999, s.p).

A raíz de los avances de las prácticas de gestión de riesgos, de la tecnología y de los mercados bancarios, el método tan sencillo de medición del capital del Acuerdo de 1988 ha perdido el sentido para muchas organizaciones bancarias ya que, por ejemplo, se establecen exigencias de capital sobre la base de clases generales de riesgos y no distingue entre los grados relativos de solvencia de los prestatarios individuales.

Asimismo, las mejoras de los procesos internos, la adopción de técnicas de medición de riesgos más avanzadas y el creciente uso de prácticas complejas de gestión de riesgos, tales como, la titularización, han cambiado el seguimiento y la administración de riesgos y actividades de las principales organizaciones bancarias. (Basilea II, 1999, s.p).

2.3 Definición de riesgos financieros

Para efectos del presente trabajo de investigación, se trata únicamente lo relacionado con los riesgos económico financieros, entendiéndose como tales, a la pérdida de valor económico.

Se entiende por riesgo a la posibilidad de que eventos anticipados o no, puedan tener impacto adverso contra los ingresos y el patrimonio de las entidades bancarias. En economía se define el riesgo como el conjunto y peligros que debe afrontar el empresario para conseguir beneficios en su actividad o la probabilidad de no obtener el resultado esperado (Ulrich, 1998, s.p).

Nicholas (1999) comenta:

> En un banco se considera que el riesgo aparece cuando la entidad asume, mediante la intermediación la responsabilidad de cumplir sus obligaciones con los ahorristas e inversores, lo que va a depender en gran medida de la amortización a tiempo y en forma de los deudores bancarios. Riesgo que asume al financiar a terceros. Para el mercado financiero se define como la imputación de riesgo de un activo financiero en concreto respecto del riesgo de una cartera diversificada, depende de cómo reacciona el rendimiento de ese título a una subida o bajada general de todo el mercado. (s.p)

2.3.1 Riesgo operacional

Este riesgo tiene su justificación en la pérdida potencial derivada de deficiencias significativas en la integridad o confianza del sistema. Las consideraciones de seguridad son importantes, en la medida en que los bancos pueden ser sujetos de ataques externos o internos sobre sus sistemas o productos. El riesgo operacional puede también surgir de un mal uso del cliente, de un diseño inadecuado o de un sistema de banca electrónica mal implantado (Ulrich, 1998, s.p).

2.3.2 Riesgos implícitos en la banca en internet

Feria (2018) expone que:

> Debido a los rápidos cambios en las tecnologías de la información, la lista de riesgos que afectan a la banca electrónica no puede ser exhaustiva. Sin embargo, sí podemos describir un grupo de riesgos, suficientemente significativo, que nos permita diseñar una guía general de apoyo a la gestión de los mismos. (s.p)

Hay que advertir que los tipos básicos de riesgo generados en la banca electrónica no son nuevos; la novedad estriba en la forma específica bajo la cual estos riesgos surgen, así como la magnitud de su impacto (Lima, 1984, s.p).

En este sentido, las categorías de riesgo más importantes para la banca electrónica, especialmente para la banca internacional diversificada son: riesgo operacional y de este subdividirse en otros riesgos (Lima, 1984, s.p).

2.3.2.1 El riesgo de seguridad informática

El riesgo operacional se encuentra en estrecha relación con el control sobre el acceso a los sistemas de gestión de riesgo y a la contabilidad de un banco. Este control de acceso a los sistemas bancarios se ha convertido en algo tremendamente complejo debido a los avances informáticos, a la dispersión geográfica de los puntos de acceso, y al uso de vías alternativas de comunicación, incluyendo las redes públicas como Internet. (Lara, 2013, s,p).

A pesar de que la banca en Internet se encuentra implantada en España, sin embargo, la seguridad constituye una de las barreras de entrada para los clientes potenciales. El usuario aún no confía en las medidas de seguridad existentes como, por ejemplo, la encriptación de datos, aunque todo es cuestión de tiempo y de acostumbrar a los clientes a estos canales de distribución (Lara, 2013, s,p).

Lo cierto es que los accesos no autorizados, ya sean realizados por piratas informáticos (hackers) o por empleados del banco (insiders), pueden dar lugar a pérdidas directas debido al uso y manipulación de información confidencial del cliente. Por esta razón, es preciso diseñar sistemas que aseguren la confidencialidad e integridad de cualquier transacción y garanticen la privacidad de la información (Lara, 2013, s,p).

2.3.2.2 Diseño de banca electrónica

Un banco afronta el riesgo de que el sistema por él elegido no se encuentre bien diseñado o implantado. Por ejemplo, un banco está expuesto al riesgo de una interrupción de su sistema de banca electrónica si éste no es compatible o no satisface los requerimientos de sus usuarios.

Muchos bancos delegan en suministradores de servicios externos y expertos (outsourcing) la operativa y el mantenimiento de sus actividades de banca electrónica. Esta delegación puede ser conveniente porque permite al banco desprenderse de aspectos que no puede suministrar de forma eficiente por sí mismo. Sin embargo, el outsourcing expone al banco al riesgo operacional, en la medida en que los proveedores de servicios pudieran no estar tecnológicamente preparados para prestar los servicios esperados o fallar en la actualización de su tecnología. Si esto ocurriera la reputación bancaria se vería seriamente dañada (Télles, 1996, s.p).

Hay que añadir que, debido a los rápidos cambios que se suceden en las tecnologías de la información, los bancos se enfrentan también al riesgo de obsolescencia de su sistema. Por ejemplo, el software empleado por la banca electrónica requiere de una actualización constante; al mismo tiempo, los canales de distribución de las actualizaciones de software plantean problemas de seguridad para los bancos, ya que pudieran ser interceptados y manipulados. Además, no debemos olvidar una dificultad añadida que estriba en la continua asimilación de las nuevas tecnologías por el banco y su personal (Télles, 1996, s.p).

2.3.2.3 Pérdidas financieras para una institución bancaria

Los malos usos de los clientes, tanto intencionados como inadvertidos, constituyen otra de las fuentes de riesgo operacional. El riesgo puede ser mayor si el banco no "educa" adecuadamente a sus clientes sobre las precauciones de seguridad. Además, en ausencia de medidas adecuadas para verificar las transacciones, los clientes podrían anular operaciones que, previamente, autorizaron, dando lugar a importantes pérdidas financieras para el banco (Hidalgo, 2014, s.p).

El uso personal de información del cliente (como por ejemplo la verificación de información, número de las tarjetas de crédito, número de las cuentas bancarias, etc.) en una transmisión electrónica carente de seguridad permitiría a un experto (hacker) tener acceso directo a las cuentas de los clientes. Consecuentemente, el banco podría incurrir en pérdidas financieras debido a transacciones de clientes no autorizados. (Hidalgo, 2014, s.p).

2.3.3 El riesgo tecnológico

Del Campo (2015) expone:

> Que el riesgo tecnológico se mide en relación con el nivel de efectividad de las medidas adoptadas por las Instituciones en la gestión de la seguridad para contrarrestar el continuo incremento de la vulnerabilidad en las herramientas y aplicaciones tecnológicas. (s.p)

Es una realidad que la infraestructura y las aplicaciones tecnológicas están siendo blancos de ataques debido a vulnerabilidades existentes ya sea por no contar con medidas de protección apropiadas o por el cambio constante, factores que hacen cada vez más difícil mantener actualizadas las medidas de seguridad (Campo, 2015, s.p).

Un aluvión de ataques cibernéticos dañinos está sacudiendo a empresas y organizaciones a nivel mundial al punto que ya no están asumiendo que pueden

mantener a raya a los piratas informáticos y en lugar de eso, han pasado a librar una guerra de guerrillas desde el interior de sus redes (Campo, 2015, s.p).

Según Gartner (2015) el:

> Gasto mundial en seguridad informática fue muy superior a los 70,000 millones de dólares en el 2014. ABI Research estima que el gasto en seguridad cibernética sólo en infraestructura crítica en los bancos, las empresas relacionadas con la energía y el sector militar, llegará a los 109,000 millones de dólares para el año 2020. Como ejemplo, las empresas españolas vienen gastando unos 14,000 millones de euros al año en reforzar su ciberseguridad. (s.p)

2.3.4 Fraude

La Federación Internacional de Contadores según sus siglas IFAC (2016). “Es acción intencional que realizan una o varias personas de la entidad, ya sea los empleados, terceros o hasta la misma gerencia que conlleve a la utilización del fraude con el objetivo de conseguir ventaja injusta o ilegal” (s.p)

RAE –Real Academia Española (1979) “Del latín fraus, fraudis. Es la Acción opuesta a la sinceridad y rectitud el cual afecta a la persona contra quien se comete dicho acto.” (s.p)

2.3.4.1 Fraude laboral

Asociación de Examinadores de Fraude (2013) “es la acción de Aprovechar el puesto de trabajo obtenido para enriquecerse por medio del uso indebido o el mal empleo de los recursos activos de la organización empleadora” (s.p).

La triada del fraude está constituida por tres elementos básicos que son:

Motivación: Se produce por las necesidades de factores económicos que afectan a la familiar del defraudador ya sea que esta necesidad sea real o artificial. (Cressey, 1987, s.p)

Racionalización: Se da cuando el defraudador busca justificar su accionar con una justificación psicológica para no verse como un delincuente. En su interior el conoce y diferencia bien y del mal de sus actos. (Cressey, 1987, s.p)

Oportunidad: Se da cuando el defraudador percibe la oportunidad de ejecutar el fraude sin que sea descubierto, por ello idealiza como ejecutar el delito usando y abusando de su posición de confianza y poder. (Cressey, 1987, s.p)

2.3.4.2 Sistema de información para la prevención del fraude

Este sistema de información busca prevenir y controlar el fraude a través de la identificación de cuentas individuales y mancomunadas del personal que labora en dicha entidad, si se realiza esta operación financiera inmediatamente el sistema que se está aportando bloqueara la ejecución. (RAE, 2018, s.p)

2.3.4.3 Ataques al sistema financiero

El sector financiero constituye el objetivo prioritario de los cibercriminales, hasta el punto de que cerca de la mitad de los ciberataques afectan a este sector. Las amenazas y ataques que experimentan diariamente ya no solo proceden de individuos deseosos de quebrar la seguridad de un Banco, como los hackers, sino que se está convirtiendo en práctica habitual también de cibercriminales que buscan lucro económico, así como de ciber terroristas que tratan de atentar contra la seguridad de una Institución, o del ciber espionaje entre entidades financieras (Molina, 2001, s.p).

Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de las vulnerabilidades y los riesgos a los que se exponen las organizaciones (Molina, 2001, s.p).

Todo esto lleva a crear una estrategia Institucional que dimensione el riesgo tecnológico desde tres aspectos: a nivel de la infraestructura tecnológica (redes, recursos de hardware y acceso físico), a nivel lógico (riesgos asociados al software, aplicaciones y los datos), a nivel de los riesgos derivados del mal uso que hace el recurso humano de lo anterior (Molina, 2001, s.p).

Es fundamental que las Instituciones analicen los aspectos anteriores y que elaboren un mapa de riesgo que documente las posibles causas de riesgo tecnológico, así como sus efectos y que mitigue de forma eficiente y efectiva las amenazas procedentes de entornos como la movilidad, la computación en la nube y los medios sociales (Serrahima, 2010, s.p).

2.3.5 Privacidad tecnológica

Carrocera (2017) se refiere:

> A la importancia de la privacidad la cual se remonta a los inicios de la humanidad y ha adquirido mayor importancia desde la revolución industrial hasta transformarse en el principal activo de las personas y empresas en la sociedad de la información contemporánea. Acción: Los datos personales y financieros deben almacenarse de manera segura y todas las comunicaciones con el sistema de Banca en Línea deben estar encriptados. Esto asegura la confidencialidad de los datos desde los sistemas del Banco hasta el navegador del cliente. También debe ofrecerse un servicio que permita intercambiar correo electrónico, de manera segura. (s.p)

Los avances tecnológicos en la actualidad, cuando hablamos de privacidad, ya no podemos hablar solamente de cuidar el interior de nuestras cosas u oficinas con cristales

oscuros para evitar que se vea de afuera. Estamos en un mundo donde la mayoría de las personas porta una cámara y un micrófono a donde vaya, estamos hablando de los dispositivos móviles (Carrocera, 2017, s.p).

Sumado a esto, se debe tener presente que ni los propios usuarios saben quién más tenga acceso a su información almacenada. Como pueden ser agencias de mercadotecnia, Estados, anunciantes, cibercriminales o hackers, entre otros. Por esto, Internet y la hiperconectividad han revolucionado también las cuestiones de privacidad y seguridad (Carrocera, 2017, s.p).

2.3.5.1 Certificados Digitales

Acción: Las páginas Web deben hacer uso de certificados de validez extendida (EV - Extended Validity) para comprobar la identidad de los visitantes. Estos certificados requieren de una verificación exhaustiva y proporcionan el más alto nivel de confianza del usuario con respecto a la autenticidad del sitio Web (Piloña, 2012, s.p).

2.3.5.2 Verificación de identidad

Acción: Para obtener un nivel más alto de seguridad, el sistema de Banca en Línea debe requerir dos niveles de autentificación para acceder a las cuentas bancarias (Piloña, 2012, s.p).

2.3.6 El usuario y contraseña

Una contraseña de un solo uso (one-time password) generada automáticamente. Este segundo paso previene un acceso no autorizado en el caso de que un Usuario/Contraseña haya sido comprometido (Piloña, 2012, s.p).

2.3.6.1 Bloqueo de cuenta y finalización de sesión

Acción: para proteger los datos contra intentos de adivinar una contraseña, la cuenta será bloqueada si la contraseña (o el código del token) son introducidos erróneamente cuatro veces consecutivas. Además, una sesión bancaria en línea debe desconectarse automáticamente después de doce minutos de inactividad (SIB, 2018, s.p).

2.3.6.2 Identidad del sitio web

Los usuarios reciben correos electrónicos que aparentemente son enviados por la institución y q que generalmente solicitan que se sigan ciertos enlaces para conectarse a su cuenta en línea para resetear la contraseña u otras acciones similares. Generar una campaña de correos electrónicos que adviertan al usuario del riesgo de responder a este tipo de correos (SIB, 2018, s.p).

2.4 Actividad de las entidades bancarias

Monroy (2016) indica:

> La principal actividad de las entidades bancarias es la crediticia, la cual le genera la mayor parte de sus beneficios y consecuentemente está sujeta a una serie de riesgos y es que normalmente la palabra riesgo tiene una connotación negativa algo que debemos evitar; sin embargo, el negocio bancario supone precisamente eso, la gestión de riesgos con el objetivo de obtener una rentabilidad que compense adecuadamente el capital invertido. (s.p)

2.4.1 Transacciones electrónicas en Guatemala

El mundo se ha convertido en una plataforma digital para realizar prácticamente cualquier tipo de transacciones. Desde la compra electrónica de arte, hasta convertir el dinero en digital para usos que nunca antes imaginamos, tales como el pago de servicios y la adquisición de productos de consumo diario (SIB, 2018, s.p).

Para comprender y analizar los términos que dominan en este momento las transacciones digitales es necesario primero definirlos y entender sus diferentes significados.

2.4.1.1 Dinero electrónico, banca móvil y servicios financieros móviles

El dinero electrónico es una transformación o digitalización del dinero físico en electrónico, que se origina al momento de la recepción de los fondos entregados por el usuario a la entidad por un monto y con un valor igual al dinero electrónico creado. En este sentido, está respaldado 1 a 1. Dicho valor monetario se refleja en un dispositivo móvil, que pueden ser teléfonos celulares, computadoras, tarjetas, entre otros. Luego de ser transformado se acepta como medio de pago por otras partes (comercios, personas, servicios, etc.) que no sean el emisor, con la capacidad de que se pueda convertir en efectivo nuevamente (SIB, 2018, s.p).

En el caso de la banca móvil, es necesario el uso de cualquier dispositivo electrónico para tener acceso a servicios bancarios y llevar a cabo operaciones financieras; a menudo este término se utiliza para hacer referencia a clientes con cuentas bancarias. Constituye un canal de banca electrónica que incluye una amplia gama de instrumentos y canales bancarios en donde cada cliente requiere una cuenta bancaria, convirtiéndolo en un servicio exclusivo para los bancos (SIB, 2018, s.p).

Los servicios financieros móviles, incluyen tanto la banca móvil como los pagos móviles con dinero electrónico. No es necesario que los clientes requieran o dispongan de una cuenta bancaria, ya que este servicio puede ser ofrecido por instituciones diferentes a los bancos del sistema.

2.4.1.2 Beneficios ofrece el dinero digital

Los beneficios son altísimos, al incrementar la inclusión financiera hasta en un 20%, esto es un incremento del 38% al 58% a nivel poblacional, así como el potencial de incrementar el PIB hasta 3% es inminente. También crea canales que dan acceso al desembolso de créditos para micro y pequeños empresarios. Contribuye de la misma manera a la formalización de remesas y pagos, por consecuencia aumenta la recolección del IVA (Impuesto al Valor Agregado) sobre transacciones que anteriormente no eran visibles (SIB, 2018, s.p).

Contribuye a la visibilidad y trazabilidad de transacciones, reduciendo los costos de impresión, manejo de efectivo y monitoreo de transacciones para la prevención del lavado de dinero (SIB, 2018, s.p).

2.4.2 Educación financiera

Esto es sumamente necesario en sociedades como las nuestras. La educación en cuanto a seguridad, uso y administración del efectivo puede llevar a aumentar la calidad de vida de los consumidores y lograr un acceso cada vez más amplio a servicios financieros más sofisticados como seguros de vida, desembolso de créditos, entre otros. Es de suma importancia y es necesaria llevarla a la acción (SIB, 2018, s.p).

2.4.2.1 Dinero digital con el esquema financiero actual

El mundo bancarizado está conectado con el no bancarizado, lo que sucede es que esta conexión no la vemos porque sucede en efectivo, ocurre a diario. Tener sistemas abiertos e interoperables permite un dinamismo de la adopción del dinero digital. Entre más abiertos e inter-operables sean los sistemas, la industria del dinero digital crecerá, permitiendo la entrada de nuevos jugadores y dinamizando la industria. Para esto es necesario crear alianzas estratégicas con instituciones financieras adquirentes para promover créditos, seguros, soluciones de pagos y cobranzas a pequeños comercios,

con el fin de generar un ecosistema financiero más amplio en donde todos ganan. (Schnier, 2000, s.p).

2.4.2.2 Industria del dinero digital

Se necesita de un apoyo integral y específico que abarque otras empresas diferentes al sistema bancario tradicional. Es necesario que fomente la inter-operatividad y colaboración entre los distintos actores y que permita la formalización sostenida de la población no bancarizada (Salellas, 2012, s.p).

2.4.3 Administración del riesgo

Es una herramienta importante para combatir el lavado de dinero y la financiación al terrorismo pues todas las transacciones reflejan una trazabilidad y son susceptibles de ser monitoreadas y parametrizadas para generar alertas. Contribuye a aplicar estándares internacionales y controles adecuados al tipo de transacción. Se generan políticas de identificación al cliente, validaciones de transacciones, esquemas preventivos y alarmas por operaciones sospechosas, esto ayuda a identificar y prevenir posibles fraudes en el uso del dinero electrónico para actividades no lícitas. Un modelo de negocio basado en riesgo genera la confianza al consumidor y al sistema (Salellas, 2012, s.p).

2.5 Phishing

Cardoso (2017) indica que;

> La palabra phishing proveniente del inglés con que se ha descrito a los robos de identidad realizados por correo electrónico y teléfono, en el que el estafador se hace pasar por una entidad o empresa prestataria de servicios al individuo en cuestión, de manera que este último le confíe al primero información personal sobre cuentas bancarias, contraseñas, y datos similares, también se le conoce como brand spoofing y/o carding. (s.p)

2.5.1 El término phishing

Cardoso (2017) expone:

> Que el término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). (s.p)

El término phishing proviene de la palabra inglesa fishing (pesca), haciendo alusión al intento de hacer que los usuarios "piquen en el anzuelo". A quien lo practica se le llama phisher. También se dice que el término "phishing" es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que el dígrafo 'ph' es comúnmente utilizado por los hackers para sustituir la 'f', como raíz de la antigua forma de hacking telefónico conocida como phreaking. (Salellas, 2012, s.p).

2.5.1.1 Técnicas de phishing

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor. Direcciones URL mal escritas o el uso de subdominios son trucos comúnmente usados por phishers, tales como www.nombredetubanco.com/ejemplo. Otra forma para disfrazar enlaces es el de utilizar direcciones que contengan el símbolo de la arroba (@), para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares), como en el enlace www.google.com[arroba]members.tripod.com puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente) (Schnier, 2000, s.p).

Este método ha sido erradicado desde entonces en los navegadores de Mozilla e Internet Explorer. Otros intentos de phishing utilizan comandos en JavaScripts para alterar la barra de direcciones. Otro método de phishing muy extendido es el Cross Site Scripting, en que el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos (Cisco Systems, Inc., 2014, s.p)

En este método de ataque los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, siendo muy difícil de detectar si no se tienen los conocimientos necesarios. Otra técnica de ataque de phishing es el llamado IDN spoofing (o también ataques homógrafos), relacionado con el manejo del Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo, dominio.com se ve similar a dominio.com, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega ómicron "o") (Cisco Systems, Inc., 2014, s.p)

Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. El phishing también ha dado lugar al lavado de dinero.

2.5.1.2 Anti-phishing

Se ha intentado detener la práctica del phishing recurriendo a varios métodos, desde el punto de vista técnico, legislativo, y también organizativo. Se han creado programas informáticos capaces de detectar los intentos de phishing en sitios web y correos electrónicos. Los filtros de spam también han ayudado a proteger a los usuarios de correo electrónico de los ataques de phishing. Leyes como la Anti-Phishing Act (Acta Anti-

phishing), aprobada en Estados Unidos en marzo de 2005, han intentado frenar el robo electrónico de identidad estableciendo altas multas, e incluso prisión. (APWG, 2017, s.p)

La compañía Microsoft (2019) indica:

> También ha implementado iniciativas en la lucha contra el phishing, llevando ante las cortes judiciales a muchos individuos que ha monitoreado intentando realizar estas prácticas. También se ha creado el Anti-Phishing Working Group, una asociación dedicada a aplicar leyes contra el phishing, surgida en el año 2003, que cuenta con el apoyo y la colaboración de más de mil agencias y compañías de seguridad informática en todo el mundo, entre las que se encuentran Symantec, McAfee, BitDefender, IronKey, VeriSign, y otras. (s.p)

2.5.2 Phishing en Guatemala

Guatemala es el segundo país más vulnerable a ataques por internet. Según el informe del (2016) sobre ciberseguridad del Banco Interamericano de Desarrollo y otros organismos, se calcula que el cibercrimen le cuesta al mundo hasta US$575 mil millones al año. En América Latina y el Caribe constituye alrededor de US$90 mil millones anuales.

Según el ESET Security Report (2016) nos indica que:

> Una encuesta reveló que las empresas que se vieron más afectadas por códigos maliciosos son las de Nicaragua, que ocupa el primer lugar, con el 58.3% de las warezing respuestas afirmativas; luego, Guatemala, con el 55.8%, y Ecuador, con 51.9%. Los países más afectados por casos de phishing son Ecuador (24%), Perú (22%) y Guatemala (20%). (s.p)

2.5.2.1 Políticas de seguridad informática

Es importante que cada organización cuente con un plan estratégico de políticas de seguridad informática, que sea capaz de resguardar y proteger la información y demás

recursos lógicos que representan valor para dicha organización. Además de eso, el plan de seguridad debe abarcar más allá de los recursos lógicos e intangibles; se deben tomar en cuenta los recursos físicos como computadoras, impresoras, fotocopiadoras y demás hardware que utilice la compañía, así como el inmueble en el que se trabaje y los recursos humanos (Cisco Systems, Inc., 2014, s.p)

Por lo tanto, al momento de pensar en crear un plan de seguridad para protección de la organización y todos los recursos que maneja, tanto lógicos como físicos, debe conocerse a profundidad cada elemento y su funcionamiento, así como todo lo que implica poseer dicho recurso, sus debilidades, vulnerabilidades, riesgos y el posible impacto que algún tipo de amenaza podría ocasionarle (Cisco Systems, Inc., 2014, s.p).

2.5.3 Amenaza informática

En informática, cualquier acción o evento que sea capaz de ocasionar algún daño sobre elementos del sistema o perturbaciones a la información, causando pérdidas materiales o lógicas, es conocido como una amenaza informática. Este tipo de vulnerabilidades puede presentarse en cualquiera de las partes que conforman una computadora (software, hardware) (Cisco Systems, Inc., 2014, s.p).

Muchas amenazas son inevitables e incluso no pueden ser pronosticadas, por lo que cada sistema informático debe contar con la protección necesaria para controlar el efecto de acción de una amenaza, según sea el tipo de sistema que se maneje.

Existe gran cantidad de amenazas para sistemas informáticos, formas en que pueden ser atacados, infectados o hasta sufrir robos de información. Es importante conocer la constitución de las amenazas y la figura 5 muestra la anatomía de las mismas. Las amenazas informáticas suelen mostrar muy poco o nada de los síntomas que ocasionan, por lo que pueden vivir sumergidas en el sistema durante un largo tiempo, sin ser detectadas (Cisco Systems, Inc., 2014, s.p).

2.5.4 Amenaza humana

Son todos aquellos seres humanos atacantes del sistema informático que buscan causar un daño significativo o llevar a cabo el robo de algún recurso; a estas personas comúnmente se les llama: hacker.

El término “hacker” se ha ido distorsionando con el pasar de los años y se cree que son personas con un profundo conocimiento sobre máquinas y que se aprovechan de ello para realizar estafas sobre cualquier organización. Sin embargo, hacker es en realidad una persona que vive aprendiendo y es paciente, indaga en aspectos minuciosos para alimentar sus conocimientos y todo lo ve como un reto, una meta por alcanzar. (Cisco Systems, Inc., 2014, s.p)

2.5.5 Ingeniería social

La ingeniería social, se refiere a todas las actividades tendientes a obtener la confianza de la víctima, en las que se entrega una serie de razones plausibles o incentivos idóneos en orden a que el receptor se forme la convicción de que el mensaje es verdadero y, por ende, entregue sin reservas sus datos. Algunas de las ingenierías sociales más destacables son las “actualizaciones de seguridad”. A modo de ejemplo, las supuestas empresas proveedoras de servicios online comunican a sus usuarios que se está introduciendo un nuevo servicio para aumentar la seguridad del consumidor y, de esta manera, evitar fraudes. Junto con ello, para activar el servicio es necesario que el usuario autentifique cierta información con lo que el phisher logra su cometido (Piloña, 2012, s.p).

Asimismo, otra clara manifestación de este mecanismo se encuentra con motivo de una supuesta “información de cuenta incompleta”, situación en la cual se les dice a los usuarios que los servidores poseen información obsoleta o incluso, que hay ciertos datos que se han perdido, por lo que para mantener el servicio es necesario que ingresen al sitio web indicado y actualicen la información solicitada (Piloña, 2012, s.p).

2.5.6 Importancia histórica de la seguridad de la información

Según el Informe sobre Investigaciones de Brechas en los Datos de Verizon (2016) se refiere a:

> La importancia de la seguridad de la información nació al mismo tiempo que se inició a transmitirse la información, desde cilindros de madera, tableros de sustitución de letras, cifrados alterando la posición que ocupaban los caracteres en el alfabeto, discos mecánicos de cifrado, hasta que hizo su aparición la tecnología para cifrar mensajes y aparece la maquina enigma durante la segunda guerra mundial. (s.p)

3. Metodología

La metodología contiene los criterios y procedimientos generales para guiar el trabajo profesional de graduación; y, las técnicas, reglas y operaciones para el manejo de instrumentos, en la aplicación del método científico de investigación. En general, son las herramientas metodológicas de investigación para la consecución de los objetivos formulados.

3.1. Definición y Delimitación del Problema

La definición del problema, presenta la especificación con la mayor claridad y precisión; además, incluye la presentación del tema y subtemas en forma interrogativa, así como la identificación del punto de vista con que se enfoca el problema.

En la República de Guatemala, las instituciones bancarias del sistema financiero que se dedican de servir a los usuarios, para el óptimo manejo de sus finanzas personales, al administrar el ahorro. Las instituciones bancarias, tienen la finalidad de administrar cuentas que generen rendimientos a los clientes que depositen allí su excedente de dinero.

El problema financiero del trabajo profesional de graduación identificado para el sistema bancario de Guatemala, se refiere al robo de información de clientes mediante phishing y por ende transferencias electrónicas ilícitas, lo que repercute en reclamos que generan pérdidas económicas además de desconfianza y mala publicidad a las instituciones bancarias guatemaltecas.

La propuesta de solución que se plantea al problema del trabajo profesional de graduación, riesgo financiero ante phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco consiste en la identificación del impacto financiero para la elaboración de mecanismos e instrumentos que puedan

prevenir y mitigar ataques de phishing en transacciones electrónicas en una entidad bancaria.

La delimitación se deriva de la especificación del problema, lo cual sirve de base para definir la unidad de análisis, el período y el ámbito geográfico que comprende la investigación.

3.1.1. Temas y Subtemas

Tema

- ¿Cuál es el impacto financiero por los ataques de phishing en transacciones electrónicas, en una entidad bancaria del sistema financiero de Guatemala, y qué mecanismos e instrumentos se pueden proponer para mitigar el robo de información a de clientes de una institución bancaria?

Subtemas

- ¿Qué impacto financiero tiene el riesgo tecnológico por robo de información a clientes de una institución bancaria y así elaborar estrategias de contingencia ante estos casos de phishing?

- ¿Cómo pueden reducirse los gastos no deducibles por incidentes de phishing con base a procesos y políticas administrativas que contengan instrucciones detalladas para el manejo de este, además de proponer tácticas de información a clientes con base en la forma de actuar de hackers que utilizan el phishing e informar las consecuencias de no tener los estándares mínimos de ciberseguridad?

- ¿Qué procesos se pueden proponer ante la forma de proceder en los reclamos de robo por medio de phishing, con base a investigación de los sistemas y canales

electrónicos, así como de hechos históricos para comprobar que se tenga la certeza que no sea una estafa elaborada? (ver numeral 4.5.2)

3.1.2. Punto de vista

Administración financiera.

3.2. Objetivos

Los objetivos constituyen los propósitos o fines del presente trabajo profesional de graduación relacionada con la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco.

3.2.1. Objetivo General

Determinar el impacto financiero en una institución bancaria ocasionado por defraudaciones por medio de phishing en transacciones electrónicas y elaborar mecanismos e instrumentos que puedan ayudar a mitigar los ataques de phishing con base en la implementación de nuevos procesos y políticas preventivas.

3.2.2. Objetivos Específicos

- Cuantificar el impacto financiero del riesgo tecnológico por robo de información a clientes de una institución bancaria y así elaborar estrategias de contingencia ante estos casos de phishing.

- Reducir los gastos no deducibles por incidentes de phishing con base a procesos y políticas administrativas que contengan instrucciones detalladas para el manejo de este, además de proponer tácticas de información a clientes con base en la forma de

actuar de hackers que utilizan el phishing e informar las consecuencias de no tener los estándares mínimos de ciberseguridad.

- Proponer procesos adecuados ante la forma de proceder en los reclamos de robo por medio de phishing, con base a investigación de los sistemas y canales electrónicos, así como de hechos históricos para comprobar que se tenga la certeza que no sea una estafa elaborada.

3.3. Diseño de la Investigación

Delgado (2016) señala que el método científico, se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando técnicas para minimizar la influencia de la subjetividad en el resultado del presente trabajo de investigación. Además, que gracias a él se pueden realizar leyes que nos permitan a los seres humanos conocer de manera correcta no sólo lo que fue el pasado sino también el futuro. Y es que, dándole determinados valores, sabremos qué le va a suceder a una variable. Por tanto, el método científico utiliza las matemáticas como clave fundamental para establecer las correspondientes relaciones entre las distintas variables. (s.p)

Aguilar (2015) indica que el método científico es el procedimiento planeado y sistematizado que se sigue en la investigación, para descubrir formas de existencia de la materia y sus procesos o fenómenos de la naturaleza, de la sociedad, y el pensamiento que determina leyes científicas, lo cual profundiza el conocimiento y sus fases son las siguientes:

- Indagatoria: que se utilizará para recolectar toda aquella información bibliográfica y de campo que es básica y necesaria para el desarrollo del plan de trabajo.
- Demostrativa: durante esta fase se comprobarán las variables de las hipótesis plasmadas en el plan de trabajo, por medio de las técnicas de investigación.
- Expositiva: siendo esta fase la parte final dentro del desarrollo de la investigación la

> cual deberá estar contenida dentro del informe final que se presentará y en él se plasmarán las propuestas de solución del problema actual. (pp. 35,39)

El método científico es el fundamento del presente trabajo profesional de graduación relacionado con la incidencia financiera por el riesgo operativo de phishing en transacciones electrónicas en una institución bancaria del sistema financiero guatemalteco.

El trabajo profesional de graduación fue diseñado con el planteamiento metodológico del enfoque cuantitativo, pues es el que mejor se adaptó a las características y necesidades de este trabajo.

El enfoque cuantitativo utiliza la recolección y análisis de datos para contestar preguntas de investigación y probar hipótesis establecida previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamientos en una población (Hernández, Fernández & Baptista 2014, p. 73).

Mediante el enfoque cuantitativo se tomó en cuenta la técnica estadística para medir la percepción de incidencias de phishing en transacciones electrónicas de una entidad bancaria del sistema financiero guatemalteco.

El estudio fue un diseño no experimental y transversal.

2.6 Técnicas de investigación

Las técnicas son reglas y operaciones para el manejo de los instrumentos en la aplicación del método de investigación científico. El trabajo profesional de graduación se fundamentó en la utilización de técnicas de investigación documental y de campo.

3.4. Unidad de Análisis

Un banco del sistema financiero de la República de Guatemala.

3.5. Período Histórico

Información financiera del año 2019.

3.6. Ámbito Geográfico

República de Guatemala.

3.7. Universo y Muestra

El universo corresponde a 16 bancos del sistema financiero regulado de Guatemala.

La muestra comprende un banco del sistema, que tiene casos de Phishing inmersos en la cuenta contable de Fraudes, específicamente en los apartados de Fraudes externos y reclamos de clientes.

3.8. Instrumentos Aplicados

Estos instrumentos se aplican directamente a las fuentes primarias, por lo que se hace necesario acudir al lugar donde ocurre el fenómeno para observarlo, describirlo y analizarlo, estableciendo las variables de causa y efecto, de las cuales podemos mencionar las siguientes:

- Observación directa: es un método de recolección de datos que consiste en observar al objeto de estudio dentro de una situación particular. Esto se hace sin intervenir ni alterar el ambiente en el que el objeto se desenvuelve. De lo contrario, los datos obtenidos no serían válidos. “Si el sujeto que observa está presente ante el fenómeno

(ordinaria); o si está involucrado (participa) del mismo.” (Nicuesa, 2015, s.p).

- Entrevista dirigida focalizada: “Define, con anterioridad, un tema esencial y específico sobre el que cuestiona profundamente. Es planificada, aunque las preguntas son abiertas.” (Nicuesa, 2015, s.p).

Se utilizó la entrevista dirigida focalizada en el área de digitalización y recepción de denuncias de phishing con el técnico encargado de visitar a clientes, la información recabada se describe en el caso de la señora Damaris Ruano en el capítulo cuatro, con el propósito de obtener información real y confiable a través de un interrogatorio verbal, utilizando instrumentos adecuados y un formulario estructurado de entrevista (guía), ver Anexo I.

4. Discusión de los Resultados

4.1. Institución objeto de análisis

Banco Llave Segura, S. A. (BANLLASE, S. A.) es la unidad de análisis, fundado en 05 de febrero de 1986, su creación se fundamentó por el enérgico impulso de establecer una institución sólida y de proyectos para la ciudad de Guatemala, por un grupo de prestigiosos empresarios y por ende presentaron la solicitud donde incluían la razón para crear el banco de emisión, giro, descuento, ahorro y depósito, siendo un banco dedicado a una variedad de productos financieros disponibles para los guatemaltecos con el afán de servir a sus cuentahabientes.

Teniendo como propósito el ampliar sus funciones económicas a todo el país logra abrir una agencia en la ciudad de Guatemala que posteriormente se convirtió en su sede central para que luego contara con un edificio propio que se encuentra en la zona uno de la capital logrando tener un mayor público. Abriendo otras agencias en la ciudad y en varios departamentos del país.

La institución bancaria, abre sus puertas al público el lunes 09 de febrero de 1987, con la misión de dar acceso a soluciones financieras, innovadoras y oportunas para los guatemaltecos, para hacer posible las metas de los clientes y sus familias. Cuenta con más de 60 puntos de servicios, considerándose como un banco solido dentro del sistema financiero guatemalteco en créditos de consumo y créditos para pequeñas y medianas empresas.

El banco obtuvo un alto progreso y alcance con sus cuentahabientes y clientes implementando diferentes tipos de préstamos en el área de agricultura, comercio, y algunas industrias, banca electrónica y con la activación de una garantía hipotecaria.

Proporciona empleo directo para 2,500 colaboradores y de forma indirecta a más de tres 1,000 personas, colaborando con la economía de estas familias, ya que el bienestar de

los guatemaltecos es parte fundamental de sus principios y valores. El Banco ofrece variedad de opciones en cuanto a sus productos y servicios, dando campo para que el cliente decida el que mejor se adapte a sus necesidades económicas, para personas y empresas.

El avance de las nuevas tecnologías ha sido beneficioso para múltiples disciplinas o campos de estudio, sin embargo, esta herramienta da muchas más opciones para cometer delitos financieros, por el desconocimiento y la aversión a los cambios tecnológicos.

El patrimonio de cuentahabiente y público en general, deben de ser resguardado con precisión para llegar a comprender las consecuencias que afectará a Banllase, debido a ataques de ingenierías sociales frecuentes y evitar que vuelvan a ocurrir en un futuro cercano, para que la entidad bancaria objeto de estudio frene estos casos, debió conocer los fraudes financieros a los que fue objeto de ataques, y los tipos de amenazas tecnológicas que existen.

Para Banllase un fraude es un delito destinado a obtener un beneficio económico a costa de sus cuentahabientes mediante vías ilegales a pesar del perjuicio de otros, se define también como el acto intencional por parte de uno o más individuos de dentro de la administración, empleados o terceras partes, el cual da como resultado una representación errónea de los estados financieros (Flores, 1981, s.p).

Los fraudes financieros que se han dado a Banco Llave Segura, S. A., fueron en un entorno económico. No se realizó el uso de la violencia, pero si se ocasionan pérdidas económicas a clientes particulares, empresas, inversores y empleados, en el caso de nuestro objeto de estudio tiene repercusiones debido a que los reclamos de clientes representan un gasto el cual según las condiciones sufridas deben de realizarse para el beneficio del cliente y para recuperar su confianza.

Los reclamos asociados a transacciones fraudulentas para el banco según lo reportado corresponden a transferencias electrónicas realizadas a cuentas de otras instituciones bancarias del país, que es donde hay un mayor número de resolución de conflictos a favor del cliente, pues cuatro de cada cinco incidentes implican un reembolso para el usuario, debido a que los estafadores emplean técnicas cada vez más sofisticadas que les permiten actuar sin mayores inconvenientes y sin ser detectados observando un alza en el año 2019.

4.2. Formas de ataque de Phishing

Banllase, S. A., se ha enfrentado a un incremento de casos de Phishing, durante la implementación de su aplicación móvil, la cual realiza transferencias electrónicas a otras cuentas del mismo banco, pagos a empresas, universidades y transferencias a cuentas de otras instituciones bancarias. Como se menciona en el capítulo dos las ingenierías sociales son las formas que los hackers obtienen información esencial de las personas, pero las formas fraudulentas son variadas, Banllase se enfocó en recopilar y clasificar los casos específicos de Phishing y determino que estos se comportaban de acuerdo a los siguientes patrones.

Cuando Banllase implementaba promociones para incentivar el uso de su aplicación y pagina web, los maleantes aprovechaban a utilizar correos con el mismo logo de la institución, simulando la apariencia de la página web. El cuentahabiente de la institución bancaria recibe el correo de su banco pensando que por ser cuentahabiente puede obtener un premio o un cambio al servicio contratado, debido a que estos correos animan al cliente a revelar información confidencial como datos personales, bancarios, número de celulares, números de tarjetas de crédito, contraseñas, por ejemplo.

Los e-mails utilizados por los hackers, son modificados constantemente para simular la imagen del sitio web, a medida que los clientes confían en los artilugios van revelando información, estos e-mails contienen links que redireccionan al usuario a sitios web, que

solicitan el reinicio de contraseñas, o que confirmen datos que la pagina original nunca solicitaría.

Otra de las formas comunes en que se apropian de la información es por medio de los links adjuntos a los correos simulando ser Banllase y el cliente al darle clic sobre el link ejecuta un virus troyano o un programa peligroso con apariencia inofensiva que instalará un capturador de escritura el cual almacenará lo que se escriba mediante el teclado incluyendo usuarios y contraseñas detectándose el uso de keylogger[1] para los casos de robo sustancial.

Dependiendo de la información recabada los hackers utilizan varios medios para complementarla, utilizando distintas formas desde redes sociales como Facebook, Instagram, Twitter, además de información donde labora el cliente o registros de entidades como la Superintendencia de Administración Tributaria -SAT- por medio del registro unificado tributario (RTU), así como el Registro Nacional de las Personas -RENAP-.

Al obtener esta información se hacen pasar por el cuentahabiente en las empresas telefónicas asociadas, solicitan la reposición de la tarjeta SIM o el bloqueo de la misma y así el cliente no se entera de la estafa, en los casos de Banllase se detectó que los hackers obtenían el número celular registrado y cuando carecían de la contraseña y usuario utilizaban el servicio de call center en horario nocturno simulando un robo y obteniendo el acceso o la vinculación a otro dispositivo.

La particularidad de los casos en las que se vulnero las medidas de seguridad de Banllase y del cliente en un 60% de casos fue porque el hacker que obtuvo la información, tenía conocimiento de las actividades que los cuentahabientes realizaban, siendo empleados de confianza, familiares o personas allegadas o que mantenían una relación cercana, un

[1] Keylogger (derivado del inglés: key ('tecla') y logger ('registrador'); 'registrador de teclas') es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet, malware del tipo Daemon.

35% fue por información recabada al azar y un 5% fue por robo del dispositivo móvil durante el año 2019.

Inicialmente los hackers utilizaban lo robado para realizar pagos a empresas de servicios básicos, telefonía, universidades, pero al incrementarse los casos se observó que los hurtos eran más elaborados, involucrando transferencias a terceros del mismo banco y otras instituciones bancarias, mediante transferencias electrónicas, al solicitar el apoyo de las empresas e instituciones bancarias se obtuvo gran negativa debido a que no querían absorber las pérdidas económicas por no contar con políticas de devolución derivado de fraudes por ingenierías sociales.

4.3. Impacto financiero por Phishing

Banllase, S.A. atravesó dificultades financieras debido a que los ataques de phishing repercutieron tanto de forma económica como en la imagen de la institución ya que la vulnerabilidad de su nueva página web que deseaba competir con las páginas ya existentes de las instituciones sólidas del país, se veía involucrada en críticas y malas calificaciones. Lo que llegó a repercutir en un bajo rendimiento de clientes durante el segundo semestre del año 2019. A continuación, se presentan los estados financieros de la unidad de análisis, los cuales, por confidencialidad, fueron modificados por un mismo dígito.

Tabla No. 1

Estado de Resultado, Banco Llave Segura, S. A. Al 31 de diciembre de 2019 (expresados en quetzales)	
Productos por colocación	1,300,000,000
Gastos por captación	500,000,000
Margen financiero	800,000,000
Productos por servicios	150,000,000
Gastos por servicios	40,000,000
Margen de servicios	110,000,000
Otros productos y (gastos) de operación – neto	(500,000,000)

Continúa en la siguiente página…

…Viene de la página anterior	
Margen operativo bruto	410,000,000
Gastos de administración	340,000,000
Margen operacional neto	70,000,000
Productos (gastos) extraordinarios – neto **Nota "A"**	40,000,000
Productos (gastos) de ejercicios anteriores – neto	5,000,000
Utilidad bruta	115,000,000
Impuesto sobre la renta	15,875,000
Utilidad neta	99,125,000

Fuente: Proporcionado por la unidad de análisis, 2020.

El Banco se encuentra en el régimen de Utilidades de Actividades Lucrativas, el cual consiste en aplicar una tasa del 25% sobre la renta imponible determinada a partir de la utilidad. El impuesto se paga mediante pagos trimestrales vencidos con una liquidación al final del año 2019.

Tabla No. 2

Nota "A" Productos y Gastos Extraordinarios	
Productos:	
Recuperación de cartera	54,000,000
Reversión de exceso de provisión de indemnizaciones	4,000,000
Reversión de provisión	3,000,000
Liquidación de saldos de clientes	4,000,000
Activos extraordinarios	300,000
Otros	2,000,000
Total, productos extraordinarios	67,300,000
Gastos:	
Descuentos en cuentas morosas	(20,300,000)
Activos extraordinarios	(3,000,000)
Pérdida en venta de bienes muebles -	(1,000,000)
Otros	**(3,000,000)**
Total, gastos extraordinarios	(27,300,000)
PRODUCTOS (GASTOS) EXTRAORDINARIOS – NETO	40,000,000

Fuente: Proporcionado por la unidad de análisis, 2020

Los productos y gastos extraordinarios registrados por Banllase, son reconocidos directamente a resultados del periodo, la entidad no presentará ninguna partida de ingreso o gasto como partidas extraordinarias en el estado de resultados por lo que se utiliza la nota “A”.

Tabla. No. 3
Conciliación entre la Utilidad Contable y la Renta Imponible, BANLLASE

Rubros	Descripción	Saldos
Utilidad Contable (-) Rentas Exentas (-) Rentas no Afectas (-) Rentas de Capital	Utilidad según libros Menos: ingresos exentos Menos: ingresos no afectos Utilidades Netas	115,000,000 (45,000,000) (9,500,000) 60,500,000
(+) Gastos no Deducibles (+) Otras	(+) Más gastos no deducibles (+) Más gastos no deducibles (reclamos no documentados)	739,400 2,260,600
(=) RENTA IMPONIBLE	Renta imponible	63,500,000
(X) Tasa De ISR (25%)	Tasa de impuesto	25%
(=) ISR a pagar	Impuesto Sobre la Renta del período	15,875,000

Fuente: Proporcionado por la unidad de análisis, 2020.

En el año 2019 se observó que los gastos no deducibles por reclamos de clientes representan tres cuartas partes del total de la cuenta Gastos Varios, por lo que se observa que el impacto financiero afecta la utilidad del ejercicio, además que representa alertas al riesgo tecnológico por ataques de phishing a la entidad bancaria por medio de transferencias electrónicas en cuentas de clientes.

Se muestra a continuación el desglose del costo de cada una de las categorías de casos de phishing durante el año 2019.

Tabla. No. 4

Casos de phishing por transferencias electrónicas a Telefonía

Año 2019	No. Transferencias	Telefonía
Enero	4	22,000
Marzo	3	30,000
Abril	1	1,000
Junio	3	9,000
Julio	9	50,000

Año 2019	No. Transferencias	Telefonía
Agosto	3	23,000
Octubre	5	20,000
Noviembre	1	5,000
Total	**29**	**160,000**

Fuente: Proporcionado por la unidad de análisis, 2020.

Tabla. No. 5

Casos de phishing por transferencias electrónicas a Servicios Básicos

Año 2019	Clientes afectados	Servicios Básicos
Enero	3	20,000
Febrero	8	50,000
Marzo	9	80,000
Abril	1	4,500
Mayo	1	200
Junio	2	8,000
Julio	15	80,000
Noviembre	4	15,000
Total	**43**	**257,700**

Fuente: Proporcionado por la unidad de análisis, 2020.

Tabla. No. 6

Casos de phishing por transferencias electrónicas a terceros

Año 2019	No. Transferencias	Transferencias a terceros
Enero	19	100,000
Febrero	26	150,000
Marzo	26	240,000
Abril	23	103,500
Mayo	1	800
Junio	28	93,000
Julio	101	550,000
Agosto	30	241,000
Septiembre	9	80,000
Octubre	36	160,000
Noviembre	13	45,000
Diciembre	1	600
Total	**313**	**1,763,900**

Fuente: Proporcionado por la unidad de análisis, 2020.

Tabla. No. 7

Casos de phishing por transferencias electrónicas a Universidades

Año 2019	No. Transferencias	Universidades
Enero	4	20,000
Febrero	2	8,000
Marzo	2	10,000
Julio	7	41,000
Total	**15**	**79,000**

Fuente: Proporcionado por la unidad de análisis, 2020.

Los registros contables de la institución bancaria pertenecen a la cuenta No. 706199 **Gastos Varios**, de la subcuenta 706199.9903 **Fraude** correspondiente a registros del año 2019, la cual comprende casos de Phishing inmersos en la cuenta contable de Fraudes, específicamente en los apartados de Fraudes externos y reclamos de clientes, los cuales se identifican por 400 casos divididos en cuatro categorías: telefonía, servicios básicos, transferencias a terceros y pago a universidades, por un costo total de Q.2,260,600 siendo las transferencias a terceros el método más utilizado por los hackers, quienes utilizan cuentas de otras entidades bancarias para realizar los hechos ilícitos.

4.4. Evaluación del riesgo phishing en Banllase, S. A.

La valoración del riesgo para el Banllase, S. A., significa la pérdida que se puede sufrir en condiciones normales en un intervalo de tiempo con un cierto nivel de confianza para lo cual se tendrá que evaluar el nivel de la probabilidad, la valoración del impacto y el riesgo inherente.

4.4.1. Valoración de la probabilidad

Desde el punto de vista de Banllase, S. A., cada evento de riesgo, ya sea una amenaza o una oportunidad, existe la probabilidad de que pueda suceder, categorizada según el nivel: baja, media baja, media, media alta y alta cuantificada según un porcentaje de ocurrencia que va desde un <5%, 5 a 25%, >25 a 50%, >50 a 70%, >70, respectivamente al nivel de probabilidad.

Tabla. No. 8

Valuación de la Probabilidad

Revisión de incidentes Phishing según unidad de Análisis del año 2019

Datos

Cantidad de Casos de phishing	Phishing	400	75%	**Alta**
Otros casos de gastos varios	Otros	133	25%	
Cantidad de casos Gastos no deducibles 2019	Total	533	100%	

Valor	Nivel	% de Ocurrencia	Definición
5	**Alta**	> 70%	Muy Probable: Riesgo cuya probabilidad de ocurrencia es **Muy Alta**. Se tiene un alto grado de seguridad que este se presente.
4	**Media Alta**	> 50 a 70%	Probable: Riesgo cuya probabilidad de ocurrencia es **Alta.**
3	**Media**	> 25 a 50%	Posible: Riesgo cuya probabilidad de ocurrencia es **Media.**
2	**Media Baja**	5 a 25%	Poco Probable: Riesgo cuya probabilidad de ocurrencia es **Baja**.
1	**Baja**	< 5%	Improbable: Riesgo cuya probabilidad de ocurrencia es **Muy Baja.**

Fuente: Proporcionado por la unidad de análisis, 2020.

Se estableció durante el año 2019 para Banco Llave Segura, S. A., 533 incidentes de reclamos, demandas y solicitudes de reembolso por parte de clientes, de los cuales 400 son en concepto de phishing lo que representa el 75% del total de casos. La probabilidad de que ocurran estos ataques cibernéticos es Alta, debido a las debilidades de controles y carencia de políticas administrativas que minimicen el riesgo evaluado, bajos estándares de seguridad en la plataforma utilizada por Banllase (solicitud de información ante el reinicio de contraseñas) durante el año 2019 cuando se empezó a utilizar este servicio, para competir con otras instituciones que poseen este servicio. Se propone políticas administrativas que puedan mitigar este riesgo (ver numeral 4.5.2).

4.4.2. Valoración del impacto

El impacto para la entidad bancaria es una herramienta de análisis de riesgos que permite establecer prioridades en cuanto a los posibles riesgos que afecten a la institución financiera en función tanto de la probabilidad.

Tabla. No. 9

Valuación del Impacto

Valor	Nivel	Perdida Probable	Comentarios
5	Catastrófico	Mayor a Q 1,000,000.00	Pérdidas financieras registradas por Q.2,260,600 para el año 2019
4	Mayor	Hasta Q 1,000,000.00	
3	Moderado	Hasta Q 500,000.00	
2	Menor	Hasta Q 250,000.00	
1	Insignificante	Hasta Q 125,000.00	

Valor	Nivel	Pérdidas Financieras	Reputación	Externos
5	**Catastrófico**	Mayor a Q.1,000,000	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, pérdida patrimonial o deterioro significativo de la imagen.	Factores que afecten el Sistema Financiera (catástrofes naturales, conflictos u otros)
4	**Mayor**	Hasta Q.1,000,000	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de los objetivos.	Factores que afectan el funcionamiento del negocio
3	**Moderado**	Hasta Q.500,000	Riesgo cuya materialización causaría una pérdida importante en el patrimonio o un deterioro de la imagen.	Factores que afectan parcialmente a la institución
2	**Menor**	Hasta Q.250,000	Riesgo que causaría un daño en el patrimonio o imagen, que se podría corregir en el corto tiempo y que no afecta el logro de los objetivos.	Factores que afectan indirectamente los intereses de la institución
1	**Insignificante**	Hasta Q.125,000	Riesgo que podría tener un efecto pequeño o nulo en la institución.	Riesgo que podría tener un efecto pequeño o nulo en la institución.

Fuente: Proporcionado por la unidad de análisis, 2020.

En el caso de ataques de phishing sufridos en el año 2019, se cuantifica que el impacto es mayor Q.1,000,000, lo que para la entidad representa una valuación catastrófica por no tener el debido cuidado ante este riesgo, cuya materialización perjudica directamente en el cumplimiento de la misión, además que representa pérdida patrimonial.

4.4.3. Valoración del riesgo inherente

Para la institución Banllase, S. A., el riesgo inherente es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto, bajo estas premisas se establece en el mapa de calor de riesgos.

4.4.4. Mapa de calor

El mapa de calor representa gráficamente ubicando los riesgos en un cuadrante, dependiendo de la probabilidad de que determinado riesgo pueda ocurrir y el impacto cuantitativo o cualitativo que se produce en caso de que se materialice el riesgo:

Tabla. No. 10

Mapa de calor

Riesgo Inherente

Probabilidad						
	Alta	Medio	Alto	Crítico	Crítico	Crítico
	Media Alta	Medio	Medio	Alto	Crítico	Crítico
	Media	Bajo	Medio	Alto	Alto	Crítico
	Media baja	Bajo	Medio	Medio	Medio	Alto
	Baja	Mínimo	Bajo	Bajo	Medio	Medio
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Fuente: Proporcionado por la unidad de análisis, 2020.

Para la evaluación del riesgo inherente se identifica que se encuentra en el estrato, critico, derivado a una probabilidad de riesgo alta y un impacto del riesgo catastrófico, esto es

por la razón de no haber implementado medidas acordes al riesgo de phishing en transacciones electrónicas las cuales no tenían planificado en el lanzamiento de la nueva plataforma virtual.

4.5. Formas de prevenir identificar ataques de phishing

Cualquier usuario que sea cliente del Banco Llave Seguro, S. A., y realice habitualmente, operaciones en la nueva banca electrónica, deberá de cerciorarse de las notificaciones por medio de correos electrónicos que no pertenezcan a la entidad de correos sospechosos.

Tabla. No. 11

Ejemplo de correo electrónico phishing

De:	*GrupoBan11ase@banc.com.gt*
Asunto:	Revisión de datos maestros
Descripción:	Suspensión de tarjeta de tarjeta
Remitente:	Servicio al Cliente
Para:	Mí
Fecha	16 oct. 2020 03:22
Seguridad:	Encriptación estándar (TLS) Más información

Estimado Cliente de Banllase,

Estamos teniendo dificultades para verificar la información de su tarjeta.
Le invitarnos a corregir este problema haciendo clic en el enlace de abajo, siguiendo las instrucciones.

Ingrese al sitio web, por medio de los enlaces, llenar los campos que se le solicitan, confirma los saldos a la fecha de corte.
De tener algún inconveniente puede comunicarse a servicio al cliente, xxxxx-xxxx, con gusto le atenderemos.

Banllase, marca registra todos los derechos reservados.

https://www.Ban11ase@banc.com.gt
https://www.actualización-Ban11ase@banc.com.gt

Fuente: Proporcionado por la unidad de análisis, 2020.

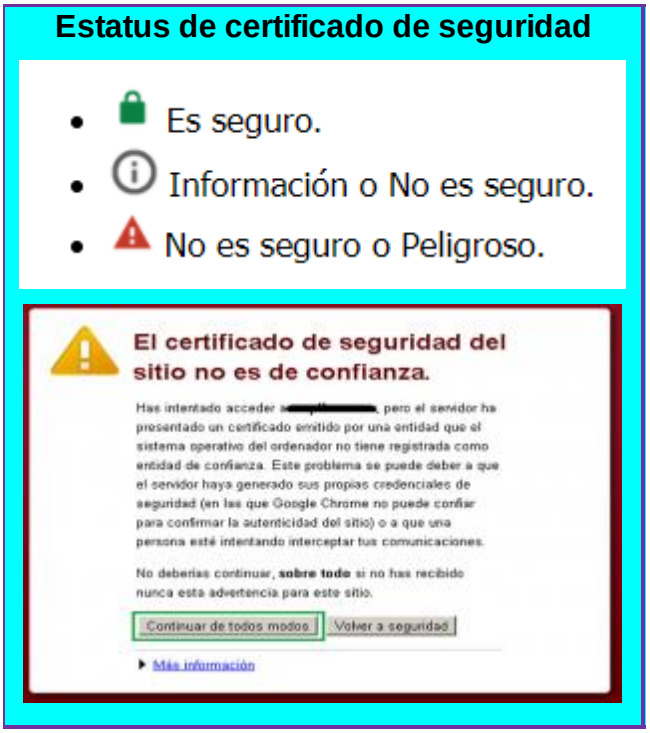
La forma más utilizada para realizar phishing, es por medio de una solicitud de actualización de datos simulando ser la institución bancaria, en este correo se podrán

identificar situaciones anómalas como la utilización de números el correo falso tiene números que reemplazan las letras “l” https://www.Ban11ase@banc.com.gt, en otras ocasiones puede ser la falta de una letra en el certificado de seguridad, en el nombre del dominio o la adición de alguna otra letra, numero o carácter especial.

Otra característica común, es que el correo se indicó que tiene un problema con su cuenta que vincula al cliente con el banco, ya sea por cargo de intereses, multa, mora y por incentivos como premiación por ser cliente de la institución bancaria, lo que va de la mano con la solicitud de actualizar la información personal.

En algunos casos se registran números de teléfono con el cual intentan simular ser parte de la unidad de servicio al cliente para obtener la mayor parte de información.

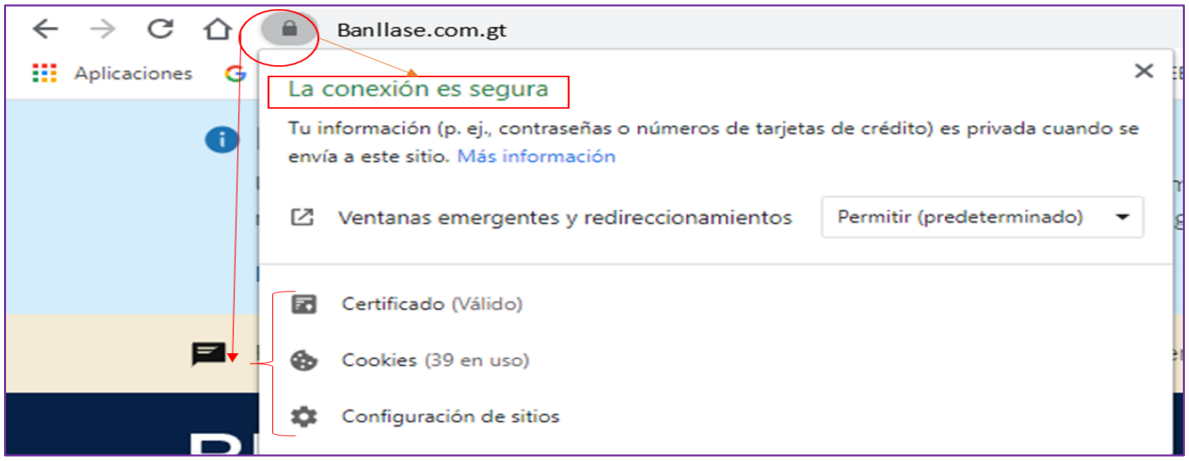
Figura No. 1



Fuente: Proporcionado por la unidad de análisis, 2020.

Figura No. 2

Certificado de seguridad Banllase original



Fuente: Proporcionado por la unidad de análisis, 2020.

Se identificó por el personal de Banllase, que los clientes piensan que los sitios cuyo URL empieza con las letras “https://”, o con un candado verde, son 100 por ciento seguros; sin embargo, la realidad es otra debido a que este tipo de certificaciones de seguridad ya pueden ser adquiridas por los piratas informáticos, la vigencia suele durar poco tiempo por lo general un día.

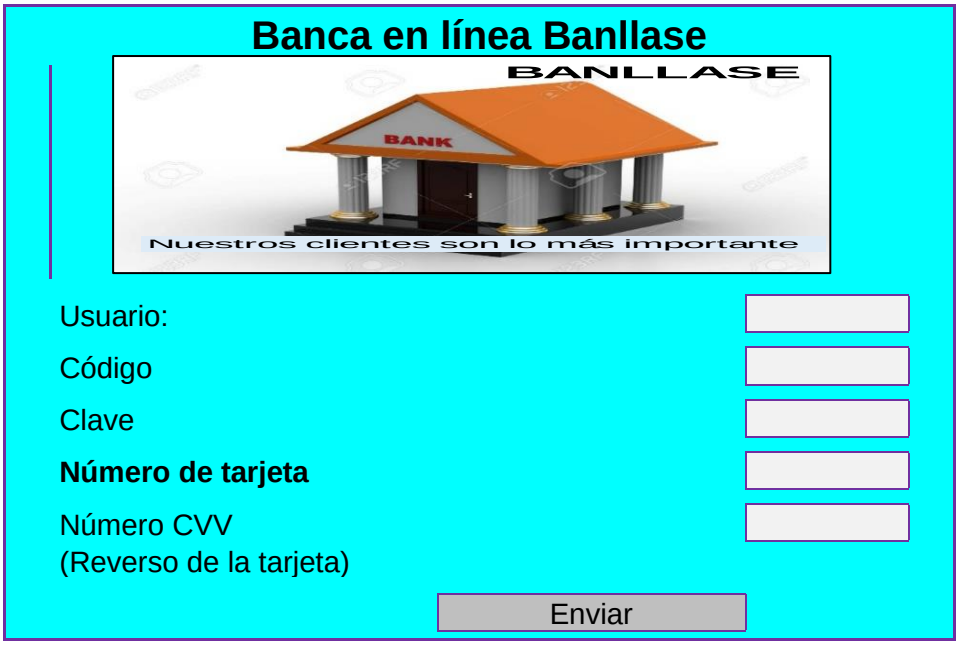
Figura No. 3

Logotipos, original y falso

Fuente: Proporcionado por la unidad de análisis, 2020.

Figura No. 4

Sitio web falso



Fuente: Proporcionado por la unidad de análisis, 2020.

Los campos solicitados pueden variar, pero el objetivo principal es obtener la información esencial, con la cual puedan ingresar a la banca en línea del cliente y de esta forma realizar transferencias electrónicas a otras cuentas del mismo u otros bancos, así como el pago a distintos proveedores.

El Card Verification Value (CVV) o código valor de verificación validación es un número de tres o cuatro dígitos que está situado en la parte trasera de las tarjetas de crédito y débito utilizado como clave para compras en línea o pago con tarjetas en sitios web.

Una vez introducidos los datos el usuario, será redirigido a la página web legítima del Banco Llave Segura, con el afán que el cliente crea que su información no fue comprometida.

4.5.1. Caso de phishing en BANLLASE

Durante el mes de julio 2019 los casos de phishing hacia la entidad Banllase establecieron un alza, se asignaron técnicos de información tecnológica, para que

visitaran las oficinas de algunos clientes para examinar sus equipos de cómputo y se determinó que estaban infectadas con Keylogger, provenientes de correos maliciosos que pretendían ser de la entidad, entre los casos a destacar se encuentra la señora Damaris Ruano (nombre ficticio), quien recibe depósitos y realiza pagos electrónicos en sus cuentas monetarias y de ahorro, adicionalmente se encontraban vinculadas las cuentas de su esposo.

La señora Ruano, por el giro de su negocio que es compra y venta de artículos de oficina mantenía un ritmo constante de transacciones electrónicas, pero los días 14, 15 y 17 de julio le aparecían un total de 12 débitos que no había realizado por medio de transferencias electrónicas. Los primeros dos días se efectuaron pagos a distintos comercios de telefonía por montos para el día 14 de Q. 5,000.00 y el día 15 de Q. 12,500.00 para el día 17 los hackers realizan el reinicio de contraseña del correo electrónico y de forma simultánea solicitan un reinicio de contraseña de la aplicación a la unidad de call center de Banllase, quienes en la llamada de seguridad consta que solo le solicitó la dirección de email sin verificar los demás datos, con la cual adicionan cuentas ajenas de otros bancos y tarjetas de crédito, al tener acceso total tanto de la aplicación y del correo electrónico al cual llegan las alertas para la señora Ruano.

Al obtener acceso total los delincuentes realizaron un robo de Q 376,000 debido a que la cifra era mayor, pero se recuperaron las transferencias realizadas al mismo banco y de algunos proveedores y bancos que tienen la política de prever estos incidentes.

Para Banllase existe un problema adicional debido a que la señora Damaris Ruano, no tiene su contabilidad al día por documentos en circulación, aduce que el robo a sus cuentas, es de tres días antes de lo recabado por la institución bancaria y que el personal de la institución bancaria tiene relación, de lo cual según las llamadas de seguridad indican solo negligencia y falta de controles por lo que la señora Damaris Ruano solicita el reintegro de Q. 500,000 este caso se encuentra en investigación por la diferencia mencionada.

Por la magnitud de este caso se realizó el análisis de la valoración del riesgo phishing durante el mes de julio 2019.

Tabla. No. 12

Valuación de la Probabilidad caso señora Ruano

Revisión de incidente Phishing mes julio 2019

Datos

				Nivel
Monto de casos de phishing Sra. Ruano	Phishing	376,000	52%	**Media Alta**
Otros casos de gastos varios	Otros	345,000	48%	
Monto de casos Gastos 2019	Total	721,000	100%	

Valor	Nivel	% de Ocurrencia	Definición
5	**Alta**	> 70%	Muy Probable: Riesgo cuya probabilidad de ocurrencia es **Muy Alta**. Se tiene un alto grado de seguridad que este se presente.
4	**Media Alta**	> 50 a 70%	Probable: Riesgo cuya probabilidad de ocurrencia es **Alta.**
3	**Media**	> 25 a 50%	Posible: Riesgo cuya probabilidad de ocurrencia es **Media.**
2	**Media Baja**	5 a 25%	Poco Probable: Riesgo cuya probabilidad de ocurrencia es **Baja**.
1	**Baja**	< 5%	Improbable: Riesgo cuya probabilidad de ocurrencia es **Muy Baja.**

Fuente: Proporcionado por la unidad de análisis, 2020.

En el mes de julio 2019 se identificó el caso de la señora Damaris Ruano, el que establece la cantidad más alta en defraudación y fue el caso pionero para establecer la falta de controles en los procesos de solicitud de reinicio de contraseñas, este dato se seleccionó de la Tabla. No. 4 casos de phishing por transferencias electrónicas de BANLLASE, S. A., se estableció en el nivel: Media Alta de probabilidad.

Tabla. No. 13

Valuación del Impacto caso de la señora Ruano

Valor	Nivel	Pérdida Probable	Comentarios
5	Catastrófico	Mayor a Q 1,000,000.00	
4	Mayor	Hasta Q 1,000,000.00	
3	Moderado	Hasta Q 500,000.00	Pérdidas financieras registradas por Q.376,000 en el mes de julio de 2019
2	Menor	Hasta Q 250,000.00	
1	Insignificante	Hasta Q 125,000.00	

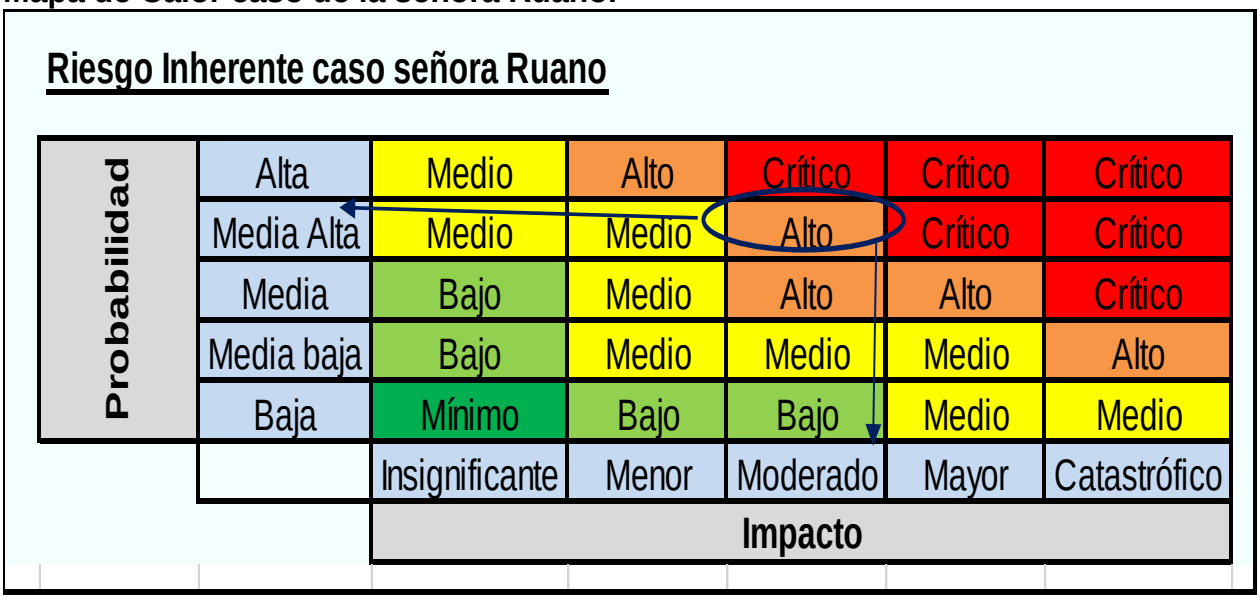
Valor	Nivel	Pérdidas Financieras	Reputación	Externos
5	**Catastrófico**	Mayor a Q.1,000,000	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, pérdida patrimonial o deterioro significativo de la imagen.	Factores que afecten el Sistema Financiera (catástrofes naturales, conflictos u otros)
4	**Mayor**	Hasta Q.1,000,000	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de los objetivos.	Factores que afectan el funcionamiento del negocio
3	**Moderado**	Hasta Q.500,000	Riesgo cuya materialización causaría una pérdida importante en el patrimonio o un deterioro de la imagen.	Factores que afectan parcialmente a la institución
2	**Menor**	Hasta Q.250,000	Riesgo que causaría un daño en el patrimonio o imagen, que se podría corregir en el corto tiempo y que no afecta el logro de los objetivos.	Factores que afectan indirectamente los intereses de la institución
1	**Insignificante**	Hasta Q.125,000	Riesgo que podría tener un efecto pequeño o nulo en la institución.	Riesgo que podría tener un efecto pequeño o nulo en la institución.

Fuente: Proporcionado por la unidad de análisis, 2020.

En la valuación del caso de la señora Ruano, se observó una ponderación de moderado, lo que representa que solo este caso afecta parcialmente a la institución bancaria.

Tabla. No. 14

Mapa de Calor caso de la señora Ruano.



Fuente: Proporcionado por la unidad de análisis, 2020.

Se observó que la probabilidad indicada en la tabla 9 y el impacto del caso cliente de la tabla 10, muestra que el riesgo inherente se encuentra en Alto, tomando en consideración el caso representativo de entre todos los incidentes del mes de julio del año 2019.

El impacto financiero de este caso repercute adicionalmente al gasto no deducible de la cuenta, a otros gastos derivados en los que se incurrieron al momento del reclamo, investigación y ejecución de medidas correctivas.

Tabla. No. 15

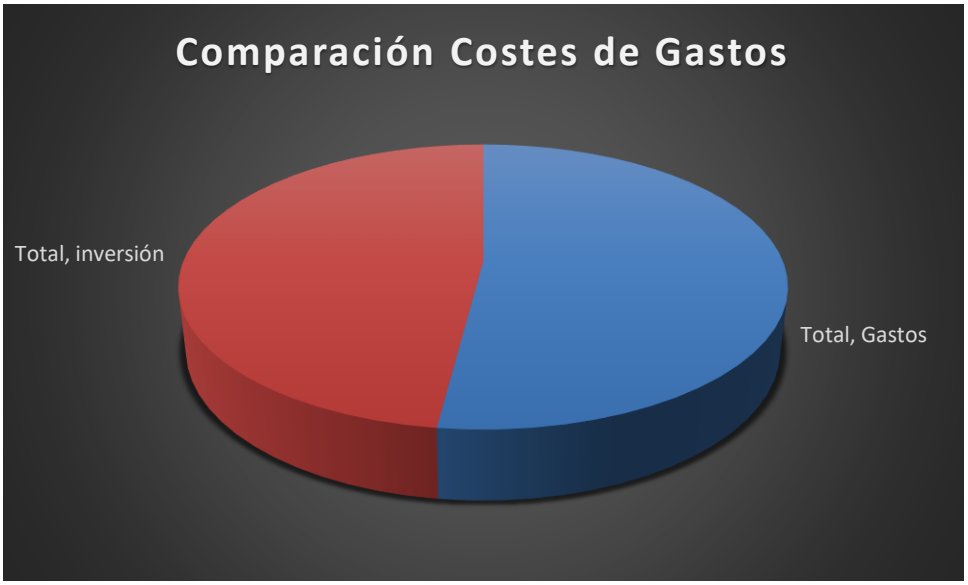
Comparación de Gastos y Medidas Correctivas por BANLLASE			
Caso señora Ruano	**Valor**	**Medidas Correctivas**	**Valor**
Gasto por reintegro de Phishing	366,000	Implementación de controles (Manuales, políticas, otros)	10,000
Gastos administrativos (Pruebas de confidencialidad, otros)	6,000	Capacitación al personal (procesos, ética, otros)	50,000
Baja de personal sin acción penal (2 colaboradores)	64,000	Cambio de sistemas automatizados en la plataforma virtual	190,000
Proceso penal contra el perpetrador (+/-)	10,000	Asesoría y mantenimiento de servicios informáticos (externo)	175,000

Comparación de Gastos y Medidas Correctivas por BANLLASE			
Demanda a terceros (+/-)	10,000		
Reemisión de estados financieros, otro tipo de reporte, informe	5,000		
Total, Gastos	461,000	Total, inversión	425,000

Fuente: Proporcionado por la unidad de análisis, 2020.

El cuadro anterior indica los gastos incurridos en el caso de la señora Damaris Ruano, y los gastos realizados para la implementación de medidas correctivas, lo que refleja que de haber tenido la debida planificación en el lanzamiento de la plataforma de transferencias móviles de Banllase, el impacto financiero ante los casos de phishing habría sido menor a los presentados en el año 2019 específicamente en el mes de julio como se muestra en el caso de la señora Ruano.

Figura No. 5



Fuente: Proporcionado por la unidad de análisis, 2020.

Los casos de phishing repercuten el funcionamiento e imagen de la institución bancaria, pero las áreas afectadas en cuanto al presupuesto del año 2019, son: Sistemas tecnológicos, Canales Virtuales, Atención al cliente y recursos humanos tanto en gastos por incidentes phishing y por medidas correctivas derivados de estos casos.

4.5.2. Propuesta de nuevos procesos

Para los clientes que utilizan la plataforma web de la página oficial de Banllase, se les informará las medidas de seguridad para prevenir y mitigar el riesgo de phishing mediante campañas de concientización por medio de videos explicativos en la plataforma de la banca virtual, sitio web y afiches colocados en agencias de Banllase, las campañas contendrán las siguientes recomendaciones como regla general:

- No responder nunca los correos electrónicos que soliciten dinero, envíos de giros, datos bancarios, contraseñas o datos de tarjetas de crédito.

- No hacer clic en los enlaces de estos mensajes. Si cree que el mensaje puede ser verdadero y que proviene de Banllase, ingrese al sitio web de la institución escribiendo la dirección directamente en la barra del navegador, para evitar ingresar en alguna página web realizada por el atacante.

- Ingresar manualmente a la web de Banllase, nunca utilizar enlaces recibidos por correo electrónico.

- Banllase no solicita datos personales o confidenciales (número de cuenta, tarjeta, contraseñas, PIN de acceso, número de documento, etc.) por correo electrónico.

- En el navegador se puede verificar y confirmar que se está en el sitio seguro de Banllase, observando que la barra de dirección tiene un fondo color verde, un candado y la identificación del Banco.

- No ingresar el usuario y clave de Banca Web sin haber verificado la autenticidad del sitio accedido.

- Evitar acceder a la página web de Banllase desde lugares públicos, tales como: cibercafés, accesos públicos a WiFi o desde cualquier lugar que se considere de riesgo.

- Utilizar su banca en línea únicamente sitios seguros y dispositivos personales.

- No compartir contraseñas, usuarios, códigos de verificación.

- Llamar al banco a través de números que la institución mantiene registrados en sus redes sociales verificadas y autorizadas.

Los procesos que se sugieren fortalecer o establecer en la institución bancaria, en las distintas áreas operativas que intervienen en los puntos vulnerables detectados por los hackers.

Para la unidad de Call Center se sugiere añadir los siguientes procedimientos a cada una de sus actividades:

- Completar un check list con la información necesaria y que el cliente debe de conocer, dejando evidencia del cumplimiento de este proceso.

- Supervisar los casos en los que los clientes no cuenten con la información solicitada.

- Enviar alertas de adiciones de cuentas a los dispositivos móviles y correos electrónicos.

- Implementar códigos de seguridad para transacciones móviles, pagos de servicios y pago a proveedores.

- Capacitar al personal, con el fin de que ellos puedan identificar posibles casos de phishing.

- Mantener contacto con supervisores y jefes inmediatos

- Establecer auditorias constantes y monitoreo al personal de los distintos turnos.

Para el personal de atención al cliente, canales virtuales, sistemas tecnológicos y recursos humanos, se les recomienda trabajar en equipo para solventar los reclamos por phishing, y así poder controlar los gastos no deducibles recolectando la documentación necesaria ante cualquier reparo ante la Superintendencia de Administración Tributaria, además de establecer parámetros ante posibles estafas elaboradas por lo cual se sugiere:

- Solicitar la documentación que respalde que el solicitante sea el cuentahabiente de Banllase y no un tercero, a excepción de casos especiales se le solicitará una carta de poder.
  -Denuncias ante el Ministerio Público.
  -Denuncias ante alguna comisaria o juzgado.
  -Documentación personal, DPI, en caso de robo o extravío una certificación de trámite de RENAP.
  -Si el caso de Phishing es en una cuenta de ahorro presentar la libreta de la cuenta.

- Monitorear las gestiones de los clientes, verificar que no exista reincidencia de solicitudes.
  Mediante el sistema Monitor Plus, establecer parámetros para que, en casos de reincidencia, se pueda tener alertas, de sospechas de un fraude elaborado por terceros ajenos a las cuentas de un cliente de Banllase.

- Establecer un control mediante bitácoras de uso de la plataforma de transferencias móviles delimitando el tiempo que indica el cliente le fue sustraído ilícitamente de sus cuentas el dinero que reclama, con el de las posibles alertas a adiciones de cuentas o pagos de servicios o proveedores no frecuentes.

- Verificar el uso de códigos de seguridad para transacciones móviles, pagos de servicios y pago a proveedores, mantener al día una base de datos para establecer que quien solicita el reintegro conoce las medidas de seguridad de Banllase.

- Mantener capacitaciones constantes al personal de recién ingreso y retroalimentación y actualización a todo el personal involucrado en estos procesos sobre las nuevas formas que hackers utilizan para sustraer el dinero de cuentahabientes.

- Reportar las anomalías de transacciones sospechosas realizadas en la plataforma web de Banllase.

La principal herramienta contra este tipo de estafa está relacionada con la educación para los clientes de Banllase y para el personal la capacitación sobre temas tecnológicos y de ética profesional son de vital importancia.

Las principales políticas administrativas a proponer para la mitigación del riesgo de phishing en transferencias electrónicas en la institución son:

Todas las políticas se consignen deberán detallarse en un manual de Procedimientos Administrativos y será divulgado en la institución al personal encargado de las actividades relacionadas, banca en línea, jefes y funcionarios.

Según el código de ética de la institución, la información indicada no deberá usarse para fines ajenos y en perjuicio a Banllase.

1. El personal de call center que atiende los requerimientos de clientes mantendrán un reporte de casos creados en el cual consignará:
    - Fecha de atención
    - Hora de atención
    - Número de caso en el Sistema
    - Descripción del problema del cliente.

Si es por reinicio de contraseña, se le solicitará la siguiente información:

- Nombre completo
- Número de CUI
- Número de Identificación tributaria
- Número de teléfono registrado ante el banco
- Correo electrónico registrado ante el banco
- Solicitar el motivo del reinicio de contraseña

2. De no cumplir con los requisitos anteriormente solicitados se denegará la asistencia y se le remitirá a la agencia más cercana donde tendrá que presentar la documentación necesaria.

3. En el caso de robo o extravió se le indicará al cliente del bloqueo de las cuentas de ahorro, monetaria o tarjetas de débito o crédito.

4. No dar información que no sea la solicitada inicialmente.

5. El jefe o funcionario a cargo mantendrá monitoreo constante al personal a cargo y establecerá indicadores de rendimiento.

6. Auditoría interna realizará revisiones periódicas a las áreas involucradas en el proceso de transferencias electrónicas.

7. El personal de atención al público atenderá los casos de reclamos de clientes.

8. Mantendrá en el sistema un historial actualizado de los casos reportados.

9. Solicitará la información pertinente y necesaria.

   Ante casos específicos, se asignará un asesor encargado de recolectar la información que indique si procede el reintegro de hurto, además de establecer la documentación

que ampare ante la Superintendencia de Administración Tributaria la deducibilidad del Gastos a incurrir por caso de phishing.

10. Ante la negativa del solicitante se cancelará el proceso de solicitud de reintegros.

11. Ante un posible caso elaborado de estafa, se solicitará al área de cumplimiento la verificación del estatus del cliente, ante cualquier tipo de restricciones que pueda tener. Mediante el Sistema o parametrización del Sistema de Alertas Monitor Plus.

12. El personal que no cumpla con las normas establecidas y aprobadas por la administración será sancionado con lo establecido en el manual de Sanciones al personal, que consta de llamada de atención, carta al expediente, y suspensión de labores, así como otras sanciones que sean necesarias.

De ser necesario se adicionarán políticas específicas por cada área que interviene. Para establecer controles adicionales a los descritos.

Conclusiones

1. Se determinó que el impacto financiero de ataques de phishing por medio de transacciones electrónicas a la institución bancaria BANLLASE, S. A., ascendió a la cantidad de Q.2,260,600 durante el periodo comprendido del 01 de enero al 31 de diciembre de 2019, la categoría más alta corresponde a transferencias móviles a terceros con un monto de Q.1,763,900 que representa un 78% del total de casos reportados en ese año.

2. Se observa el incremento en los gastos no deducibles por incidentes de phishing debido a las malas políticas administrativa, además de deficientes instrucciones para el manejo y tratamiento de estos casos, la cuenta de gastos no deducibles aumento a Q 3,000,000.00 para el año 2019, los casos de ciber ataques representa un 75% de los gastos no deducibles.

3. La entidad bancaria no cuenta con adecuados procesos ante la forma de proceder a los reclamos de robo por medio de phishing, debido a que no se documenta la información mínima requerida para comprobar que no sea una estafa elaborada. Además de incrementar los gastos no deducibles y por ende el pago de impuestos.

4. Se determinó que la falta de políticas y medidas de precaución ante eventuales contingencias inciden financieramente, derivado a estas situaciones los cuentahabientes pueden llegar a abandonar el banco, además de poner en riesgo el prestigio de la entidad bancaria al tener problemas de imagen.

Recomendaciones

1. Prever el impacto financiero del riesgo por robo de información a clientes de la institución bancaria unidad de análisis mediante la elaboración de estrategias de contingencia ante estos casos de phishing.

2. Planificar medidas correctivas ante la documentación de gastos no deducibles por incidentes de phishing estableciendo políticas administrativas, evaluando la vulnerabilidad de los procesos de transacciones electrónicas, estableciendo medidas de control más estrictas.

3. Evaluar y analizar la propuesta de implementación de campañas informativas y divulgación de medidas de reconocimiento, seguridad informática, así como asesoría a clientes y capacitación al personal de la entidad.

4. Establecer una línea específica de asesoría e información la cual será de beneficio para establecer que caso corresponde a un posible ataque de phishing o es una estafa elaborada y así prevenir ser objeto de estos, para recuperar la confianza de sus clientes y fortalecer el crecimiento de la institución bancaria.

Bibliografía

Aguilar Elizardi (2015). "*Lecturas para el curso Métodos y Técnicas de Investigación*." 1ra. Edición. Editorial Estudiantil Fénix, páginas 26-27.

Asamblea Nacional Constituyente. Guatemala 1985, "*Constitución Política de la República de Guatemala*," páginas 73-133.

Bernal Torres, Cesar Augusto (2012). "*Metodología de la Investigación, Para administración, economía, humanidades y ciencias sociales," Guatemala*, Editorial Pearson Educación, 2da. Edición, página 304.

Decreto del Congreso Número 2-70 del Congreso de la República de Guatemala, "*Código de Comercio de Guatemala*", página 18

Decreto del Congreso Número 19-2002 del Congreso de la República de Guatemala –"*Ley de Bancos y Grupos Financieros"*

Decreto del Congreso Número 16-2002 del Congreso de la República de Guatemala – "*Ley Orgánica del Banco de Guatemala"*

Gil Domínguez, A. (2005): "*Neoconstitucionalismo y Derechos colectivos"* (Edición Ediar) Argentina-Buenos Aires.

Hernández Sampieri, R.; Fernández Collado, C.; y, Baptista Lucio, P. (2014). "*Metodología de la Investigación"*. México. McGraw-Hill Interamericana. Sexta edición.

Leonett, José (2018), REDLIF (*Red Latinoamericana de Informática Forense REDLIF Guatemala / El Derecho Informático Iberoamérica /Observatorio Iberoamericano de Protección de Datos*)

Lima de Luz, M. (1984): "*Delitos Electrónicos*" (Ediciones Porrúa). México. Molina Wilson (2001). Efectos Financieros en una institución bancaria CPA, Guatemala.

Manuel Osorio. (2000). "*Diccionario de Ciencias Jurídicas Políticas y Sociales,"* Editorial Heliasta S.R.L. Buenos Aires.

López Geoffroy, Hugo (2019). "*Informe Sectorial Banco de Guatemala, Desempeño y perspectivas"*, ZummaRatings.

Moliner Ruiz, M. (1996). "*Diccionario de María Moliner*" (Edición Digital). Copyright© Novel Inc.

Palma Geovanni – Efectos Financieros en una institución bancaria por reforma a la Ley de bancos (Decreto 26-99), CPA, Guatemala octubre 2001 – Tesis Usac.

Piloña Ortiz, Gabriel Alfredo (2012). **"***Métodos y técnicas de Investigación documental y de campo*". 6ª. Ed. Litografía Cimgra, Guatemala Página 67.

Sanchez, C. (s.f) "*Normas APA, 7ª. Edición, Recuperado el 11 de marzo de 2020 en https.//normas-apa.org/"*

Salellas, L. (2012): "*Delitos informáticos-Ciberterrorismo*" (Sr Hadden Security Consulting Group) USA-New York.

Schnier, B. (2000): "*SECRETS & LIES Digital Security in a Networked World*" (Editorial: John Wiley & Sons - Díaz de Santos) USA-New York.

Serrahima, Joaquim. (2010): "*La Amenaza Digital*". (Editor Bresca). España Barcelona.

Télles Valdez, J. (1996): "*Derecho Informático*" (Segunda Edición). Edición Mc Graw Hill. México.

Universidad de San Carlos de Guatemala. Facultad de Ciencias Económicas. Centro de Documentación Vitalino Girón Corado. (2001). *Normas para la Elaboración de Bibliografías en Trabajos de Investigación*. Licda. Dina Jiménez de Chang. Segunda edición.

Universidad de San Carlos de Guatemala. Facultad de Ciencias Económicas. Escuela de Estudios de Postgrado. (2018). *Instructivo del trabajo profesional de graduación para optar al grado académico de maestro en artes, Facultad de Ciencias Económicas*.

Universidad de San Carlos de Guatemala. Facultad de Ciencias Económicas. Escuela de Estudios de Postgrado. (2015). *Normativo de la escuela de estudios de postgrado.*

Valdés Domínguez, M. (2006): "*Criminalidad Informática, un fenómeno de fin de siglo*" Cuba.

Egrafía

Anti-Phishing Working Group, APWG, (2017), Recuperado de: https://apwg.org/

Barry Collin, (2015), Recuperado de: http://www.af.mil/news/Feb1998/n19980206_980156.html

Cisco Systems, Inc. (2014). Recuperado de: https://www.cisco.com/c/en/us/products/index.

Dorothy E. Denning (2016) Special Oversight Panel on Terrorism, Committee on Armed Services, de la cámara baja estadounidense: Recuperado de: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Fernando Martín del Campo (2015), https://www.estrategiaynegocios.net/opinion/863212-345/riesgo tecnol%C3%B3gico-y-seguridad-en-la-banca

Fraud.org is a project of the National Consumers League (2019). Copyright © 2019. Recuperado de: https://www.fraud.org/tips/internet/phishing.htm

Humberto Cardoso Cabrera (2015). Supervisor de EcuRed (http://www.ecured.cu) José Manuel Feria Domínguez (2015), Recuperado de: https://thales.cica.es/rd/Recursos/rd98/Economia/02/texto3.html

Matías Carrocera (2016), Revista Forbes, Comunicación y Negocios. México, Recuperado de https://www.forbes.com.mx/brand-voice/poder-la-privacidad-digital-las-empresas/

Microsoft (2019), Recuperado de: https://www.microsoft.com/en-us/education

Seguridad de la información (2015), Recuperado de: http://www.segu-info.com.ar/legislacion/

Superintendencia de Bancos de Guatemala, Estándares Internacionales. ¿Qué es Basilea I? (2018), Recuperado de https://www.sib.gob.gt/web/sib/faq/basilea

Superintendencia de Bancos (2018), SIB Guatemala, GRUPOS FINANCIEROS, Recuperado de: https://www.sib.gob.gt/c/documentlibrary/getfile?folderId=832833& 05.pdf. Consulta realizada el 25 de septiembre de 2018.

Anexos

Formato de instrumentos utilizados

Formulario Phishing Banllase, S.A.

Entrevista focalizada phishing

Área Digitalización y recepción de denuncias de phishing

Fecha: 25/03/2020

No.	Procedimiento
1	¿Qué experiencia técnica posee ante hallazgos de phishing?
2	¿Qué experiencia académica posee ante hallazgos de phishing?
3	¿Cuántos años ha desempeñado el puesto actual de técnico de investigación clientes?
4	¿El Funcionario a cargo de la agencia en línea, le proporciona el total de casos de inconformidad de clientes?
5	¿Qué tipo de ingeniería social es más propensa en la institución BANLLASE?
6	¿Cuántos casos de ingeniería social se han reportado durante el año 2019?
7	¿Cuántos casos de phishin se han reportado durante el año 2019?
8	¿Qué tipo de malware utilizan los hackers, para realizar phishing?
9	¿Cómo funciona el software malicioso?
10	¿Cómo funciona un keylogger?
11	¿Cómo el cliente, fue engañado por medio de phishing?
12	¿Cómo se puede prevenir el ataque de phishing?
13	¿Qué se procede al tener certeza de ataques de phishing?

14	¿BANLLASE, cuenta con alguna herramienta que detecte estos ataques de phishing?
15	¿Se puede recuperar las transferencias electrónicas que el hacker sustrajo al cliente?

(f) _____
Jefe / Técnico Asignado

Firma y Sello

(f) _____
Entrevistador

Firma

Guía de Observación	
Banco Llave Segura, S. A.	
No.	**Procedimiento**
1	Observar el área de call center, cuenta con el equipo necesarios para atender las necesidades de los clientes ante reinicio de contraseñas.
2	Los colaboradores atienden de forma correcta las llamadas de los clientes, tomando todos los datos necesarios para validar las consultas.
3	Los colaboradores utilizan los sistemas necesarios para verificar la información proporcionada por los clientes de Banllase.
4	Los colaboradores registran los datos recabados en el sistema establecido para crear un caso digital.
5	¿El jefe o funcionario a cargo verifica periódicamente las actividades de sus colaboradores?
6	¿El área de call center cuenta con una bitácora de acciones diarias?
7	¿El jefe de agencia o funcionario a cargo, realiza los siguientes procedimientos?
	a) verificar el 100% reclamos
	b) sella y certifica la bitácora de casos de mayor nivel de incertidumbre

OBSERVACIONES:

Índice de Tablas

Índice de Figuras

Índice de Anexos