FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho y Ciencias Políticas

“EL DEBER DE IDONEIDAD DE LAS ENTIDADES BANCARIAS DE LA REGIÓN LA LIBERTAD EN EL FRAUDE ELECTRÓNICO CON TARJETAS DE CRÉDITO Y DÉBITO”

Tesis para optar el título profesional de:

Abogada

Autora:
Luisa de los Milagros Linares Nuñez

Asesor:
Dr. Gerson Andree Del Castillo Gamarra

Trujillo - Perú

2020

DEDICATORIA

A Dios por haberme guiado y darme fuerzas para no rendirme y seguir adelante.

A mis padres y a mi hermano, por apoyarme y darme palabras de aliento cada día para poder cumplir mis metas y crecer como profesional.

A mis abuelos, porque con su amor infinito me han motivado en mi crecimiento personal.

A mi Petita, mi segunda madre.

AGRADECIMIENTO

Agradezco a la Universidad Privada del Norte por ser una universidad preocupada por el bienestar y aprendizaje de sus alumnos. Al asesor por inculcarme con sus conocimientos y por la paciencia para concretar este trabajo de investigación

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente tesis ha sido desarrollada con la búsqueda de resoluciones expedidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi, por artículos científicos, tesis y noticias que hayan podido avalar al tema de investigación, aunado a ello se ha encontrado antecedentes que han llegado a determinar que el fraude electrónico con tarjetas de crédito y débito afecta al consumidor en el momento de que el banco no toma las medidas de seguridad correspondientes. Ante la indagación de indicios que han contribuido con la delimitación del tema, se ha propuesto como objetivo de la investigación demostrar si los Bancos de la región La Libertad cumplen con el deber de idoneidad en las operaciones bancarias virtuales en donde sucede fraude electrónico con tarjetas de crédito y débito en los periodos 2017-2019.

En ese sentido, se ha tomado como instrumentos de investigación 15 Resoluciones sobre operaciones no reconocidas emitidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi- La Libertad, análisis de legislación internacional, encuestas a usuarios, obteniéndose como resultados que los Bancos incumplen con el deber de idoneidad al no cumplir con las medidas de seguridad para evitar que se efectúe el fraude electrónico con tarjetas de crédito y débito.

Palabras clave: deber de idoneidad, entidades bancarias, tarjeta de crédito y tarjeta de débito, fraude electrónico.

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad, las operaciones bancarias presenciales han sido reemplazadas por operaciones virtuales bancarias; ante ello los Bancos han implementado las tarjetas de crédito y débito a fin de facilitar a los usuarios al momento de realizar transacciones financieras, pagos en efectivo o en sus obligaciones, así como también para realizar operaciones adicionales, tales como compras por páginas de internet y pagos de servicios.

Sin embargo, ante el uso continuo de estas tarjetas se han acarreado problemas como son los fraudes; dicho fraude se realiza por terceras personas que utilizan tarjetas extraviadas, robadas o clonadas para hacer compras o retirar dinero físicamente, pero además no es necesario que tengan la tarjeta en físico sino que también pueden realizar sin tener la tarjeta; esto es que pueden realizar compras por internet o hacer transferencias por los aplicativos de las entidades bancarias, estas operaciones la persona malintencionada lo puede realizar con solo tener datos importantes de las tarjetas.

De esta manera, el fraude electrónico ha ido apoderándose en diferentes países tal como lo señala Diario Gestión (2019) en “Nuevo récord de fraudes de dominio en internet en el 2018”; informó que la Organización Mundial de la Propiedad Intelectual (OMPI) recibió 3,447 denuncias por fraude electrónicos. Por otro lado, Diario Gestión (2017) dio a conocer en su noticia“ Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017” que, en Latinoamérica las pérdidas económicas originadas por este tipo de fraudes cibernéticos ascienden a US$ 76, 766 millones. Aunado a ello, Diario Peru21 (2018) en “Conoce los fraudes del comercio electrónico”; estableció que

Perú está en el séptimo lugar entre los países afectados, registrando pérdidas de US$ 4,782 millones.

En el Reglamento de Tarjetas de Crédito y Débito (Resolución S.B.S 6523-2013) y con su modificatoria la Resolución N° 5570-2019 (Resolución que entrará en vigencia en enero del 2021), establece que a fin de evitar el fraude electrónico, las entidades del sistema bancario deben adaptar medidas de seguridad según lo que se ordena; esto en concordancia con la calidad e idoneidad del servicio, es decir que el banco por tener una actividad riesgosa debe tener las suficientes medidas para que ante cualquier contingencia o fraude electrónico se proteja el patrimonio del consumidor. Se entiende por la idoneidad del servicio según el Art. 18° del Código de Protección y Defensa del Consumidor la correspondencia entre lo que el proveedor ofrece en relación a la naturaleza y características del producto o servicio y lo que el consumidor recibe, de la misma manera el Art. 19° menciona que el proveedor debe responder por la calidad y la idoneidad de los servicios o productos que brinda.

Sin embargo, los Bancos confían que las compras por internet o las transacciones las está realizando el usuario, debido a que la clave secreta y los números de la tarjeta solo el titular las conoce; y, ante tal confianza de las entidades bancarias y por no adaptar medidas necesarias para evitar patrones de fraude, se originan los reclamos por operaciones que el usuario no las reconoce. Esto es que, el Banco no ha prevenido que se cometa dichas operaciones aplicando las medidas de seguridad, por lo tanto ha infringido la idoneidad del servicio que le había ofrecido al usuario que contrató las tarjetas.

En ese sentido, el propósito de este trabajo de investigación es analizar resoluciones emitidas por la Órgano Resolutivo de Procedimientos Sumarísimos del Indecopi-La

Libertad en los periodos 2017 al 2019 para determinar si es que la entidades bancarias cumplen con el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito. Asimismo, se analizará dentro de la legislación internacional los aspectos normativos sobre el deber de idoneidad en los servicios bancarios, para que se realice una comparación con la legislación peruana, por último, se determinará mediante encuestas a usuarios de los Bancos de la región La Libertad la afectación que les causan los Bancos por haberse efectuado el fraude electrónico con tarjetas de crédito y débito.

1.2. Antecedentes

La presente investigación es importante para el derecho, debido a que aborda un tema de la cual no existen muchos estudios realizados en nuestro país. Es por ello que se ha escogido algunos artículos y tesis que tengan mayor relación con el tema de investigación:

1.2.1. A nivel internacional:

1.2.1.1. En el artículo de investigación titulado "Responsabilidad de las entidades financieras en eventos de fraudes electrónicos" publicado en la Revista Nueva Época de la Universidad Libre, Guarnizo y Segura (2018) concluyen que las entidades financieras tienen la responsabilidad por un fraude electrónico, debido a que su simple actividad exige que no solamente se deban tener mecanismos de control y seguridad, sino que también se debe responder de todas las amenazas y vulneraciones que se pueden llegar a presentar con los usuarios y sus respectivas cuentas. Es la entidad quien debe ser responsable por su función de las actividades que realiza y no excusarse que por utilizar los medios de seguridad disminuye las obligaciones y responsabilidades frente a los usuarios.

1.2.1.2. En la tesis "Predicción del fraude con tarjetas para una entidad financiera a través del modelo Arimax", de la Universidad Los Libertadores- Sede Bogotá Molano y Correa (2016) concluyeron que las entidades bancarias deben de tomar medidas orientadas a disminuir el fraude por internet para que se siga manteniendo una buena reputación frente al cliente.

1.2.1.3. En el artículo científico "La culpa del consumidor en la responsabilidad financiera y proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia", publicado en la Revista de Derecho Privado de la Universidad Externado de Colombia, Paz (2018) señala que el banco debe tener especial diligencia y el consecuente derecho del consumidor a tener servicios y productos con esquemas de calidad. Asimismo, concluye que si la entidad bancaria no cumple con las medidas para prevenir fraudes electrónicos se hallaría su responsabilidad.

1.2.2. A nivel nacional:

1.2.2.1. La tesis para optar el título de abogado de la Pontificia Universidad Católica del Perú "El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación", Meza (2012) concluye que con las tarjetas tanto el Banco como los del establecimiento afiliado deberán cumplir con la idoneidad del servicio ante el usuario.

1.2.2.2. En la tesis "La idoneidad en las tarjetas de crédito: a propósito de las denuncias ante los órganos competentes de Indecopi durante los años 2013-2015", Bellido (2018) concluye que la idoneidad en ambas tarjetas tanto las de débito como de crédito, el usuario debe tener en cuenta la información que le han brindado

los Bancos, debido a que de esa manera conocerán sus derechos, deberes y beneficios que conlleva tener este tipo de tarjetas, el punto de quiebre en donde se da el incumplimiento de este deber, es cuando el consumidor no recibe lo que el proveedor le había ofrecido.

1.3. Bases Teóricas

1.3.1. Usuario o consumidor

Es toda persona ya sea natural o jurídica que opta por un comprar un producto o adquirir un servicio con la finalidad de satisfacer sus necesidades así como lo establece el Artículo IV del "Código de Protección y Defensa del Consumidor" que el usuario o llamado también consumidor puede ser toda persona que va a querer comprar un producto o contratar un servicio, para su beneficio o la de su familia, actuando esta persona como último destinatario.

1.3.2. Deber de idoneidad

El Artículo 18° del "Código de Protección y Defensa del Consumidor" señala que: "Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo efectivamente recibe en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso".

Asimismo, en el artículo 19° hace hincapié que el proveedor que ofrece su servicios o los productos, se va a hacer responsable por la calidad y la idoneidad de lo que brinda.

Indecopi en su publicación lineamientos de protección al consumidor, define que la idoneidad no se basa solamente en lo que se ha acordado, sino que

también se basa por lo que se ha pactado y por la confianza que generan ante el consumidor, ya sea por la posición que tiene el proveedor en el comercio.

En la Resolución N° 134-2008/SC2-INDECOPI del 16 de octubre de 2008, resuelven que se presume que un producto es idóneo para las necesidades que se requiere en el comercio, teniendo en cuenta las circunstancias de los servicios o productos.

1.3.2.1. Deber de idoneidad en los servicios ofrecidos por los Bancos

El deber de idoneidad es aplicado por los Bancos cuando cumplen con brindar a sus clientes lo que se ha pactado y lo que han informado en el contrato cuando se adquirió la tarjeta de crédito o débito, sin embargo el servicio idóneo no solo concierne a emitir la tarjeta de crédito y otorgar la clave secreta, sino que al existir casos de fraude los Bancos deben adoptar medidas de seguridad a fin de que no se realice operaciones por internet por terceras personas con solo tener la información de las tarjetas, para que así no se pueda perjudicar al patrimonio del titular.

No obstante, Indecopi en una de sus Resoluciones N° 0368-2019/PSO-INDECOPI-LAL en su fundamentos señala que el Banco infringe el deber de idoneidad cuando no adoptó las medidas de monitoreo y alerta para realizar 7 operaciones de consumo con la tarjeta del usuario.

Por lo tanto, los Bancos infringe el deber de idoneidad con el servicio de las tarjetas de crédito o débito cuando:

- No alerta al titular por llamadas telefónicas.
- No bloquea temporalmente la tarjeta.

- No realiza patrones de seguimiento y supervisión en la conducta habitual de consumo. El "Reglamento de Tarjetas de Crédito y Débito" N° 6523-2013 en el artículo 2 inciso 5) establece que se entiende por comportamiento habitual de consumo las operaciones que el usuario frecuentemente realiza con sus tarjetas, considerando factores, como por ejemplo el canal que utiliza, el país, los lugares en donde compra, entre otros, esta información puede ser determinada a través de la frecuencia de las operaciones que el titular realiza y que son registradas por la entidad bancaria.
- No cuenta con un sistema de monitoreo para detectar cuando una transacción no corresponde al consumo habitual que el cliente utiliza su tarjeta.
- Cuando se realizó una operación sin que el titular haya habilitado expresamente su tarjeta para realizar operaciones por internet.
- Cuando se ha realizado una operación vía internet sin haberse validado correctamente los datos importantes de la tarjeta tales como: clave secreta, códigos de seguridad contenido en la tarjeta, número de la tarjeta, fecha de caducidad, CVV (código de verificación) y claves adicionales.

1.3.2.2. Carga de la prueba

Es atribución del consumidor acreditar que existe una deficiencia en el servicio que se le ha brindado y que le ha causado un perjuicio, no obstante, después el proveedor puede demostrar que la deficiencia que señala el usuario no le es atribuible.

El artículo 104° del "Código de Protección y Defensa del Consumidor" señala que el proveedor se exonera de la responsabilidad administrativa cuando va a

acreditar una causa justificada, objetiva y que configura la ruptura que el hecho fue por caso negligente del consumidor, hechos ocasionados por un tercero o caso fortuito. Asimismo, la "Ley de Procedimiento Administrativo General"- Ley N° 27444 en su artículo 162° inciso 2 establece que corresponde al supuesto responsable aportar pruebas mediante documentos, informes, testimonios o aducir alegaciones.

1.3.3. Sistema Bancario

Según la "Superintendencia de Banca y Seguros y AFP" (SBS) en su guía "Programa finanzas en el cole" en el año 2017, señala que dicho sistema es aquel cuyo rubro de negocio es captar dinero del público en forma de depósito u otra modalidad contractual, y ofrecen créditos a las personas que lo necesitan en diferentes modalidades.

Asimismo, establece dos modalidades en las que se divide el sistema bancario siendo:

1.3.3.1. No Bancario

No son consideradas como Bancos, pero captan y canalizan los recursos; dentro de esta clasificación se encuentran:

1.3.3.1.1. Empresas financieras

Aquellas que captan los recursos del público y facilitan la colocación de emisiones de valores, utilizando valores mobiliarios y brindan asesoría financiera a los usuarios.

1.3.3.1.2. Microfinancieras

a) **Cajas rurales:** Capta recursos del público y otorga financiamiento a las medianas, pequeñas y microempresas de las zonas rurales.
b) **Edpymes:** Otorga financiamiento a las pequeña y microempresa, está en sus funciones captar fondos del público
c) **Cajas Municipales:** Financia operaciones a las micro y pequeñas empresas
d) **Empresas de arrendamiento financiero:** Adquieren bienes muebles e inmuebles que serán otorgados en uso a persona jurídicas o naturales, por una renta mensual y con la opción de compra del bien.
e) **Empresas de factoring:** Su especialidad consiste en adquirir facturar y cualquier valor mobiliario que represente una deuda.
f) **Almacenes de depósito:** Realizan almacenamiento, custodia o conservación de bienes y mercancías, y también emiten certificados de depósito.
g) **Empresas fiduciarias:** Se encarga de administrar patrimonios fiduciarios.

1.3.3.2.Banca Múltiple

Conocido como banca comercial o privada, en la cual su función es contar con diversos instrumentos para captar y canalizar recursos.

1.3.3.2.1. Productos y servicios

La Ley N° 26702 “Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros” en el Art. 283° (Articulo modificado mediante D. Leg. N° 1028-2008) menciona en el Art. 221° las operaciones que las entidades bancarias están facultadas

para realizar, entre las 44 operaciones que le autorizan realizar a los Bancos, está en el numeral 34 el administrar y otorgar tarjetas de crédito y débito.

1.3.3.2.1.1.Tarjeta de Crédito

Además, la "Superintendencia de Banca y Seguros y AFP" (SBS) en la "Resolución S.B.S N° 5570-2019" define en su artículo 3°:

> Artículo 3.- "La tarjeta de crédito es un instrumento de pago que puede tener soporte físico o representación electrónica o digital y que está asociado a una (1) línea de crédito, otorgada por la empresa emisora. De acuerdo con lo establecido en el respectivo contrato, a través de la tarjeta de crédito, el titular (o usuario) puede realizar el pago por bienes, servicios u obligaciones, así como hacer uso de los servicios adicionales conforme a lo establecido en este reglamento".

Castro (2014) define que esta tarjeta tiene un crédito asociado, para que el usuario pueda realizar pagos generándose un interés por hacer uso de su tarjeta.

La tarjeta de crédito es el instrumento plastificado que los Bancos otorgan para facilitar a los consumidores al realizar sus operaciones, debido a que mediante esta se les presta dinero. Al otorgarse estas tarjetas los Bancos establecen mediante un contrato las obligaciones que el usuario debe de tener en conocimiento. Además, el usuario tendrá que cumplir con pagar en una determinada fecha a la entidad bancaria por el uso que ha efectuado con la tarjeta, aplicándose una tasa de interés.

1.3.3.2.1.1.1. Contenido del contrato

El Art. 5° del Reglamento N° 5570-2019 que modifica el "Reglamento de Tarjetas de Crédito y Débito" (reglamento que entra en vigencia en enero de 2021) establece la información que debe tener el contrato al momento de que se adquiere la tarjeta de crédito:

- Condiciones para reducir y aumentar la línea crediticia, así como los mecanismos que se aplicaran para solicitar el consentimiento del usuario para el aumento de la línea crediticia.
- La forma y los medios en las que se puede pagar.
- Responsabilidades y los procedimientos cuando la tarjeta se pierda, la sustraigan, roben o hurten.
- Casos en la cual se va a bloquear o anular la tarjeta de crédito y cuando se daría resuelto el contrato.
- Condiciones para que se pueda renovar el contrato.
- Fechas que se entregarán los estados de cuenta.
- Nombres completos del titular a quien se le emitirá el estado de cuenta.
- Condiciones en la que se van a emitir el estado de cuenta de manera física o electrónica y el plazo de aceptación.
- La imputación para el pago de línea de crédito no debe ser confusas para el usuario.
- Cuando se exceda la línea de crédito, las condiciones deben ser por montos razonables.
- Información y condiciones sobre los servicios asociados a la tarjeta de crédito.

1.3.3.2.1.1.2. Información contenida en la tarjeta de crédito

El Art. 6° del "Reglamento de Tarjetas de Crédito y Débito" señala que las tarjetas de crédito deben tener lo siguiente:

- La denominación social de la empresa que otorgue el producto, además de la marca a la que pertenece, si fuera el caso.
- Número de tarjeta.
- Nombres completos del titular y su firma. La firma puede ser una clave o firma que permita identificar si es que el usuario es quien está realizando la operación.
- Caducidad de la tarjeta, el plazo no puede exceder los 5 años.

1.3.3.2.1.1.3. Servicios adicionales a las tarjetas de crédito

El Art.7° de la "Resolución N° 5570-2019 que modifica el Reglamento de tarjetas de crédito y débito" señala que los bancos otorgaran a los usuarios los siguientes servicios:

- Disponer de efectivo, señalando el número de cuotas en las que se pagará lo utilizado.
- Compra, consumir o pagar utilizando páginas de internet y/o aplicaciones móviles.
- Operaciones o consumos realizados en el exterior con la tarjeta física.
- Exceso de la línea de crediticia.

Los servicios adicionales se pueden incorporar en el momento de la celebración del contrato o después, teniendo la facultad de deshabilitar cuando el titular lo desee.

Los Bancos tienen que informar las condiciones que serán aplicadas y los riesgos que puede acarrear al utilizar estas tarjetas, además de las medidas de seguridad que se debe tener cuando se hace uso de los servicios, en cualquiera de los canales autorizados.

1.3.3.2.1.1.4. Activación de tarjeta de crédito

La entidad bancaria activa la tarjeta cuando es solicitada por el titular, una vez que le haya sido entregada; en algunos casos la tarjeta puede ser activada automáticamente por el banco luego de ser entregada.

1.3.3.2.1.1.5. Cargos

Las entidades bancarias cargarán el monto de los bienes, obligaciones o servicios que el usuario haya adquirido utilizando su tarjeta, en los servicios que se le autorizó, dichos cargos con los comprobantes de pago que el titular autorizó.

1.3.3.2.1.2. Tarjeta de débito

Se entiende por esta tarjeta según Boquera citado en Soto (2015) indica que es lo que va a permitir que se obtenga dinero en la entidad de crédito emisora o en otras entidades unidas a la red, mediante la exhibición en la oficina bancaria o haciendo uso de los cajeros automáticos.

La "Superintendencia de Banca y Seguros y AFP" (SBS) en la "Resolución S.B.S N° 5570-2019" que modifica el "Reglamento de Tarjetas de Crédito y Débito" define en su artículo 4°:

Articulo 4.- "La tarjeta de débito es un instrumento de pago que puede tener soporte físico o representación electrónica o digital, que permite realizar operaciones con cargo a depósitos previamente constituidos

en la empresa emisora. A través de la tarjeta de débito el titular puede realizar el pago de bienes, servicios u obligaciones, efectuar el retiro de efectivo o realizar transferencias, a través de los canales puestos a disposición por la empresa emisora u otros servicios asociados, dentro de los límites y condiciones pactadas".

Según Flores, Pilco y Haro (2015) señalan que la tarjeta de débito permite utilizar el dinero que ha sido depositado en una cuenta corriente o de ahorro en la que el usuario esté asociado. Dicha tarjeta puede ser utilizado para retirar dinero en cajeros u oficinas, así como para realizar pagos en establecimientos. La operación se realiza inmediatamente a la cuenta, que en principio se debe contar con saldo suficiente.

1.3.3.2.1.2.1. Información mínima de la tarjeta

El artículo 12° del citado Reglamento menciona que la tarjeta de débito debe contener lo siguiente:

- Nombre del banco que emite la tarjeta, así como el sistema al que pertenece.
- Número de tarjeta.
- Fecha de vencimiento (no deberá exceder los 5 años).
- Mecanismos que permitan identificar al cliente, ya sea por una clave que se le otorga al usuario y que tiene que ser cambiada.

1.3.3.2.1.2.2. Servicios asociados

En el Art. 13° del mencionado Reglamento y modificado mediante Resolución N° 5570-2019 se establece los servicios que los titulares pueden hacer uso, según corresponda:

- Consumos, compras o pagos por internet.
- Operaciones efectuadas en el extranjero.

Los servicios señalados se deben informar en el momento de que se firma el contrato, y el titular tiene la facultad de habilitarlos o deshabilitarlos cuando lo requiera. Asimismo, los Bancos deben de comunicar a los usuarios las condiciones y los riesgos asociados, además tienen que informar las medidas de seguridad que debe tener el usuario cuando usa su tarjeta.

1.3.3.2.1.2.3. Cargos

Los Bancos cargarán a la cuenta de la tarjeta el importe de lo que haya adquirido el usuario como consecuencia de los servicios que se le han autorizado.

1.3.3.2.1.3. Medidas de seguridad contenidas en la tarjeta de crédito y débito

Según la "Superintendencia de Banca y Seguros y AFP"(SBS) en el "Reglamento de Tarjetas de Crédito y Débito", Resolución S.B.S N° 6523-2013 establece algunas de las medidas que deben implementar los Bancos con respecto de ambas tarjetas, debiendo contar con un chip integrado y una clave secreta que va a servir identificar al usuario, además de aplicar una técnica de autenticación que brinde seguridad, así también como disponer mecanismos sobre el chip que contienen las tarjetas para una operación en línea con la finalidad de modificar los perfiles de riesgo.

Además, se establece medidas de seguridad con respecto a lo que se le otorgará al usuario, de acuerdo al Art. 16° del reglamento (modificado por Resolución N° 5570-2019) al considerar que cuando se entrega la tarjeta al usuario con una primera clave generada por el Banco, en la cual el titular debe realizar el cambio de la clave antes de efectuar la primera operación, y cuando se utilice una clave como autenticación se debe de admitir que el usuario pueda cambiar la clave cuantas veces lo requiera.

No obstante, dicho artículo también menciona la medida de seguridad que debe implementar los Bancos en caso de que se identifique que se esté cometiendo un fraude con dichas tarjetas, estableciendo lo siguiente:

Articulo 16.- Medidas de seguridad respecto a los usuarios:

"(…) 4. Para las operaciones que se realicen con cargo a la línea de crédito o a los depósitos previamente constituidos, la empresa debe habilitar y brindar un servicio de notificaciones para todos los usuarios para que se les informe de las operaciones realizadas con sus tarjetas inmediatamente después de ser registradas por la empresa, mediante la utilización de alguno de los siguientes mecanismos de comunicación directa tales como mensajes de texto, correo electrónico, llamadas, entre otros, que pueden ser pactados con los titulares; debiendo este servicio estar activo desde el momento de la contratación del producto. Para este servicio, las empresas pueden establecer mecanismos a través de los cuales los usuarios puedan configurar o limitar las notificaciones sobre la base de umbrales o variables como montos mínimos, entre otros. Los titulares pueden

solicitar la habilitación o deshabilitación de este servicio, en cualquier momento, a través de los mecanismos establecidos por las empresas, los cuales no podrán ser más complejos que los ofrecidos al momento de la celebración del contrato".

Por lo tanto, las empresas bancarias al detectar un fraude que va a perjudicar al titular de la tarjeta tienen el deber de avisar al usuario a través de notificaciones mediante mensajes a través del correo electrónico o al número de celular que el titular proporcionó en el momento de adquirir tales productos, considerándose que se debería enviar primero al celular debido a que dicho dispositivo se usa con mayor frecuencia y se puede leer la notificación de las operaciones inmediatamente.

Así también, se establece el artículo 17° con respecto a la realización de operaciones que los usuarios van efectuar usando sus tarjetas, es así que se debe contar con el sistema de monitoreo de operaciones, con la finalidad de que se detecte operaciones que no corresponde al comportamiento usual de consumo del usuario; los Bancos tienen que implementar procedimientos que complementen la gestión de alertas; usar un mecanismo de autenticación; en caso de que el usuario decida realizar retirar el efectivo deberá de requerirle la clave secreta, para todo tipo de operación, pero que medida se considera cuando se detecta fraude, en el numeral 3 y 4 de dicho artículo se establece así:

Articulo 17.- Medidas respecto al monitoreo y realización de operaciones:

3. “Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones”.

4. Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude.

Es decir, al momento de que los Bancos identifiquen que se está efectuando fraude debe de constatar con la historia de consumos que el titular tiene, esto es por la habitualidad del consumo que realiza el usuario. Por otro lado, el Art. 18° del citado Reglamento se establece las medidas que se deben implementar con respecto al procesamiento, almacenamiento y ceder los datos que contienen las tarjetas, entre ellas se tiene que las empresas bancarias deben de adoptar configuraciones para restringir permisos y evitar accesos que no sean autorizados; implementar técnicas para que el uso de la clave secreta, mantener sistemas y aplicaciones que sean seguras; tener monitoreado y registrar los accesos a redes y a datos de los titulares, entre otras.

Por último, las medidas que se han señalado son con respecto a los controles que las entidades bancarias deben cumplir con las medidas señaladas, también se establece las medidas de seguridad que se deben implementar para las operaciones que corresponden a fraude, es así que el artículo 22° del Reglamento (modificado por la Resolución N° 5570-2019) señala que el Banco debe tener procedimientos para que se realice el seguimiento de operaciones que se están efectuando a causa de fraude, señalándose lo siguiente:

Artículo 22°. - Seguimiento de operaciones que pueden corresponder a patrones de fraude

"1. Mecanismos para la comunicación inmediata al usuario sobre las posibles operaciones de fraude.

2. Acciones para proceder con el bloqueo temporal o la cancelación definitiva de la tarjeta, en caso sea necesario".

Por lo tanto, cuando las entidades bancarias al detectar que se están realizando operaciones a causa del fraude a través de internet o aplicativos móviles debe comunicar inmediatamente al usuario a través de un mensaje de texto al teléfono móvil y/o al correo electrónico como ya se había especificado líneas arriba, y tomar las acciones correspondientes como son la que se procesa a bloquear o la cancelación de la tarjeta de débito o crédito.

1.3.3.3. Cláusulas abusivas

La "Constitución Política del Perú" en el art. 65° consagra la tutela efectiva que protege al consumidor en situaciones que no perjudiquen en sus intereses, garantizando la información sobre productos y servicios que se ofrezcan en el comercio, para ello que se han emitido normas sobre el contrato de consumo que busca equilibrar una buena práctica en la contratación, sin embargo está la asimetría informativa entre ambas partes del contrato, que ocasiona que el Banco tiene mayor conocimiento de lo que ofrece y que redacta sus cláusulas generales del contrato, por lo tanto debe informar de modo transparente y entendible hacia la otra parte, quien cree que el proveedor actúa de buena fe, si el proveedor no otorga la información idónea, clara y completa se ocasionará

un desequilibrio de la posición del consumidor, que va a provocar que este en desproporcionalidad. (Arana, SF).

Herrera (2015), señala que se consideran cláusulas abusivas las que permiten modificar unilateralmente el contenido del contrato; trasladar al consumidor la responsabilidad que tiene el proveedor; disponer términos de prescripción; exoneren la responsabilidad del proveedor por vicios en lo que ofrece, o por la insuficiente información de los peligros o condiciones de utilización de los servicios; impongan al consumidor cargas probatorias diferentes a las que les corresponda; autoricen la terminación del contrato de manera unilateral por parte del proveedor; se establezca que el proveedor no reintegre lo pagado; autoricen al proveedor a modificar unilateralmente tarifas o condiciones pactadas; inviertan la probanza en perjuicio del consumidor; excluyan la obligación del proveedor a respetar los acuerdos; impongan al consumidor prestaciones adicionales; impongan al deudor la obligación de celebrar otros contratos accesorios.

1.3.4. Fraude electrónico

Es definido como la acción que se ha originado ante el avance del internet, este crecimiento ha traído un riesgo de fraude, facilitando los ataques cibernéticos mediante virus; a través de diferentes estrategias por el defraudador tales como la falsificación de la banda magnética, el cambiazo, la suplantación, el robo y el extravío. (Molano y Correa, 2016).

Además, Rodríguez (2014) define al fraude electrónico como la conducta que es realizada por un tercero ajeno al titular de la tarjeta, que no ha sido autorizado ni consentido por este, además que realiza transacciones por conductos web y

que le causa un perjuicio. También, Sarmiento (2015) señala que el fraude electrónico se da cuando se utilizan sistemas comerciales lícitos, y le dan una utilización indebida de tal manera que se origine una pérdida de valor.

En efecto el fraude electrónico es realizado por terceras personas que no tienen el consentimiento del titular de la tarjeta para que puedan realizar compras por internet. El hecho delictivo lo realizan con solo tener información necesaria de las tarjetas como clave y dígitos, ya que esa información se solicita al momento de realizar operaciones.

El fraude electrónico se ha propiciado con el desarrollo de las tecnologías, es eso lo que ha favorecido a la creación de fraudes. Gabaldón (2006) menciona que el desarrollo de Internet abre el suceso de negocios y de fraudes a una escala inimaginable hace dos décadas. La unión de tecnologías origina obtener información de personas que forman parte de organizaciones; las tarjeta de crédito o débito es la herramienta que se puede clasificar, analizar y seleccionar las vidas de la gente para tales fines.

1.3.4.1. Tipos de fraude electrónico:

Las operaciones no reconocidas que se realiza por una tercera persona se realizan por extravío, hurto y otros tipos de fraudes electrónicos comunes como son:

- **Phishing:**

Se realiza utilizando el engaño de que el cliente ha ganado un premio y que tiene que ingresar mediante una página web e ingresar su clave secreta y número de tarjeta, esto originando que esta información sea guardada y

utilizada para suplantar al cliente, generando compras o transferencias de su dinero (Balcazar, 2017).

Porco (2015) señala que el phishing es una técnica que es realizada por los delincuentes a fin de obtener la información confidencial tales como: nombres de usuario; contraseñas; número de tarjeta de crédito, haciéndose pasar por una comunicación que es confiable y segura.

- **Clonación o Skimming:**

Este tipo de fraude Cabrera y Lombana (2016) señalan que es un fraude moderno, que se trata de clonar la tarjeta en otra tarjeta en blanco. Este tipo de modalidad se puede realizar cuando los delincuentes se hacen pasar como empleados y ofrecen ayudar a usar la tarjeta pidiéndole la clave, después la cambian por una tarjeta que es similar a la original pero ya es falsa.

Tal clonación puede ser de manera general o parcial, así como lo señala Javato (2013) explica que cuando la clonación total se va a confeccionar una tarjeta nueva, en cambio con la clonación parcial se graban los datos en una banda magnética adherida a una tarjeta que está en blanco y después se procede a utilizarla en cajeros automáticos para sacar dinero introduciendo el número insertando la clave que solicitan.

Es así que después de haber clonado las tarjetas, las personas inescrupulosas adquieren bienes, servicios o dinero ya sea de manera presencial o través de equipos electrónicos.

- **Mail spoofing:**

Tipo de forma fraudulenta en la que se envía un mensaje para abrir un enlace al correo electrónico, para que se valide la dirección de correo y validar datos

personales. Sánchez (2012) señala que es un procedimiento en donde se crea correos que supuestamente son verdaderos para enviar mensajes, en estos mensajes se suele recibir como por ejemplo este tipo de información: "Este mensaje ha sido enviado por nuestro servidor para verificar su dirección de correo electrónico. A fin de que se valide la dirección, haga clic en el siguiente enlace".

- **Web spoofing:**

  Es una técnica en la cual se hace creer al usuario que la página que está visitando es auténtica cuando realmente el ciberdelincuente solo pretende extraer información. Consiste en hacer creer al internauta que la página que está visitando es real, pero se trata de una réplica que se encuentra monitoreada por un delincuente que lo que quiere lograr es obtener información para que pueda realizar compras en su nombre. (Sánchez, 2012).

- **Smishing:**

  En esta modalidad se realiza a través de celulares, en donde los delincuentes mandan un mensaje para que los usuarios accedan a un enlace y puedan hackear la información del teléfono. Díaz, Angulo y Barboza (2018) señalan que en este delito se utiliza los celulares de los usuarios financieros, para que los delincuentes pretendan suplantar la identidad, con la finalidad de que los usuarios accedan mediante mensaje de texto a un link para hackear el teléfono del usuario.

- **Software espía:**

  El delincuente hace uso de un programador que se instalan en las computadoras que permite que se monitoree las actividades que realiza el

usuario, ya sea que sepa que páginas visita, la información que busca, la información de sus correos electrónicos; el ciberdelincuente lo realiza desde otra computadora. Ñaupas (2016) señala que, mediante tal modalidad, el delincuente a través de una computadora utiliza un software espía que son programas que se instalan sin autorización, esto con la finalidad de averiguar las páginas que visita el usuario o la información que contiene en la computadora.

- **Pharming:**

  Ñaupas (2016) define que consiste en redireccionar al usuario hacia una página web fraudulenta sin que se dé cuenta, es decir que el usuario trata de entrar a una página web similar a la original en donde ingresa su clave y su usuario, responde que hay un error para que intente de nuevo y al intentarlo, lo direcciona al sitio legítimo. Por lo tanto, dicha modalidad utiliza URL falsos haciendo creer que es la página web verdadera a fin de que el usuario ingrese su datos y el delincuente se apropie de esta información para realizar fraudes con los datos que obtuvo.

- **Vshing:**

  En dicha práctica el criminal utiliza números telefónicos de forma aleatoria para informar al cliente que se debe comunicar con tal número telefónico para que se comunique con la entidad bancaria, entonces cuando la víctima se comunica al número que se le proporcionó, le indican que su cuenta tiene que ser verificada y por lo tanto debe proporcionar número de tarjeta, usuario y clave, es así que el delincuente obtiene toda la información para realizar operaciones fraudulenta por canales de internet.

1.3.4.2. Convenio de Budapest

Convenio sobre ciberdelincuencia, es un convenio que entró en rigor el 1 de julio de 2004 y que fue aprobado Estados del Consejo Europeo, asimismo 61 estados firmaron, ratificaron y se adhirieron a dicho convenio, entre ellos está Perú quien se adhirió al Convenio de Budapest en el año 2019 mediante el Decreto Supremo N° 050-2018-PCM dentro de la cual se estableció la Seguridad Digital en el ámbito nacional para dar confianza a los ciudadanos en el medio digital, así también se aprobó la Ley Gobierno Digital mediante Decreto Legislativo N° 1412 que establece la gestión de la seguridad digital en el Perú. Por lo tanto, la adhesión al Convenio de Budapest va a permitir la seguridad digital debido que se habilitará consecuencias para los ciberdelincuentes.

Por otro lado, dicho Convenio establece acciones sobre las acciones contra la piratería, pornografía infantil, violación de la propiedad intelectual, y en especial importancia con respecto al fraude informático, señalando en su Art. 8° que las partes deben adoptar medidas legislativas que resulten necesarias para que se tipifique como delito en cada país que ha suscrito tal convenio, los actos deliberados que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos y la interferencia en el funcionamiento del sistema informático con la intención dolosa de obtener un beneficio económico ilegítimo.

1.3.5. Operaciones no reconocidas

Es importante también definir las dimensiones que se desarrollan en base a las categorías establecidas, recalcándose lo que se origina al efectuarse el fraude electrónico con las tarjetas de crédito o débito. Las operaciones no reconocidas que son reclamados por los usuarios primero ante la entidad bancaria y si no le dan al usuario la solución correspondiente, acuden ante Indecopi para reclamar sobre una operación vía internet que los titulares no realizaron.

Por tal motivo se define como operación no reconocida según el "Reglamento de Tarjetas de Crédito y Débito" (Resolución S.B.S N° 5570-2019) en su artículo 23° menciona que el usuario rechaza la transacción de que tal operación fue realizada incorrectamente. Tales operaciones se pueden realizar de manera presencial o virtual, pero siempre sin el consentimiento del titular; efectuándose a través de páginas web, cajeros automáticos, establecimientos comerciales.

1.3.5.1. Daños que ocasiona las operaciones no reconocidas

Las operaciones que son rechazadas por los usuarios y que han sido efectuadas sin haber adoptado medidas de seguridad por la entidad bancaria, le ocasionan los siguientes daños:

a) **Daños al patrimonio económico:** Se origina este daño, por la conducta del Banco y terceras personas que dispusieron del dinero del consumidor indebidamente, ocasionándole una disminución en su patrimonio. Además, que se invierte tiempo para reclamar por un hecho injusto.

b) **Daño a la persona:** Se ocasiona este tipo de daño cuando el Banco le cobra al usuario por la operación que se ha realizado con la tarjeta mediante internet, no obstante como el usuario rechaza y no paga la deuda que se le

imputa, el Banco reporta ante la SBS con calificación como deficiente, lo que le ocasionaría al usuario un daño moral porque al figurar en la central de riesgo, dañaría su imagen como cliente y como consecuencia no podría celebrar transacción alguna con algún otro Banco.

c) **Daños al mercado:** La conducta del Banco al no adoptar las medidas de seguridad y no cumplir con el deber de idoneidad genera una percepción negativa de los consumidores, debido a que pensarían que tener ese sistema de pagos ocasiona un riesgo permanente para su patrimonio, generando desconfianza e inseguridad respectos a las operaciones que se pueden efectuar con estas tarjetas.

1.3.6. Procedimiento para presentar un reclamo

Cuando se presente el inconveniente de las operaciones por internet que el usuario las rechaza, la SBS recomienda que se puede presentar un reclamo, queja o denuncia; cuando la entidad bancaria no ha prestado adecuadamente el servicio financiero, ocasionando problemas a los usuarios o cuando no ha recibido atención del reclamo por parte del banco o el usuario no está de acuerdo con la solución que se le brinda, así también como otros casos que pueden ser reclamados.

Por lo tanto, el procedimiento para realizar el reclamo ante la entidad bancaria según algunos Bancos es el siguiente:

-**BBVA**: Se podrá hacer el reclamo de manera presencial, mediante banca móvil o banca por internet. El banco tiene 30 días para que responda mediante correo electrónico o el domicilio del usuario, pero también se puede conocer la respuesta por la Banca por Internet, Banca móvil o sede del banco. Si es que el

cliente no está conforme con la respuesta a su reclamo puede acudir a las instancias externas de Defensor del Cliente Financiero, la SBS o Indecopi.

- **Scotiabank:** El usuario podrá presentar un reclamo a través de la Banca telefónica, Red de agencias y Banca por internet, en la cual un asistente brindará la información requerida o indicará el número de la Hoja de Reclamación. Si es que el cliente no está de acuerdo con el reclamo puede presentar una carta dirigida a la última instancia "Ombuds Office" quien se encarga de los casos que no son resueltos a satisfacción de los clientes.

- **Banco de Crédito del Perú:** Para reclamar se puede presentar a través de la página web del Banco, línea de teléfono y asesor de ventas. Si es que no está de acuerdo con la solución que le da el banco se puede presentar una nueva solicitud que incluya información adicional y en base a esto se realizará un nuevo análisis, además se puede acudir al Defensor de Cliente Financiero o acercarse a oficinas de Indecopi.

Asimismo, el abogado Leoni Amaya en la entrevista de RPP Noticias (2017) en la publicación "¿Cuándo presentar un reclamo ante una entidad financiera y cómo hacerlo? señala que puede recurrir a las siguientes instancias.

1° instancia: El usuario debe presentar su reclamo ante el banco sustentando su disconformidad con el servicio, el reclamo es a través del libro de reclamaciones en físico o virtual. El banco tiene 30 días calendario para hacer llegar la solución del caso al usuario, decisión que debe estar fundamentada según el Art. 24° del "Código de Protección y Defensa del Consumidor".

2° instancia: Atención al usuario de la SBS, que investiga la denuncia y sanciona de ser el caso. Asimismo, remite el caso a Indecopi.

3° instancia: El defensor del cliente financiero, instancia que es promovida por el sistema bancario, interviene como mediador entre cliente y la entidad para llegar a un acuerdo. Cabe recalcar, que este órgano solo resuelve reclamos contra Bancos afiliados, los cuales son la mayoría de los Bancos excepto el Banco de la Nación.

4° instancia: Se presente el reclamo ante Indecopi, donde se convocará a audiencia de conciliación con el banco, para que lleguen a un acuerdo con el usuario. Si es que no se llega a un acuerdo, el usuario puede presentar una denuncia ante Indecopi, si la cuantía de reclamo es hasta 3 UIT según el Art.125° y 126° del "Código de Protección y Defensa del Consumidor", será resuelto por el "Órgano Resolutivo de Procedimientos Sumarísimos" y se resolverá en un plazo de 30 días hábiles, si el caso es complejo resolverá la "Comisión de Protección al Consumidor" que puede amonestar, sancionar o dictar medidas correctivas, el plazo para resolver es de 120 días hábiles. Finalmente, como última instancia es la "Sala Especializada de Protección al Consumidor del Tribunal del Indecopi".

1.3.6.1. Competencia de Defensor de Cliente Financiero, Indecopi y SBS

1.3.6.1.1. Defensor de Cliente Financiero:

Según el Reglamento de la Defensoría del Cliente Financiero señala en su Art.7° que se encarga de resolver reclamos que los clientes planteen contra las entidades financieras; promover la conciliación entre el cliente y el banco durante el procedimiento; formular y presentar ante "ASBANC (Asociación de Bancos del Perú)" informes y propuesta encaminado a dar solución al caso y solicitar información a los Bancos vinculados.

Asimismo, según el Art. 8° la admisión para el trámite del reclamo se tiene lo siguiente: a) haber presentado el reclamo previamente al banco o entidad financiera; b) que se presente por escrito en el formulario; c) el formulario debe detallar de manera clara los hechos que motivan el reclamo, la entidad a quien va dirigida, la petición concreta y documentos que sustenten el reclamo.

Además, según el Art. 10° será declarado improcedente el reclamo si no se presenta dentro del plazo de 1 año desde el conocimiento de los hecho y siempre que no transcurran 3 años.

1.3.6.1.1.1. Entidades afiliadas:

Banco Continental	Crediscotia Financiera S. A	Banco Scotiabank Perú S.A.A.
Banco de Comercio	Banco Pichincha	Banco Falabella Perú S.A.
Banco de Crédito del Perú	Banco Interamericano de Finanzas	Banco Ripley Perú S.A.
Banco Interbank S. A	Citibank del Perú S. A	Banco GNB
Financiera Confianza	Financiera QAPAQ S. A	Caja Rural

1.3.6.2. "Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi)":

Según el artículo 2° del "Decreto Legislativo N° 1033"; es el organismo autónomo que se encarga de:

a) Supervisar a las empresa controlando y eliminando las barreras burocráticas ilegales que afectan a las consumidores y empresas.
b) Proteger la libre y leal competencia, sancionando conductas anticompetitivas y desleales.

c) Corregir problemas en el mercado que se originan por prácticas dumping y subsidios.

d) Proteger los derechos de los consumidores, vigilando que la información que dan los proveedores sea la correcta, asegurando con cumplir la idoneidad los servicios y productos que ofrecen en concordancia con la información que se ha brindado y evitando la discriminación.

e) Supervisar el proceso que facilita el comercio al exterior eliminando barreras comerciales no arancelarias.

f) Defender el crédito mediante la conducción de un sistema concursal que reduzca costos de transacción

g) Administrar el otorgamiento y protección de derechos de propiedad intelectual.

1.3.6.3. "Superintendencia de Banca y Seguros y AFP (SBS)":

Se encarga de controlar y regular el sistema financiero, de seguros y privado de pensiones, así como también de las empresas que reciben depósitos del público, tal entidad regulado por la "Constitución Política del Perú" en el Art. 87°.

Sin embargo, Indecopi y la "Superintendencia de Banca y Seguros y Administradoras Privadas de Fondos de Pensiones" en el 2017 firmaron un convenio para reforzar la coordinación entre ambas entidades con el objetivo de cooperar con la mejor realización de las funciones de ambas autoridades según sus competencias, especialmente para proteger al consumidor. Esto es que, el Indecopi informará a la SBS las quejas que

recibe respecto de las entidades bancarias, solicitará un informe que le permita interpretar correctamente los alcances de la" Ley N°26702 -Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros", o las normas emitidas por la SBS, tal y como lo prescribe el Art. 89° del "Código de Protección y Defensa del Consumidor".

Además, Vodanovic citado por Rivera (2017) realiza una diferencia entre las competencias del Indecopi y la SBS:

INDECOPI	SBS
Inicia procedimiento de oficio o de parte por incumplimiento por vulnerar los derechos del consumidor.	Aprueba cláusulas para contratar los productos y servicios que otorgan el sector bancario y sanciona cuando incumplen las normas.
Resuelve controversias	No resuelve controversias
Protección directa	Protección indirecta

1.4. Formulación del problema

¿Las entidades bancarias de la región La Libertad cumplen con el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito en los periodos 2017 -2019?

1.5. Objetivos

1.5.1. Objetivo general

Demostrar si las entidades bancarias de la región La Libertad cumplen con el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito en los periodos 2017-2019.

1.5.2. Objetivos específicos

- Analizar las resoluciones finales sobre procesos de operaciones no reconocidas expedidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi- La Libertad en los periodos 2017-2019, a fin de determinar el cumplimiento del deber de idoneidad de las entidades bancarias de la región La Libertad en las operaciones que se efectúe el fraude electrónico con tarjetas de crédito y débito.
- Analizar dentro de la legislación internacional los aspectos normativos sobre el deber de idoneidad en los servicios bancarios con tarjetas de crédito y débito, con la finalidad de realizar una comparación con la legislación peruana.
- Determinar la afectación que causan las entidades bancarias de la región La Libertad a los usuarios por el fraude electrónico con tarjetas de crédito y débito.

1.6. Hipótesis

Las entidades bancarias de la región La Libertad incumplen el deber de idoneidad en las operaciones que se cometa el fraude electrónico con tarjetas de crédito y débito, debido a que no cumplen con las medidas de seguridad de no alerta al titular por llamadas telefónicas, no bloquear temporalmente la tarjeta, no realizar patrones de seguimiento y supervisión al comportamiento habitual de consumo, no contar con un sistema de monitoreo, se realizó una operación sin que el titular haya habilitado expresamente su tarjeta para realizar operaciones por internet, se ha realizado una operación vía internet sin haberse validado correctamente los datos importantes de la tarjeta.

1.6.1. Hipótesis especificas

- Las entidades bancarias de la Región La Libertad no cumplen con el deber de idoneidad en las operaciones que se efectúe el fraude electrónico con tarjetas de

crédito y débito, debido que mediante las resoluciones expedidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi en los periodos del 2017 al 2019, se han sancionado a los Bancos por la comisión de infracción al deber de idoneidad al no haber adoptado las medidas necesarias para evitar que se realicen operaciones fraudulentas.

- La legislación peruana tiene una mayor una regulación con respecto al deber de idoneidad y con respecto al reglamento de tarjetas de crédito y débito al señalar las medidas de seguridad .
- Se causa daño económico, daño personal y daño al mercado a los usuarios de las entidades bancarias de la región La Libertad por el fraude electrónico con tarjetas de crédito y débito.

CAPÍTULO II. METODOLOGÍA

2.1. Tipo de investigación

Es desarrollada en el tipo de investigación cualitativa, ya que se basa con el propósito de analizar las resoluciones emitidas por el "Órgano Resolutivo de Procedimientos Sumarísimos" para determinar si es que las entidades bancarias de la región La Libertad han cumplido con el deber de idoneidad en el fraude electrónico con tarjetas de crédito o débito, además que se ha analizado legislación comparada y se ha realizado encuestas a usuarios de las entidades bancarias de la región La Libertad. En concordancia con lo que señala Martínez (2006) que la investigación es cualitativa cuando se trata de encontrar la naturaleza de las realidades, aquello que da lógica a la conducta y sus manifestaciones.

Asimismo, la investigación es de diseño no experimental de tipo transversal debido a que se ha basado en una situación para que luego sea analizada, esto es que se va a observar la situación en un determinado momento. Sampieri (2014) establece que el diseño no experimental de tipo transversal es basado en la recolección de datos en un solo tiempo, para describir las variables y su interrelación.

2.2. Población y muestra (Materiales, instrumentos y métodos)

2.2.1. Población:

- Resoluciones de Indecopi, 2017 – 2019 en donde se evidencie la influencia del principio de idoneidad y fraude electrónico con tarjetas de crédito.
- Legislación internacional.
- Población conformada por usuarios de la región La Libertad.

2.2.2. Muestra:

Se eligió de forma aleatoria 15 resoluciones del Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi del periodo 2017 al 2019, legislación internacional y encuestas a usuarios de Bancos en forma aleatoria. Teniendo como criterios de selección lo siguiente:

Muestra	Criterios de Selección
Conformado por 15 resoluciones de los procesos de operaciones no reconocidas a causa de fraude electrónico con tarjetas de crédito y débito emitidos por el "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi en los periodos 2017-2019.	Resoluciones que establezcan en sus decisiones que se vulneró el deber de idoneidad a consecuencia de no haber adoptado medidas de seguridad para evitar el fraude electrónico.
	Se tomó en cuenta resoluciones que sancionen a Bancos por incumplimiento de las medidas de seguridad por ser un deber de idoneidad.
	Resoluciones emitidas por el "Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi- La Libertad".
Legislación internacional de Chile, Ecuador y Colombia.	Se seleccionó legislación internacional Chilena, Ecuatoriana y Colombiana para conocer los aspectos normativos sobre el deber de idoneidad en los servicios bancarios con tarjetas de crédito y débito.
Encuesta a 40 usuarios de las entidades bancarias de la región La Libertad.	Se estimó encuestar a usuarios de las entidades bancarias para determinar si han sido víctimas de fraude electrónico con sus tarjetas de crédito o débito, así como también para determinar el daño causado.

2.3.Técnicas e instrumentos de recolección y análisis de datos

2.3.1. Métodos:

2.3.1.1. Método analítico: Debido a que se analizará las resoluciones expedidas por el "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi- La Libertad sobre procesos de operaciones no reconocidas a causa del fraude electrónico con tarjetas de crédito y debido para determinar si la entidad bancaria ha cumplido con el

deber de idoneidad. Además, que se analizará legislaciones internacionales de Chile, Colombia y Ecuador para de realizar una comparación con la legislación peruana con respecto al deber de idoneidad en los servicios bancarios con tarjetas de crédito y débito.

2.3.1.2. Método inductivo: Debido a que, mediante el análisis de las resoluciones de operaciones no reconocidas emitidas por el "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi- La Libertad a causa del fraude electrónico con tarjeta de crédito y débito, se va a determinar la conclusión de la investigación. Asimismo, se ha realizado un análisis de legislación internacional para realizar una comparación con la legislación peruana, por último, se ha realizado encuestas a usuarios de las entidades bancarias para determinar la afectación que se ha causado a consecuencia del fraude electrónico. Se aplicado este método porque se está analizando de hechos particulares para que se llegue a una conclusión general.

2.3.2. Técnicas de recolección de datos:

2.3.2.1. Análisis de resoluciones: Esta técnica ayudará a determinar si es que la entidad bancaria de la región La Libertad cumple con el deber de idoneidad en las operaciones donde se cometa el fraude electrónico con tarjetas de crédito y débito mediante el análisis de las resoluciones emitidas por el "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi- La Libertad en los periodos 2017- 2019, esto con la finalidad de dar criterios de validez y confiabilidad a la investigación basándose en los criterios que se han tomado al momento de tomar una decisión.

2.3.2.2. Análisis de legislación internacional: Esta técnica se ha realizado para una comparar la legislación chilena, ecuatoriana y colombiana con la legislación peruana

sobre los normativas del deber de idoneidad en los servicios bancarios con tarjetas de crédito y débito.

2.3.2.3. Encuestas a los usuarios de las entidades bancarias: Se empleó esta técnica de encuestar a 40 clientes financieros de la región La Libertad, con el propósito conocer si es que en algún momento han sido afectados por fraude electrónico con sus tarjetas de crédito o débito, si es que el banco tomo las medidas necesarias para evitar el fraude electrónico y para conocer si es que le causó algún daño.

2.3.3. Instrumentos de recolección de datos:

Técnica	Instrumento	Características
Análisis de datos	Cuadro resumen de resoluciones de Indecopi, 2017-2019	Instrumentos que consisten en el análisis de resoluciones obre operaciones no reconocidas por haber infringido el deber de idoneidad al no haber adoptado las medidas de seguridad para que se cometa el fraude electrónico con tarjetas de crédito y débito. Dichos instrumentos han sido validados por especialistas en la materia, para que se tenga puntuaciones de confiabilidad en la investigación. Además, para que se determine si dichos instrumentos tienen criterios de calidad para llegar a la conclusión si los Bancos de la región La Libertad cumplen o no con el deber de idoneidad.
Análisis de legislación internacional	Cuadro comparativo	Instrumento que consiste en realizar una comparación de la legislación peruana y la legislación chilena, ecuatoriana y colombiana con la finalidad de conocer la regulación con respecto al deber de idoneidad en los servicios bancarios y comparar con la regulación de Perú.
Análisis de encuestas	Encuestas	Se recolectaron las opiniones a través de las encuestas a los usuarios de Bancos de la región La Libertad para determinar si es que han sido víctimas de cobro por operaciones no reconocidas a causa del fraude electrónico con sus tarjetas, para determinar el daño que se les ha causado.

2.4. Procedimiento de recolección, tratamiento y análisis de datos:

2.4.1. Procedimiento en análisis de resoluciones:

Se buscó las resoluciones en la página de Indecopi en la materia de protección al consumidor, señalándose el año, el área ("Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor"). Luego se verificó si eran resoluciones de la región La Libertad, después se descargó para que se verifique si es una resolución que cumpla con los criterios que se ha señalado en la muestra. Después de haberse leído cada resolución, se seleccionó las resoluciones que contribuyen con el tema de investigación y se procesó mediante un cuadro de resumen en Microsoft Word; donde antes del cuadro se colocaron los datos generales: expediente, resolución, banco infractor, imputación de cargos, fundamentos relevantes y decisión.

2.4.2. Procedimiento en el análisis de legislación internacional:

Se indagó legislación internacional teniendo como criterio de búsqueda la delimitación de la norma que contenga las variables estudiadas en la presente investigación, además de su tipología y el contenido. Después se eligió a los países de Chile, Colombia y Ecuador que son países de Latinoamérica que va a permitir conocer el panorama de tales países en derechos de consumidores.

2.4.3. Procedimiento en las encuestas a los usuarios de los Bancos:

Se realizó el cuestionario en la cual se elaboraron 10 preguntas de selección múltiple, después se les entregó la encuesta a los usuarios de las entidades bancarias que fueron escogidos de manera aleatoria; explicándoles primero en qué consistía la hoja de preguntas y la finalidad de la encuesta para que las personas no puedan desconfiar al respecto. Después de haber recabado la

información se realizó cuadros estadísticos empleando Microsoft Word, estableciendo en los cuadros los porcentajes por cada respuesta del cuestionario.

2.5. Aspectos éticos:

La presente investigación jurídica ha tenido los siguientes aspectos éticos: primero se han validado los instrumentos por especialistas en el tema de protección al consumidor. Asimismo, en la legislación internacional se ha optado por legislaciones que regulen al deber de idoneidad para que se puedan comparadas con la legislación peruana, así también con respecto a las encuestas; a los usuarios de las entidades bancarias de la región La Libertad se les explicó que las encuestas que se están realizando es para fines académicos y se les explicó el tema de investigación.

Asimismo, en la recaudación de la información se han utilizado las citas "APA" a fin de respetar los conocimientos de los autores que han elaborado sus investigaciones y que han contribuido con esta investigación, además se ha utilizado tal formato para dar transparencia al desarrollo del presente trabajo.

CAPÍTULO III. RESULTADOS

En la elaboración de los resultados, las resoluciones analizadas son a base a los criterios que se han establecido en la muestra, de esta manera se cumple con haberse seleccionado resoluciones que avalen a la realidad problemática que se ha planteado. Además, en observancia de las resoluciones se corrobora que el "Órgano Resolutivo de Procedimientos Sumarísimos" del Indecopi- La Libertad, resuelve en función al cumplimiento del deber de idoneidad que deben tener las entidades bancarias al adoptar medidas de seguridad para evitar el fraude electrónico con tarjetas de crédito y débito.

Así también, se analizó legislación internacional los aspectos normativos sobre el deber de idoneidad en los servicios bancarios para realizar una comparación con la legislación peruana, además se realizó las encuestas a los usuarios de los Bancos de la región La Libertad, todo esto para determinar el daño que se les ha ocasionado a causa del incumplimiento del deber de idoneidad de las entidades bancarias en el fraude electrónico sus tarjetas de crédito o débito; esta hipótesis se ha podido concretar con los siguientes resultados:

3.1. RESULTADO RESPECTO AL OBJETIVO ESPECÍFICO N° 01: Analizar las resoluciones finales sobre procesos de operaciones no reconocidas expedidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi- La Libertad en los periodos 2017-2019, a fin de determinar el cumplimiento del deber de idoneidad de las entidades bancarias de la región La Libertad en las operaciones que se efectúe el fraude electrónico con tarjetas de crédito y débito.

Con respecto a dicho resultado se ha utilizado el análisis jurídico para deducir el cumplimiento del deber de idoneidad de las entidades bancarias de la región La Libertad en las operaciones que se han efectuado por el fraude

electrónico con tarjetas de crédito y débito; para ello se ha utilizado la técnica de análisis de datos y el instrumento de cuadro de resumen.

Tabla 1

Tabla de Análisis de Resolución N° 01

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0541-2018/PSO-INDECOPI-LAL **Resolución Final N°0238-2019/ PSO-INDECOPI-LAL** **Banco infractor** **Banco Pichincha**	Presunta infracción al art.19° del "Código de Protección y Defensa del Consumidor", en tanto que el Banco no habría adoptado medidas de seguridad para evitar que se realicen 7 operaciones a través de internet con cargo a la tarjeta de crédito del titular por un monto total de S/769.13, las mismas que no son el comportamiento habitual de consumo	El Banco para sustentar la validez de la operación materia de denuncia presentó los print de pantalla dentro de las cuales no se verifica datos relevantes para que se acredite la validez de las operaciones tales, como la hora de la operación, constancia de ingreso de la tarjeta, ingreso del código de seguridad, ingreso de clave secreta, código de autorización los cuales puedan acreditar la validez de las operaciones, asimismo en el desarrollo de la transacción el banco debía activar las medidas de seguridad tales como llamadas telefónicas o bloqueos temporales, como parte del deber de idoneidad.	Sancionar al Banco Pichincha con multa de 3 UIT por infracción al art. 19° del mencionado Código. Se ordena al Banco como medida correctiva reparadora que devuelva el monto efectuado por las operaciones no reconocidas, más intereses, comisiones, penalidades y gastos generados.

Fuente: Elaboración propia

Tabla 2

Tabla de Análisis de Resolución N° 02

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N°0643-2018/PSO-INDECOPI-LAL Resolución Final N° 0191-2019/PSO-INDECOPI-LAL **Banco infractor** **Banco Falabella Perú S.A.**	Infracción al art.19° del "Código de Protección y Defensa del Consumidor", en tanto que no habría adoptado medidas de seguridad para evitar que se realice una operación por el monto de US$621,95 (S/ 2114,63) la cual fue cargado a la tarjeta de crédito del titular.	Las entidades bancarias deben adoptar medidas necesarias para que las tarjetas no resulten vulnerables por usos indebidos. Además, el Banco no ha acreditado que la titular solicitó la habilitación para realizar operaciones por internet con su tarjeta de crédito y tampoco se encuentra pactado en el contrato de la tarjeta. En consecuencia, se acredita que el Banco no realizó el monitoreo, la alerta de la cuenta y se trataría de una operación inusual en el comportamiento habitual y por ello permitió que se realice la operación por internet indebidamente.	Sancionar al Banco con multa de 2 UIT por infracción al art.19°. Como medida correctiva reparadora que anule, extorne o devuelva el importe de la operación no reconocida. Además, que se anule los intereses, penalidades, comisiones y gastos que se hubieran generado.

Fuente: Elaboración propia

Tabla 3

Tabla de Análisis de Resolución N° 03

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0727-2018/PSO-INDECOPI-LAL **Resolución Final N° 0078-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Falabella Perú S.A.**	Infracción del art.19° del "Código de Protección y Defensa del Consumidor", en tanto que el banco no habría adoptado las medidas de seguridad para evitar que se realice un consumo vía internet por el importe de S/852.38.	Al haberse acreditado que el Banco no había adoptado medidas de seguridad básicas de monitoreo y realización de operaciones, teniendo en cuenta que la operación es poco usual y no acorde con su patrón de consumo, siendo posible un fraude que causa un perjuicio económico.	Sancionar al Banco con multa de 1 UIT por infracción al art. 19° Como medida correctica que devuelva el monto que se cargó indebidamente a la tarjeta del titular y se anule todos lo interés, penalidades, comisiones y/o gastos que se hubieran generado como consecuencia del monto cargado.

Fuente: Elaboración propia

Tabla 4

Tabla de Análisis de Resolución N° 04

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N°0049-2019/PSO-INDECOPI-LAL **Resolución Final N° 0309-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Scotiabank Perú S. A**	El Banco no habría adoptado las medidas de seguridad para evitar que se realicen 2 consumos por internet por un monto de S/ 225.50.	Una vez que es procesada la transacción, se registra en el sistema de monitoreo que permite evaluar si corresponde a un patrón de fraude y evitar que se realice posteriores operaciones fraudulentas. En efecto, cuando la transacción es aprobada, el Banco puede determinar corresponde a patrón de fraude. Por lo tanto, el denunciante nunca había realizado consumos por internet y que se hayan cargado en la tarjeta de crédito dos operaciones en un solo día constituía un indicios de un patrón de consumo no habitual. En consecuencia, el Banco no adoptó medidas de seguridad para evitar que se realicen las dos operaciones por internet.	Sancionar a Scotiabank Perú S.A. con multa de 2 UIT por infracción al artículo 19° del mencionado Código. Ordenar al banco que anule o extorne las 2 operaciones no reconocidas cargadas en la tarjeta de crédito, además que se anule los intereses, comisiones o penalidades que se hayan generado.

Fuente: Elaboración propia

Tabla 5

Tabla de Análisis de Resolución N° 05

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0118-2019/PSO-INDECOPI-LAL **Resolución Final N° 0315-2019 PSO-INDECOPI-LAL** **Banco infractor** **Banco Ripley Perú S. A**	Presunta infracción de artículo 19°, en tanto no habría adoptado las medidas de seguridad de monitoreo y alerta para evitar que se realicen 10 operaciones por internet por el monto de S/1156,07 con cargo a la tarjeta de crédito del titular.	La operación cuestionada no corresponde a su patrón de consumo, y debieron ser advertidas por el Banco mediante su sistema de monitoreo, alertarle mediante algún medio electrónico o móvil de la realización de las operaciones. Asimismo, el Banco adjuntó prints de pantalla de su sistema para demostrar que la tarjeta se encontraba habilitada para realizar compras por internet.	Sancionar a Banco Ripley con 1 UIT por infracción al "Código de Protección y Defensa del Consumidor". Ordenar al banco medida correctiva reparadora que anule o extorne el importe total de las operaciones y que se incluya la anulación o devolución de los intereses que se hubieren generado

Fuente: Elaboración propia

Tabla 6

Tabla de Análisis de Resolución N° 06

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0035-2019/PSO-INDECOPI-LAL **Resolución Final N° 0243-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Interbank S.A.**	No haber adoptado las medidas de seguridad para evitar que se realicen 3 operaciones no reconocidas con cargo a la tarjeta de crédito del titular por la suma de S/6750.00	El denunciado debió generar una alerta luego de la primera operación por internet debido a que se rompía con el comportamiento que tenía el titular de la tarjeta y por lo tanto debió poner en conocimiento al cliente para que pudiera evitar la realización de las demás operaciones. En consecuencia, el Órgano Resolutivo considera que el sistema de monitoreo no funcionó correctamente para que pueda alertar al consumidor sobre las operaciones realizadas.	Sancionar al Banco Interbank con multa de 3 UIT por infracción al art. 19° del "Código de Protección y Defensa del Consumidor". Ordenar como medida correctiva cumplan con extornar o devolver el importe cargado a la tarjeta de crédito y extornar cualquier otro concepto que haya generado.

Fuente: Elaboración propia

Tabla 7

Tabla de Análisis de Resolución N° 07

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 198-2019/ PSO-INDECOPI-LAL **Resolución Final N° 0403/ PSO-INDECOPI-LAL** **Banco infractor** **Banco de la Nación**	No haber adoptado las medidas para evitar que se realice una transferencia interbancaria por un monto de S/1024 con cargo a la tarjeta de débito.	La titular señaló que había ingresado a la página web del Banco y que registró la clave Token, después la página se cerró; por lo tanto, la denunciante fue víctima de la modalidad de fraude electrónica denominado "phishing". En consecuencia, el Banco no había adoptado medidas de seguridad para evitar que se realice la transferencia interbancaria.	Sancionar al Banco de la Nación con multa de 3 UIT por infracción al deber de idoneidad. Ordenar como medida correctiva reparadora que devuelva el monto por la operación no reconocida y que se devuelva los intereses legales.

Fuente: Elaboración propia

Tabla 8

Tabla de Análisis de Resolución N° 08

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 408-2019/PSO-INDECOPI-LAL **Resolución Final N°0518-2019/ PSO-INDECOPI-LAL** **Banco infractor** **Banco BBVA Perú S.A.**	Presunta infracción al deber de idoneidad por no haber adoptado las medidas de seguridad a fin de evitar que se realice 2 operaciones por internet con cargo a la tarjeta de débito por un monto de S/8430.	No se había adoptado las medidas de seguridad al no haber realizado el monitoreo y alerta de la cuenta, además que se trataría de operaciones inusuales en el comportamiento habitual o patrón de consumo de la titular. En los casos que las operaciones de consumo no corresponden al comportamiento habitual se analizará si fueron autorizados por el titular y finalmente si las operaciones no presentaban características de fraude para que se pueda concluir si funcionó correctamente el sistema de monitoreo.	Sancionar a BBVA Perú con 3 UIT por infracción al deber de idoneidad. Ordenar al banco que devuelva el importe total por las 4 operaciones cargadas a la tarjeta de débito.

Fuente: Elaboración propia

Tabla 9

Tabla de Análisis de Resolución N° 09

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 209-2019/ PSO-INDECOPI-LAL **Resolución Final N° 438-2019/ PSO-INDECOPI-LAL** **Banco infractor** **Banco Falabella Perú S.A.**	Presunta infracción al deber idoneidad en tanto que el Banco no habría adoptado medidas de seguridad el consumo por internet por un monto de S/ 1649 con cargo a la tarjeta de crédito.	El denunciante no ha manifestado que su tarjeta de crédito haya sido extraviada, sustraída, robo, hurto o uso no autorizado de la tarjeta que lo hubiera obligado a contactarse con el denunciado, así como tampoco el Banco no ha demostrado que el denunciante ha tenido un comportamiento negligente con su tarjeta; por lo tanto, se acreditó que el denunciado permitió que se realice la operación por internet de lo cual se determina su responsabilidad infringiendo el deber de idoneidad.	Sancionar a Banco Falabella con 3 UIT por infracción al art. 19° del Código de Protección y Defensa del Consumidor. Ordenar como medida correctiva reparadora que anule, extorne o devuelva el importe correspondiente a la operación cargada a la tarjeta de crédito y que se anule los intereses, comisiones penalidades y gastos que se hubieran generado.

Fuente: Elaboración propia

Tabla 10

Tabla de Análisis de Resolución N° 10

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0185-2019/ PSO-INDECOPI-LAL **Resolución Final N°0353-2019/ PSO-INDECOPI-LAL** **Banco infractor** **Banco Scotiabank Perú**	Infracción al deber de idoneidad por no haber adoptado las medidas de seguridad necesarias para evitar que se realice un consumo por un importe de US$ 548.34.	Un primer asunto que se debe de considerar es si el titular autorizó expresamente que la tarjeta pueda utilizarse para transacciones por internet. Asimismo, el banco no cumplió con brindar las medidas de seguridad como por ejemplo de alertar sobre el consumo al ser una operación inusual.	Sancionar a Scotiabank con 3 UIT por infracción al deber de idoneidad. Ordenar al banco como medida correctiva que anule, extorne o devuelva el monto que se cargó a la cuenta, incluyendo la anulación o devolución de los intereses, comisiones, gastos que se hubiera generado.

Fuente: Elaboración propia

Tabla 11

Tabla de Análisis de Resolución N° 11

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 186-2019/PSO-INDECOPI-LAL **Resolución Final N° 0368 2019/PSO-INDECOPI-LAL-** **Banco infractor** **Banco Ripley Perú S. A**	Presunta infracción al deber de idoneidad, debido a que el Banco no había adoptado medidas de seguridad de monitoreo y alerta para evitar que se realicen 7 operaciones de consumo por internet por un monto S/ 1057.31 con cargo a la tarjeta de crédito.	Se debe analizar si en marco de la relación de consumo si primero se solicitó o autorizó expresamente que la tarjeta pueda utilizarse para operaciones por internet. En consecuencia, el Banco no adoptó las medidas de seguridad de monitoreo y alerta para evitar las operaciones por internet.	Sancionar al Banco Ripley con multa de 3 UIT por infracción al deber de idoneidad. Ordenar al banco como medida correctiva reparadora que se anule o devuelva el monto por las operaciones y que anule o devuelva los intereses, comisiones y gastos que se hayan incurrido.

Fuente: Elaboración propia

Tabla 12

Tabla de Análisis de Resolución N° 12

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N°0703-2018/PSO-INDECOPI-LAL **Resolución Final N° 0187-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Scotiabank Perú S.A**	El Banco no habría adoptado medidas de seguridad de monitoreo y alerta para evitar que se realicen 3 operaciones con cargo a la tarjeta de crédito del titular por un monto de $508.60.	Se trataría de operaciones inusuales en su comportamiento habitual de consumo, además la titular de la tarjeta de crédito no ha sufrido algún extravío, robo, hurto o uso no autorizado para que pueda conectarse con la denunciada y poder bloquearla, por lo tanto, no resulta aplicable la exoneración de responsabilidad del Banco. Por lo tanto, al no existir medio probatorio que acredite que la operación fue realizada válidamente y al no haberse acreditado la imprudencia del consumidor, se determina que el Banco no adoptó medidas de seguridad para evitar que se realicen los 3 consumos vía internet.	Sancionar a Scotiabank Perú S.A. con multa de 2 UIT por infracción al artículo 19° del código en mención. Ordenar como medida correctiva reparadora la anulación y/o devolución de los tres consumos y la anulación del pago de intereses, penalidades, comisiones, pagos derivados de las operaciones.

Fuente: Elaboración propia

Tabla 13

Tabla de Análisis de Resolución N° 13

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0694-2018/PSO-INDECOPI-LAL **Resolución Final N° 0129-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Scotiabank Peru S.A.**	No habría adoptado las medidas de seguridad para evitar que se realicen 2 operaciones con cargo a la tarjeta de crédito de la titular por un monto de S/1006.90	El Banco no ha realizado el monitoreo, alerta de la cuenta y se trataría de operaciones inusuales a su comportamiento habitual. Asimismo, del Contrato de Tarjeta de Crédito no se desprende que hubiera contado con el beneficio de poder realizar operaciones por internet, servicio que debe ser autorizado previamente por el titular de la tarjeta.	Sancionar a Scotiabank Perú S.A. con amonestación por infracción al artículo 19° del "Código de Protección y Defensa del Consumidor". Además, se ordena que se extorne o devuelva los intereses, penalidades, comisiones y gastos como consecuencia de las operaciones no reconocidas.

Fuente: Elaboración propia

Tabla 14

Tabla de Análisis de Resolución N° 14

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0685-2018//PSO-INDECOPI-LAL **Resolución final N°0141-2019/PSO-INDECOPI-LAL** **Banco infractor** **Banco Falabella Perú S.A.**	Presunta infracción al art.19° del "Código de Protección y Defensa del Consumidor", por no haber adoptado las medidas de seguridad para evitar que se realicen 2 operaciones con cargo a la tarjeta de crédito por un monto de $430,01.	El Banco no demostró que la titular autorizó que se realizaran las operaciones vía internet con cargo a la tarjeta de crédito, tampoco adjuntó el contrato de tarjeta de crédito donde suscribe que la titular autoriza el uso para hacer operaciones por internet o si se trataba de un beneficio inherente a la tarjeta.	Sancionar con 2 UIT por infracción al art.19° del Código en mención. Como medida correctiva que anule, extorne y devuelva el importe cargado a la tarjeta de crédito.

Fuente: Elaboración propia

Tabla 15

Tabla de Análisis de Resolución N° 15

N° Exp / N° Resolución	Imputación de cargos	Fundamentos relevantes de la ORPS	Decisión
Exp N° 0666-2017/PSO-INDECOPI-LAL **Resolución Final N°0330-2018/PSO-INDECOPI-LAL** **Banco infractor** **Banco Ripley Perú S.A**	El banco no adoptó medidas de seguridad necesarias para evitar la realización del consumo por internet que fue cargada a la tarjeta de crédito del titular por un monto de S/329.90, el cual no reconoce, hecho que infringe el artículo 19° del Código (deber de idoneidad).	No obra medio probatorio donde se aprecie que la operación fue efectuada válidamente con el empleo de clave secreta, códigos de seguridad, CVV (código de verificación), el número de la tarjeta, su fecha de caducidad o claves adicionales, por lo tanto, se ha infringido el artículo 19° debido a que no cumplió con adoptar medidas de seguridad para evitar la realización del consumo por internet.	Sancionar a Banco Ripley con multa de 2 UIT por haber incurrido en infracción al artículo 19°. Además, debe devolver a la tarjeta de crédito el importe que fue cargado a la cuenta.

Fuente: Elaboración propia

Análisis: De las 15 resoluciones desarrolladas, se ha podido determinar que las entidades bancarias de la región La Libertad no cumplen con el deber de idoneidad en las operaciones que se efectuaron por el fraude electrónico con tarjetas de crédito y débito; porque no han adoptado las siguientes medidas de seguridad:

- Que el usuario haya solicitado la habilitación para realizar operaciones por internet con su tarjeta de crédito o débito, ya sea después o que se haya pactado en el contrato de la tarjeta.

- Que el banco haya validado en su sistema de operaciones datos relevantes tales como la hora de la operación, constancia de ingreso de la tarjeta, ingreso de código de seguridad, ingreso de clave secreta, código de autorización y código de verificación (CVV) los cuales puedan acreditar la validez de las operaciones.

- Que el Banco deben tener un sistema de monitoreo que permite evaluar si corresponde a un patrón de fraude y evitar que se realicen las operaciones, considerando que la operación es inusual en el comportamiento habitual y no acorde con el patrón de consumo; si es que algún Banco tiene sistema de monitoreo no lo cumple adecuadamente.

- Si se trata de una operación que no corresponde al patrón de consumo, el Banco debe alertarle al usuario mediante algún correo electrónico, llamada o mensaje de texto de la realización de las operaciones y realizar el bloqueo temporal de la tarjeta.

Por lo tanto, al no haberse cumplido con las medidas de seguridad básicas y necesarias que están estipuladas en el "Reglamento de tarjetas de crédito y débito"; tales como el Art. 16° en el inciso 4) que establece que cuando se realicen operaciones con las tarjetas, el Banco debe habilitar un servicio donde se pueda notificar al usuario de las operaciones realizadas, inmediatamente después que sea registrada la operación.

Asimismo, en el artículo 17° señala que el Banco debe tener medidas respecto al monitoreo y realización de operaciones para que pueda identificar principios de fraude, por último en el artículo 22° establece que las entidades bancarias deben dar seguimiento de operaciones que se pueden estar cometiendo fraude e implementar mecanismos para la comunicación inmediata al usuario sobre las operaciones de fraude y tomar acciones para proceder al bloqueo temporal o cancelación definitiva de la tarjeta.

En ese sentido, al no cumplir con dichas medidas se está demostrando que las entidades bancarias de la región La Libertad han infringido el deber de idoneidad estipulado en el Art.

19° del "Código de Protección y Defensa del Consumidor", y eso ha conllevado que se les sancionen a las entidades bancarias con 1 UIT a 3 UIT dependiendo el importe que se les ha cargado a la cuenta de la tarjeta y el daño económico que se la ha causado al usuario; asimismo también se les ha dictado como medida correctiva que se extorne o se devuelva el importe que se les cobró por la operación, además que se les devuelva, extorne o anulen los intereses, penalidades, comisiones y gastos que se han generado como consecuencia de las operaciones no reconocidas.

3.2. RESULTADO RESPECTO AL OBJETIVO ESPECÍFICO N° 02: Analizar dentro de la legislación internacional los aspectos normativos sobre el deber de idoneidad en los servicios financieros con tarjetas de crédito y débito, con la finalidad de realizar una comparación con la legislación peruana. Con respecto a dicho resultado se ha utilizado el análisis de legislación internacional de Chile, Ecuador y Colombia para determinar la regulación sobre el deber de idoneidad en los servicios financieros, con la finalidad de realizar una comparación con la legislación peruana; para ello se ha utilizado el instrumento el análisis de la legislación internacional mediante cuadro comparativo y empleando el criterio de selección.

Tabla 16

Cuadro comparativo de legislación internacional Chilena

PAIS	TIPOLOGÍA	REDACCIÓN DE ARTICULO
	Ley N°19.496 "Ley de protección de los derechos de los consumidores"	Art. 28° inciso c) establece que se comete infracción el que, a sabiendas o debiendo saberlo y a través de cualquier mensaje publicitario induce a error o engaño respecto de: d) la idoneidad del bien o servicio para los fines que se pretende satisfacer y que se haya sido atribuida en forma explícita por el anunciante.
	Ley N°20.009 "Régimen de	Artículo 6° "Los emisores, operadores, comercios y otros establecimientos afiliados a un sistema de

Chile	limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude"	tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley conforme a la legislación y normativa que les resulte aplicable, y resguardando la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley Nº 19.496. En el caso de los emisores u operadores, según corresponda, dichas medidas de seguridad deberán considerar, al menos, lo siguiente: a) Contar con sistemas de monitoreo que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario. b) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo. c) Identificar patrones de potenciales fraudes, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones". d) Establecer límites y controles en los diversos canales de atención que permitan mitigar las pérdidas por fraude. Los referidos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar".

Fuente: Elaboración propia

Tabla 17

Cuadro comparativo de legislación internacional Ecuatoriana

PAÍS	TIPOLOGÍA	REDACCIÓN DE ARTÍCULO
Ecuador	Ley N° 2000-21 "Ley Orgánica de defensoría del consumidor"	Artículo 7° inciso 3 señala que el que comete infracción a esta ley el proveedor que a través de cualquier tipo de mensaje induce al error o engaño en especial cuando se refiere a: 3. Las características básicas del bien o servicio ofrecidos, tales como componentes, ingredientes, dimensión, cantidad, calidad, utilidad, durabilidad, garantías, contraindicaciones, eficiencia, idoneidad del bien o servicio para los fines que se pretende satisfacer y otras.
Ecuador	Resolución No.SB-2020-0540	Art. 17° en su inciso m) señala que es un derecho de los consumidores a recibir productos y servicios financieros con calidad y seguridad. Asimismo, en el inciso p) se establece exigir que se debe garantizar la seguridad de los depósitos, evitando fraudes informáticos; porque si no las entidades controladas asumirán la responsabilidad pecuniaria, esto comprende i) que las entidades cumplan con las normas de riesgo operativo para proteger los depósitos y medios de pago de los consumidores financieros.

Fuente: Elaboración propia

Tabla 18

Cuadro comparativo de legislación internacional Colombiana

PAÍS	TIPOLOGIA	REDACCIÓN DE ARTÍCULO
Colombia	Ley N° 1480 de 2011 "Estatuto del Consumidor"	El Art. 5° inciso 6 prescribe que la idoneidad o eficiencia viene a ser la aptitud del producto para satisfacer la necesidad para los cuales ha sido producido o comercializado. Así también, en el Art. 6° establece que todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca o ponga en el mercado, así como la calidad ofrecida. En ningún caso podrán ser inferiores o contravenir lo previsto en reglamentos técnicos y medidas sanitarias o fitosanitarias. Art. 51° en su primer párrafo señala que, cuando las ventas se realicen mediante mecanismos de comercio electrónico, y se haya utilizado para realizar el pago una tarjeta de crédito, débito, los participantes del proceso de pago deberán reversar los pagos que solicite el consumidor cuando sea objeto de fraude.
	Ley 1328 de 2009, "Por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones".	Art. 5° sobre "los derechos de los consumidores financieros en el inciso a) señala que, en desarrollo del principio de debida diligencia, los consumidores financieros tienen el derecho de recibir de parte de las entidades vigiladas productos y servicios con estándares de seguridad y calidad, de acuerdo con las condiciones ofrecidas y las obligaciones asumidas por las entidades vigiladas". Art.7° Obligaciones especiales de las entidades vigiladas en su inciso b) señala que debe entregar el producto o prestar el servicio debidamente, es decir, en las condiciones informadas, ofrecidas o citadas con el consumidor financiero, y emplear adecuados estándares de seguridad y calidad en el suministro de los mismos.

Fuente: Elaboración propia

Análisis: En la "Ley de Protección de los Derechos de los Consumidores" de Chile, en su artículo 28° inciso b) no hace una definición que permite determinar lo que significa

idoneidad de un producto o un servicio, sino que solamente hace referencia bajo la figura de que comete infracción el que realiza una publicidad engañosa induciendo a error con respecto a la idoneidad del servicio para los fines que se ofrece.

En cambio en la legislación peruana en el "Código de Protección y Defensa del Consumidor" regula en su Art. 18° lo que se entiende por idoneidad, que es "la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a la publicidad e información, condiciones, características y naturaleza del producto o servicio que se le ha ofrecido"; y, en el Art. 19° "la obligación de los proveedores que deben tener con respecto a la idoneidad y calidad de los productos y servicios ofrecidos". Por lo tanto, entre la legislación chilena y la legislación peruana en lo que respecta a idoneidad, Perú establece con exactitud que se refiere con idoneidad y la obligación del proveedor para que no vulnere este deber.

Por otro lado, en la legislación chilena con respecto a la responsabilidad para los usuarios de tarjetas de pago y transacciones electrónicas en caso de fraude en el artículo 6° señala las entidades que presten servicios con tarjetas de pago deben adoptar medidas de seguridad para prevenir de hecho ilícitos como son contar con un sistema de monitoreo que detecten las operaciones que no corresponden al comportamiento habitual del usuario, implementen procedimientos internos que alerten, que se identifique patrones de fraudes y que se establezca límites y controles en los diversos canales de atención que permitan mitigar las perdidas por fraude, basándose en consideraciones de riesgo; mientras que en Perú cuenta con un reglamento de tarjetas de crédito y débito en la cual se señalan las medidas de seguridad aplicables a dichas tarjetas de pago, como por ejemplo el Art. 17° señala que las empresas deben adoptar como mínimo las siguientes medidas de seguridad cuando se estén realizando operaciones: contar con un sistema de monitoreo de operaciones que detecten

operaciones que no corresponden al comportamiento habitual del consumo de usuario, implementar procedimientos complementarios para gestionar alertar, identificar patrones de fraude, establecer límites y controles en los diversos canales de atención que permitan mitigar pérdidas de fraude, además del artículo 22° que señala que los Bancos deben implementar procedimientos para el seguimiento de operaciones que corresponden a patrones de fraude lo que debe incluir mecanismos para la comunicación inmediata y deben proceder con el bloqueo temporal o definitivo de la tarjeta.

En efecto, tanto Perú como Chile señalan las mismas medidas de seguridad que deben implementar con respecto a prevenir hechos ilícitos cuando se estén realizando las operaciones, pero existe una diferencia con respecto a que la legislación peruana señala las medidas que deben de tomar las entidades bancarias cuando las operaciones corresponden patrones de fraude mientras que en Chile solo señala tres medidas de seguridad que deben de tomar las entidades bancarias para evitar hechos ilícitos.

Con respecto a la legislación ecuatoriana en su "Ley Orgánica de Defensoría del Consumidor" en su artículo 7° inciso 3 señala que comete infracción cuando a través de un mensaje induce al error cuando se refiere a idoneidad del bien o servicio para los fines que se pretende satisfacer, esto es que tampoco se hace una definición exacta del deber de idoneidad al igual que Chile, a diferencia de Perú como ya se había señalado líneas arriba en el "Código de Protección y Defensa del Consumidor" que si define que se entiende por idoneidad. En cuanto al derecho de los consumidores financieros en la Resolución No. SB-2020-0540 señala en el artículo 17° en el inciso m) que los usuarios deben recibir productos y servicios con patrones de calidad y seguridad, en el inciso p) establece que las entidades bancarias deben garantizar las operaciones de los consumidores, evitando fraudes, además señala que si los bancos entregan dinero de los usuarios a través de acciones fraudulentas,

serán responsables económicamente, esto es que las entidades deben tener sistemas de riesgo para proteger las tarjetas de pagos de los usuarios; en cambio en la legislación peruana en el artículo 23° hace mención que ante el rechazo de una operación por parte del usuario cuando fue realizada incorrectamente, las empresas serán responsables de demostrar que las operaciones fueron registradas correctamente y que el usuario no es responsable cuando la empresa fue notificada de extravío, robo, hurto o uso autorizado de la tarjeta, cuando no comunican al usuario por las operaciones que se están realizando, entro otras supuestos en las cuales se exime de responsabilidad al usuario; con respecto a esta última figura de la responsabilidad por operaciones no reconocidas Ecuador responsabiliza a la entidades por no haber garantizado calidad y seguridad en las operaciones para evitar que se realice transacciones fraudulentas y no establece supuestos en las que puede eximirlos de responsabilidad, a diferencia de Perú que regula en que supuestos la entidad bancaria es responsable por las operaciones no reconocidas y que para eximirse de responsabilidad debe de demostrar que las operaciones fueron correctamente realizadas.

Por último, el "Estatuto del Consumidor de Colombia" en el artículo 5° inciso 6 hace referencia a la idoneidad como la aptitud del productor para satisfacer la necesidad para los cuales ha sido comercializado, además el artículo 6° señala como obligación del proveedor que debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca; al igual que Perú, la legislación colombiana a definido que se entiende por idoneidad y cuál es la obligación de los proveedores con respecto al cumplimiento del deber de idoneidad, cabe recalcar que la legislación peruana hace una definición más amplia de dicha figura.

Así mismo, en el mismo estatuto en su artículo 51° establece que cuando se efectúan compras por internet usando una tarjeta de crédito o débito y que ha sido realizada como una operación fraudulenta, será obligado el proveedor, como ya se ha señalado líneas arriba en

Perú si establece los supuestos cuando la entidad bancaria es responsable por las operaciones que el usuario rechaza y que para eximirse de responsabilidad debe de probarlo.

Con respecto a los derechos de los consumidores financieros la "Ley 1328 de 2009" de Colombia señala en su artículo 5° inciso a) que los usuarios tienen derecho a recibir productos y servicios con estándares de seguridad y calidad, de acuerdo con las condiciones ofrecidas y las obligaciones que deben de asumir las entidades, asimismo el artículo 7° en su inciso b) señala que las entidades debe otorgar producto o servicio con las condiciones informadas y emplear estándares de seguridad y calidad; se diferencia de Perú en el sentido de que en el reglamento de tarjetas de crédito y débito se señalan cuáles son las medidas de seguridad mínimas que las entidades bancarias deben de cumplir para evitar que se realicen operaciones con patrones de fraude.

En consecuencia, del análisis de las comparaciones realizadas de las legislaciones de los países de Chile, Ecuador y Colombia con la legislación Peruana se ha podido determinar que la legislación peruana a diferencia de los países analizados tiene una legislación que define exactamente en el "Código de Protección y Defensa del Consumidor" que se entiende por idoneidad y cuáles son las obligaciones de los proveedores para cumplir el deber de idoneidad.

Asimismo con respecto a las medidas de seguridad que deben de tener las entidades financieras a diferencia de Chile, Ecuador y Colombia que no establecen con extensión o a profundidad sobre las medidas de seguridad que se debe de implementar como cumplimiento del estándar de calidad y seguridad que señalan, la legislación peruana cuenta con un "Reglamento de Tarjetas de Crédito y Débito" en las cuales señala las medidas de seguridad mínimas que deben cumplir para que las operaciones sean realizadas correctamente, para que se detecte patrones de fraude y la alerta que debe enviar al usuario por las operaciones,

entonces no existe un problema en la legislación con el propósito de que las entidades bancarias vulneren el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito; sino que existe una falta de compromiso y responsabilidad por parte de los Bancos de implementar un sistema de monitoreo que verifique que la operación no presente patrones de fraude, además que no se cumple con alertar al usuario mediante llamada, correo electrónico o mensaje de texto respecto de la operación que se está realizando, asimismo que no se toma en cuenta la habitualidad de consumo de los usuarios para evitar que se realice las operaciones fraudulentas con tarjetas de crédito y débito.

3.3. RESULTADO RESPECTO AL OBJETIVO ESPECÍFICO N° 03: Determinar la afectación que causan las entidades bancarias de la región La Libertad a los usuarios por el fraude electrónico con tarjetas de crédito y débito.

Para este resultado se aplicó la técnica de análisis de encuestas y el instrumento de cuestionario de encuestas a los usuarios de las entidades bancarias de la región La Libertad, habiéndose encuestado a 40 usuarios quienes fueron escogidos aleatoriamente, realizándoles 10 preguntas de selección múltiple que dan respuesta al objetivo. A continuación, se desarrollará el análisis de las encuestas:

Cuadro 1

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad respecto de si cuentan con tarjeta de crédito y/o débito

RESPUESTAS	USUARIOS	
	N°	%
SÓLO CRÉDITO	23	57,50%
SÓLO DÉBITO	4	10,00%
AMBAS	13	32,50%
NINGUNA	0	0,00%
TOTAL	**40**	**100%**

Fuente: Elaboración propia

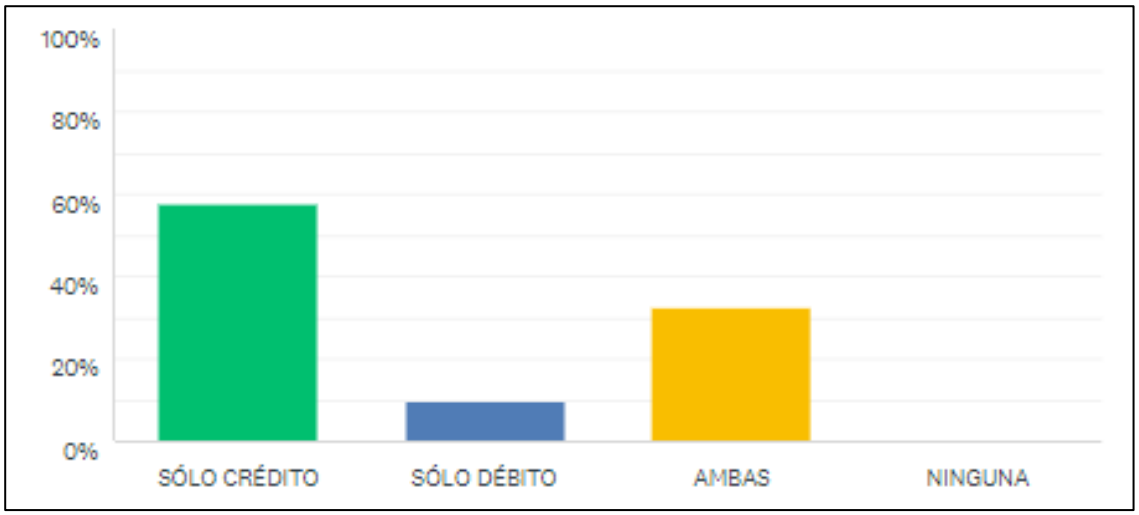

Figura 1 **Datos de los usuarios de las entidades bancarias de la región La Libertad si cuentan con tarjeta de crédito y/o débito**

Con respecto al cuadro 1 y a la figura 1 se observa que del 100% de los usuarios de las entidades bancarias de la región La Libertad el 57,50% de los usuarios tienen solo tarjeta de crédito, 10,00% sólo tienen tarjeta de crédito, 32,50% ambas tarjetas y 0,00% ninguna de las tarjetas.

Cuadro 2

Distribución de los datos de que banco de la región La Libertad adquirieron los usuarios la tarjeta de crédito o débito

RESPUESTAS	USUARIOS	
	N°	%
SCOTIABANK S.A.	10	25,00%
BCP	10	25,00%
INTERBANK S.A.	8	20,00%
BBVA	9	22,50%
OTROS	3	7,50%
TOTAL	**40**	**100%**

Fuente: Elaboración propia

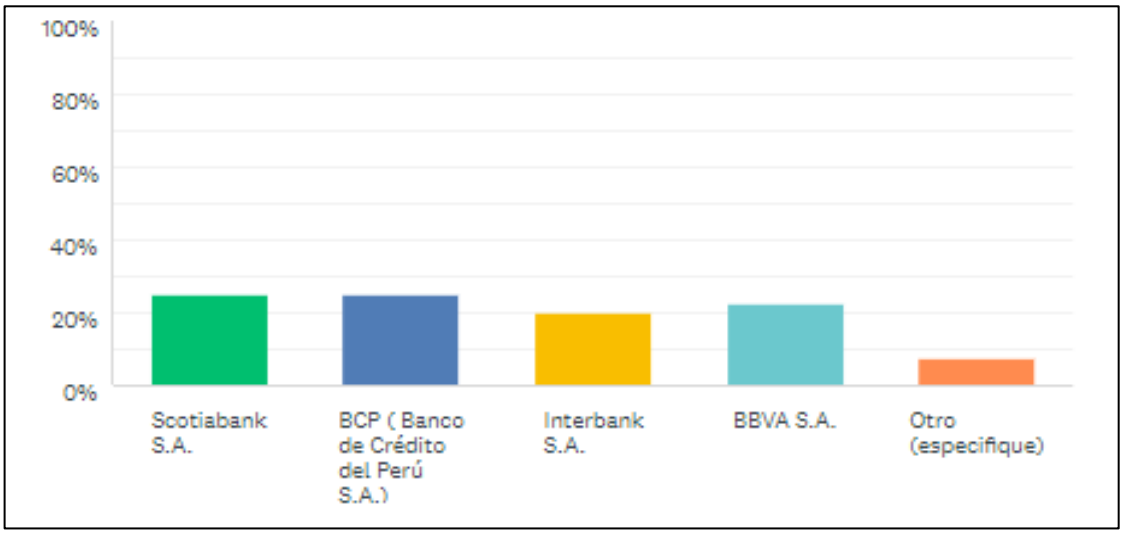

Figura 2: **Distribución de datos que banco de la región La Libertad adquirieron los usuarios la tarjeta de crédito o débito**

De acuerdo al cuadro 2 y la figura 2 se observa que del 100% de los usuarios de las entidades bancarias de la región La Libertad, el 25,00% han adquirido del banco Scotiabank S.A., 25,00% han adquirido del Banco de Crédito del Perú S.A., 20,00% han adquirido del banco Interbank S.A., 22,50% han adquirido del banco BBVA S.A. y el 7,50% han adquirido de otros Bancos.

Cuadro 3

Distribución de los datos si al momento de adquirir la tarjeta de crédito y/o débito los usuarios de las entidades bancarias de la región La Libertad, le informaron sobre la habilitación de compras por internet

RESPUESTAS	USUARIOS	
	N°	%
SI	15	37,50%
NO	25	62,50%
TOTAL	39	100%

Fuente: Elaboración propia

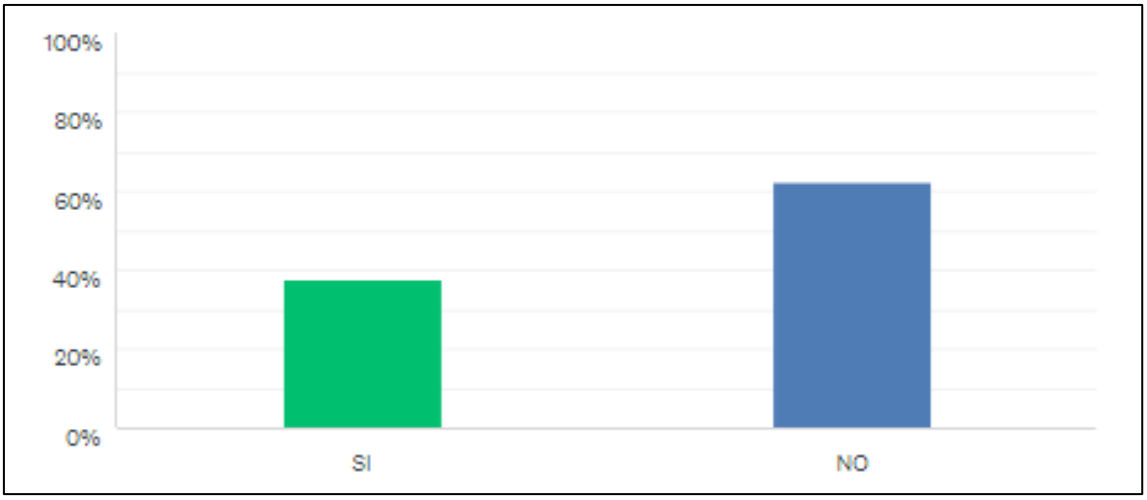

Figura 3: **Distribución de los datos si al momento de adquirir la tarjeta de crédito y/o débito los usuarios de las entidades bancarias de la región La Libertad, le informaron sobre la habilitación de compras por interne**

De acuerdo al cuadro 3 y a la figura 3 se observa que de 100% de usuarios, el 37,50% señala que en el banco donde adquirieron su tarjeta de crédito y/o débito le informaron sobre la habilitación del servicio para compras por internet con su tarjeta, mientras el 62,50% señalaron que el banco no le informó sobre la habilitación para compras por internet con su tarjeta.

Cuadro 4

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que realizan compras por internet con su tarjeta de crédito y/o débito

RESPUESTAS	USUARIOS	
	N°	%
SI	34	85,00%
NO	6	15,00%
TOTAL	40	100%

Fuente: Elaboración propia

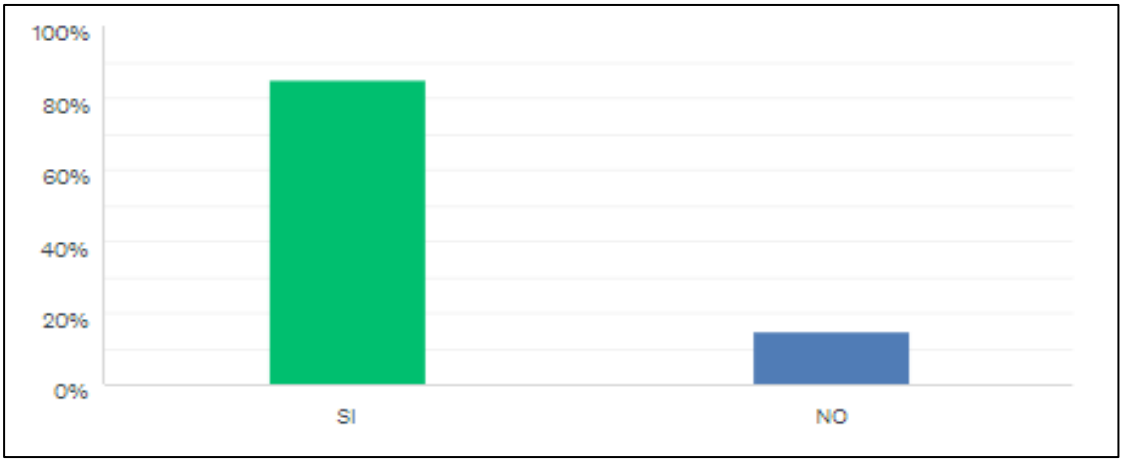

Figura 4: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que realizan compras por internet con su tarjeta de crédito y/o débito**

Con respecto al cuadro 4 y a la figura 4 se observa que del 100% de usuarios de las entidades bancarias de la región La Libertad, el 85,00% realiza compras por internet con su tarjeta de crédito y/o débito, y el 15,00% de los usuarios no realizan compras por internet con su tarjeta de crédito y/o débito.

Cuadro 5

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que han sido víctimas de fraude electrónico con su tarjeta de crédito y/o débito

RESPUESTAS	USUARIOS	
	N°	%
SI	32	80,00%
NO	8	20,00%
TOTAL	**40**	**100%**

Fuente: Elaboración propia

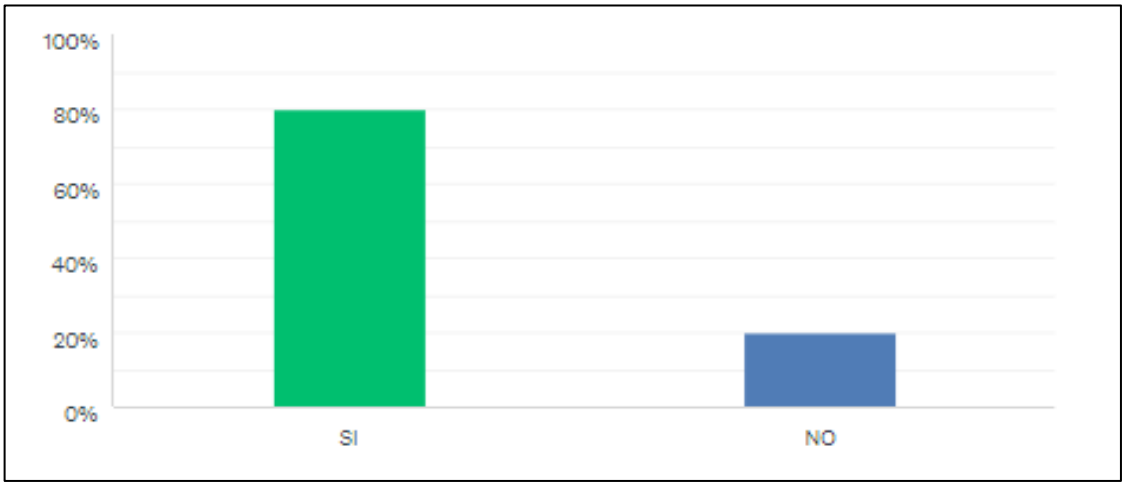

Figura 5 **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que han sido víctimas de fraude electrónico con su tarjeta de crédito y/o débito**

Con respecto al cuadro 5 y a la figura 5 se observa que del 100% de usuarios de las entidades bancarias de la región La Libertad, el 80,00% realiza compras por internet con su tarjeta de crédito y/o débito, y el 20,00% de los usuarios no realizan compras por internet con su tarjeta de crédito y/o débito**.**

Cuadro 6

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que señalan si el banco tomó algunas medidas de seguridad para evitar que se cometa el fraude electrónico

RESPUESTAS	USUARIOS	
	N°	%
ME MANDARON UN MENSAJE DE TEXTO A MI CELULAR	6	13,16%
ME MANDARON UN CORREO ELECTRÓNICO	7	18,42%
NO TOMARON NINGUNA MEDIDA DE SEGURIDAD	21	50,00%
NO FUI VICTIMA DE FRAUDE	7	18,42%
TOTAL	**40**	**100%**

Fuente: Elaboración propia

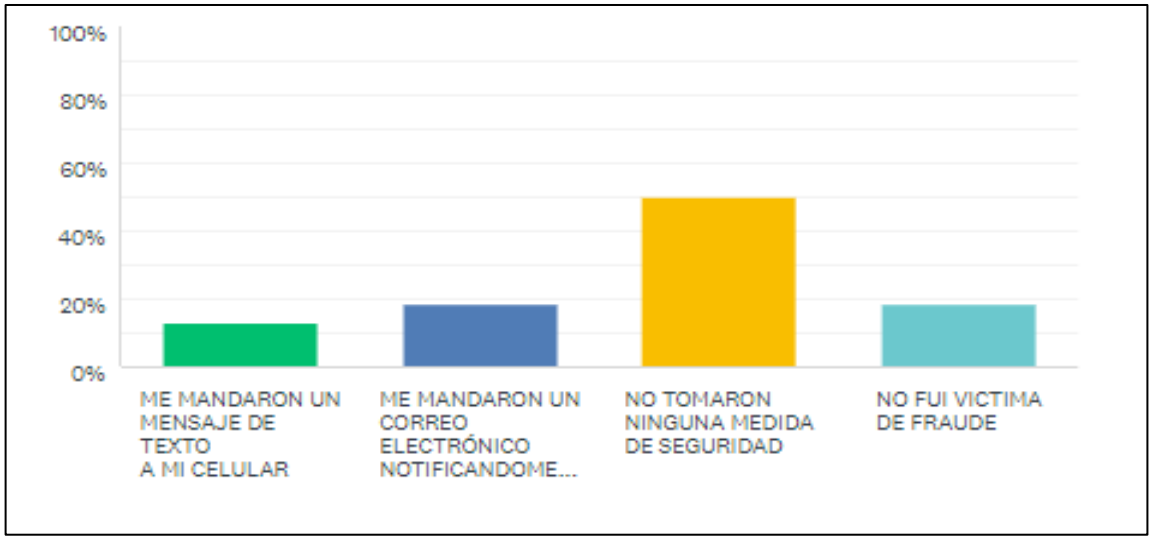

Figura 6: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que señalan si el banco tomó algunas medidas de seguridad para evitar que se cometa el fraude electrónico**

Con respecto al cuadro 6 y a la figura 6 se observa que del 100% de usuarios de las entidades bancarias de la región La Libertad, el 13,16% le enviaron un mensaje de texto a su celular como medida de seguridad, alertándolo de la operación que se estaba realizando, el 18,42% señalan que le enviaron un correo electrónico notificando de la operación, el 50,00% señalan que no tomaron ninguna medida se seguridad y el 18,42% señala que no fue víctima de fraude electrónico.

Cuadro 7

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que reclamaron ante el banco por haberse efectuado operaciones con cargo a su tarjeta por el fraude electrónico

RESPUESTAS	USUARIOS	
	N°	%
SI	30	74,36%
NO	3	7,69%
NO FUI VICTIMA DE FRAUDE	7	17,95
TOTAL	40	100%

Fuente: Elaboración propia

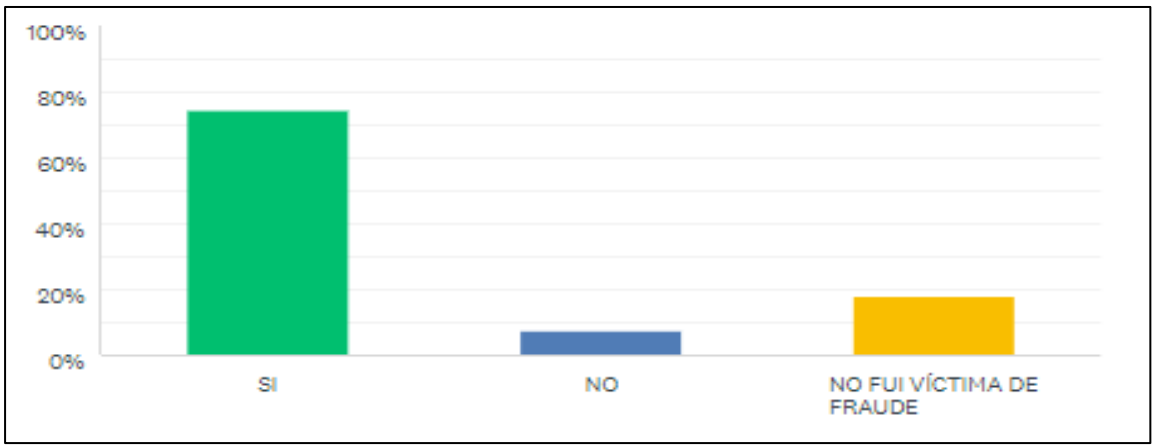

Figura 7: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que reclamaron ante el banco por haberse efectuado operaciones con cargo a su tarjeta por el fraude electrónico**

Con respecto al cuadro 7 y a la figura 7 se observa que de 100% de los usuarios de las entidades bancarias de la región La Libertad, el 74,36% reclamaron ante el banco por haberse efectuado operaciones con cargo a su tarjeta por el fraude electrónico, el 7,69% que no reclamaron ante el banco y 17,95% de los encuestados no fueron víctima de fraude electrónico.

Cuadro 8

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que fueron víctimas del fraude electrónico, de cuanto fue el importe que se les cargo a su tarjeta de crédito o débito

RESPUESTAS	USUARIOS	
	N°	%
S/5-S/50	2	5,13%
S/51-S/500	8	20,51%
S/501-S/1001	12	30,77%
S/1001-S/5000	7	17,95%
Más de S/5001	4	7,69%
NO FUI VICTIMA DE FRAUDE	7	17,95%
TOTAL	40	100%

Fuente: Elaboración propia

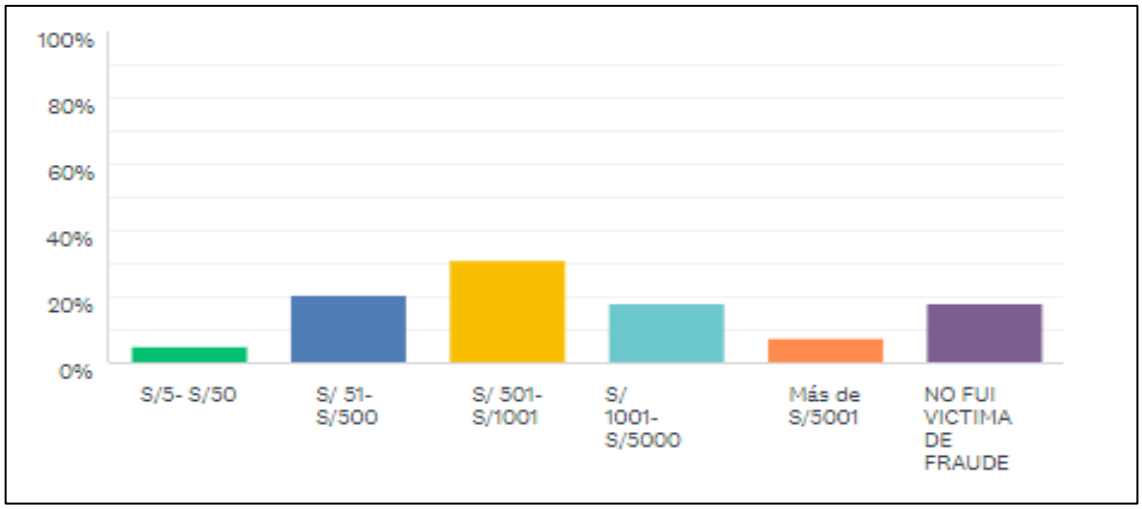

Figura 8: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que han sido víctimas de fraude electrónico con su tarjeta de crédito y/o débito**

Con respecto al cuadro 8 y a la figura 8 se observa que de 100% de los encuestados, el 5,13% se les cargó un importe de S/ 5 a S/ 50 por las operaciones que se habían efectuado con su tarjeta de crédito o débito a causa del fraude electrónico; el 20,51% que se les cargó un importe de S/51 a S/500 por haberse efectuado las operaciones; el 30,77% se les cargó un importe de S/501 a S/1001; el 17,95% que corresponde les cargó un importe de S/1001 a S/5000; 7,69% se les cargó un importe a su cuenta por más de S/5001 y 17,95% usuarios no fueron víctima de fraude.

Cuadro 9

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que consideran que se les ha causado un perjuicio económico al efectuarse las operaciones a causa del fraude electrónico con su tarjeta de crédito o débito

RESPUESTAS	USUARIOS	
	N°	%
SI	40	100,00%
NO	0	0,00%
NO FUI VICTIMA DE FRAUDE ELECTRÓNICO	0	0,00%
TOTAL	40	100%

Fuente: Elaboración propia

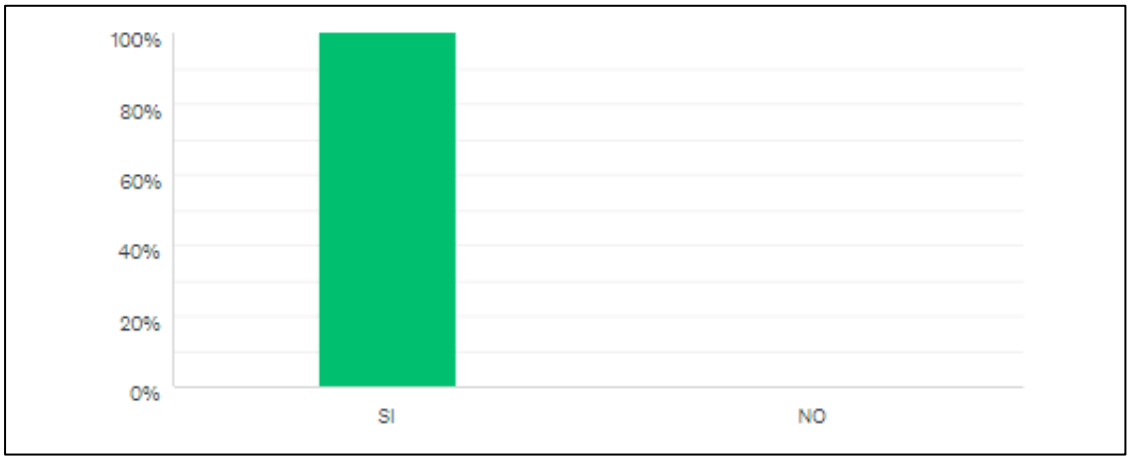

Figura 9: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que consideran que se les ha causado un perjuicio económico al efectuarse las operaciones a causa del fraude electrónico con su tarjeta de crédito o débito**

Con respecto al cuadro 9 y a la figura 9 se observa que del 100% de usuarios de las entidades bancarias de la región La Libertad, 40 usuarios respondieron que, si les estuviese causando un perjuicio económico al efectuarse las operaciones a causa del fraude electrónico.

Cuadro 10

Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que consideran que se estaría vulnerando el deber de idoneidad al momento de que el banco no cumple con las medidas necesarias para evitar el fraude electrónico con tarjetas de crédito o débito

RESPUESTAS	USUARIOS	
	N°	%
SI	40	100,00%
NO	0	0,00%
NO RESPONDIERON	0	0,00%
TOTAL	40	100%

Fuente: Elaboración propia

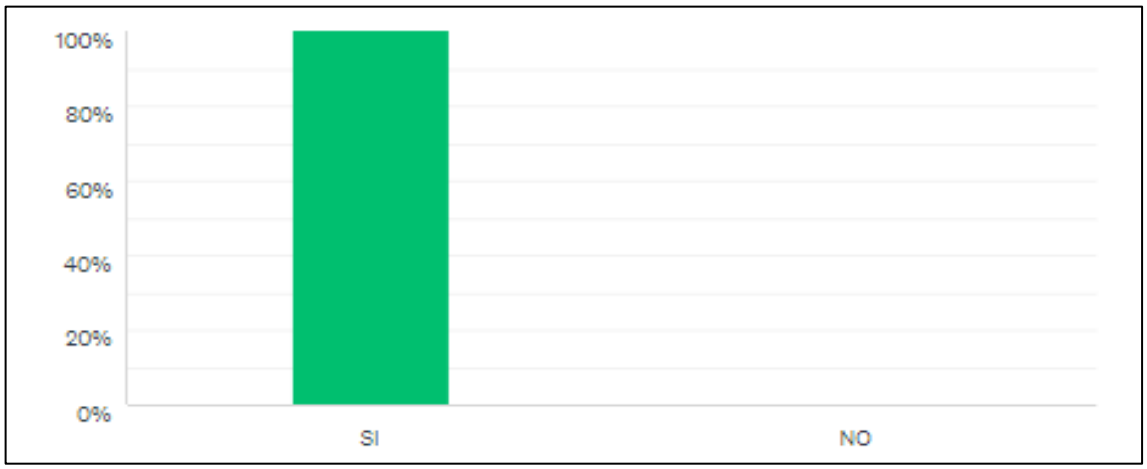

Figura 10: **Distribución de los datos de los usuarios de las entidades bancarias de la región La Libertad que consideran que se estaría vulnerando el deber de idoneidad al momento de que el banco no cumple con las medidas necesarias para evitar el fraude electrónico con tarjetas de crédito o débito**

Con respecto al cuadro 10 y a la figura 10 se observa que del 100% de usuarios de las entidades bancarias de la región La Libertad, 40 usuarios que corresponde al 100,00% respondieron que si estuviese vulnerando el deber de idoneidad al momento de que el banco no cumple con las medidas necesarias para evitar el fraude electrónico con tarjetas de crédito o débito.

Análisis de encuestas: Se ha podido determinar de las encuestas elaboradas a los usuarios de las entidades bancarias de la región La Libertad, que la mayoría de los usuarios cuentan con más tarjetas de crédito que de débito, que la mayoría adquirieron en las entidades bancarias de Scotiabank, Banco de Crédito del Perú, Interbank y BBVA. Sin embargo, en el

instante en el que adquirieron sus tarjetas de crédito o débito, el banco no les informó sobre la habilitación de compras por internet que podría ser pactado en el contrato o en cualquier momento poder habilitar el servicio de realizar operaciones por internet; por lo tanto, sin saber esta información relevante de que se podría habilitar o deshabilitar este servicio, la mayoría de los usuarios realiza operaciones con su tarjeta de crédito o débito mediante internet.

Pese a que una gran cantidad de usuarios de las entidades bancarias de la región La Libertad realiza operaciones por internet, los Bancos no toman medidas de seguridad para evitar que se cometa fraudes electrónicos con sus tarjetas, debido a que esto se ve reflejado en que el 50% de los encuestados que han sido víctimas de fraude electrónico con sus tarjetas han señalado que no se ha tomado ninguna medida de seguridad, mientras que 13 de los 40 encuestados señalaron que si se les envió un mensaje de texto a su celular o se les mandó un correo electrónico notificándoles que se estaba realizando operaciones por internet.

Por lo tanto, de los usuarios que rechazaron estas operaciones fraudulentas reclamaron al banco, debido a que se el monto que se les había cargado a su cuenta oscila desde los S/5 hasta los S/5001. En consecuencia, al haberse efectuado las operaciones no reconocidas a causa del fraude electrónico con tarjetas de crédito o débito se estaría causando un perjuicio económico porque como se ha indicado los importes que se han efectuado son cantidades considerables que el usuario tiene que asumir hasta que su reclamo sea atendido y se verifique que la entidad bancaria no cumplió con optar por medidas de seguridad como parte del deber de idoneidad, es por ello que el total de encuestados señalan que se estaría vulnerando el deber de idoneidad cuando el banco no cumple con las medidas de seguridad necesarias para evitar el fraude electrónico con tarjetas de crédito o débito.

De igual manera en las resoluciones expedidas por el órgano resolutivo de procedimientos sumarísimos de protección al consumidor de Indecopi- La Libertad y que fueron analizadas en la presente investigación, para que se tome en consideración la fijación de la sanción se ha tomado en cuenta distintos criterios entre ellos el daño resultado, lo que vendría a ser el daño económico que se le ocasionó debido a la conducta de la entidad bancaria, ya que terceras personas dispusieron del dinero ilegalmente, lo que ha generado una disminución del patrimonio.

Además, se debe tener en cuenta el tiempo, la incomodidad para reclamar por un hecho que no es justo, pero no solo se trata de haberle causado un perjuicio económico sino que también se causa un daño personal ya que en algunas resoluciones se les ha cobrado el importe por las operaciones y como el usuario no cancelaba porque es una operación que no ha realizado se les envió a la central de riesgo, lo que eso trae como consecuencia que dañen su imagen del usuario.

Sin embargo, no solo se causa un daño al usuario, sino que también este tipo de conductas de los Bancos dañan al mercado porque generan una percepción negativa en los consumidores porque pensarían que envés de facilitar las transacciones comerciales originan un riesgo a su patrimonio, generando de esto, desconfianza e inseguridad.

Por lo tanto, se ha llegado a determinar que los Bancos al no cumplir con el deber de idoneidad para evitar que se cometiera fraude electrónico con tarjetas de crédito y débito originan tres tipos de daño: Daño económico, daño personal y daño al mercado.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1. Discusión N° 1

Discusión con respecto al primer objetivo planteado: Analizar las resoluciones finales sobre procesos de operaciones no reconocidas expedidas por el Órgano Resolutivo de Procedimientos Sumarísimos de Indecopi- La Libertad en los periodos 2017-2019, a fin de determinar el cumplimiento del deber de idoneidad de las entidades bancarias de la región La Libertad en las operaciones que se efectúe el fraude electrónico con tarjetas de crédito y débito.

De los resultados obtenidos, de las 15 resoluciones analizadas sobre operaciones no reconocidas expedidas por el "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi- La Libertad en los periodos 2017-2019, se ha determinado que las entidades bancarias de la región La Libertad han incumplido con el deber de idoneidad en las operaciones que se efectuaron por el fraude electrónico con tarjetas de crédito y débito; debido a que no han adoptado las medidas de seguridad como por ejemplo: la entidad bancaria debe contar con un sistema de monitoreo que evalúe si es que corresponde a patrones de fraude, considerando el comportamiento habitual y el patrón de consumo del usuario, además que el Banco debe alertar al usuario mediante un sistema de notificaciones sobre las operaciones que se están realizando procediendo al bloqueo de la tarjeta temporalmente o de manera definitiva.

Por lo tanto, al no cumplir con las medidas de seguridad la entidades bancarias de la región La Libertad han sido sancionadas con medidas correctivas y multas por haber infringido el deber de idoneidad estipulado en el Art. 19° del Código de Protección y Defensa del Consumidor.

4.2. Discusión N° 2

Discusión con respecto al segundo objetivo planteado: Analizar dentro de la legislación internacional los aspectos normativos sobre el deber de idoneidad en los servicios financieros con tarjetas de crédito y débito, con la finalidad de realizar una comparación con la legislación peruana.

Del análisis de las comparaciones realizadas de las legislaciones de los países de Chile, Ecuador y Colombia con la legislación Peruana, Perú tiene una legislación que define exactamente lo que es idoneidad contenido en el Código de Protección y Defensa del Consumidor, además de cuáles son las obligaciones de los proveedores para cumplir con el deber de idoneidad, a diferencia de Chile, Ecuador y Colombia que no definen lo que es idoneidad, sino que incluyen dicho deber como parte de que no se otorgue una publicidad engañosa.

Asimismo, Perú cuenta con un "Reglamento de Tarjetas de Crédito y Débito" que establece cuales son las medidas de seguridad mínimas que deben tener en cuenta las entidades bancarias para que las operaciones sean realizadas correctamente y se detecte patrones de fraude, a diferencia de Chile,

Ecuador y Colombia no establecen con exactitud sobre las medidas de seguridad que se deben de implementar como cumplimiento del estándar de calidad y seguridad.

4.3. Discusión N° 3

Discusión con respecto al tercer objetivo planteado: Determinar la afectación que causan las entidades bancarias de la región La Libertad a los usuarios por el fraude electrónico con tarjetas de crédito y débito.

De las encuestas realizadas a los usuarios de las entidades bancarias de la región La Libertad, se ha podido comprobar que los Bancos al no cumplir con el deber de

idoneidad para evitar que se cometiera fraude electrónico con tarjetas de crédito y débito ocasionan estos tipos de daño:

i) el daño económico, debido a que el 50% de usuarios han sido víctimas de fraude electrónico con sus tarjetas; y se han efectuado operaciones fraudulentas que oscilan entre los S/5 hasta los S/5001, estos montos que son cargados a la cuenta del usuario le han causado un perjuicio económico porque como se ha indicado los importes que se han efectuados son cantidades que el usuario tiene que asumir hasta que su reclamo sea atentado y se verifique que la entidad bancaria no cumplió con optar medidas de seguridad como parte del deber de idoneidad.

De la misma manera en las resoluciones analizadas expedidas por el órgano resolutivo de procedimientos sumarísimos de protección al consumidor de Indecopi-La Libertad, para determinar la sanción tomaron algunos criterios entre ellos el daño económico que se le ocasionó al usuario por la conducta de la entidad bancaria, debido a que terceras personas dispusieron del dinero ilegalmente, lo que se genera una disminución del patrimonio.

ii) Daño a la persona el usuario al no pagar la operación que rechaza, el Banco lo calificará como deudor y esto acarrea que se le dañe su imagen como usuario responsable; y/o

iii) Daño al mercado porque los consumidores no le tengan confianza a las entidades bancarias porque no cumplen con las medidas de seguridad para salvaguardar el patrimonio del usuario.

4.4. Limitaciones

Se ha tenido limitaciones debido a que por la coyuntura social que se está atravesando no se ha podido entrevistar a abogados que trabajan en entidades bancarias para que

se pueda conocer con que medidas de seguridad cuentan para detectar patrones de fraude, así mismo para que se pueda conocer que solución dan cuando el usuario reclama sobre las operaciones efectuada a causa del fraude electrónico y para que den su opinión sobre el deber de idoneidad que deben de cumplir adoptando medidas de seguridad para evitar que se cometa fraude electrónico con tarjetas de crédito y débito. Además, que no se ha podido entrevistar a miembros del "Órgano Resolutivo de Procedimientos Sumarísimos" de Indecopi- La Libertad, para que den su punto de vista sobre el incumplimiento del deber de idoneidad por la entidades bancarias de la región La Libertad en el fraude electrónico con tarjetas de crédito y débito.

A pesar de estas limitaciones se les ha enviado la encuesta que se ha realizado en la investigación a abogados especialistas en la materia que también han sido víctimas de fraude; y, además han visto casos de clientes que han sido víctimas sobre este hecho. Así también, pese a ello con las resoluciones que se han analizado ha contribuido a llegar a una conclusión con respecto a la presente investigación.

4.5. Conclusiones

4.5.1. Conclusiones N° 1:

Las entidades bancarias de la región La Libertad incumplen con el deber de idoneidad en las operaciones que se efectuaron por el fraude electrónico con tarjetas de crédito y débito, debido a que no han adoptado las medidas de seguridad necesarias y básicas, tales como; que el usuario haya solicitado la habilitación para realizar operaciones por internet, que el banco haya validado en su sistema de operaciones datos relevantes para acreditar la validez de las operaciones, que el banco debe contar con un sistema de monitoreo que le permita evaluar si corresponde a un patrón de fraude considerando el comportamiento habitual, alertar mediante sistemas de

comunicación al usuario sobre la realización de las operaciones y bloquee la tarjeta temporalmente.

4.5.2. Conclusión N° 2

Las legislaciones de Chile, Ecuador y Colombia que ha sido comparadas con la legislación peruana, no cuentan con una definición exacta del deber de idoneidad diferente a Perú cuenta que lo define exactamente en el Art. 19° del "Código de Protección y Defensa del Consumidor". Así también, a diferencia de las legislaciones analizadas que no especifican las medidas de seguridad, Perú cuenta con un "Reglamento de Tarjetas de Crédito y Débito" en la cual señala las medidas de seguridad que el Banco debe tener en cuenta para que las operaciones sean realizadas correctamente, además para que se detecte patrones de fraude y la alerta que debe enviar al usuario por las operaciones.

4.5.3. Conclusión N° 3

Las entidades bancarias al no cumplir con el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito se les ha causado a los usuarios un daño patrimonial, por haberles ha cargado a las cuentas de sus tarjetas montos que oscilan entre los S/ 5 hasta los S/ 5001 por haberse efectuado las operaciones no reconocidas a causa del fraude electrónico con tarjetas de crédito y débito. Además, que se les ocasiona un daño a la persona por haberse enviado a la central de riesgo al usuario por no pagar las operaciones que se han realizado, y/o el daño al mercado porque genera una percepción negativa hacia los consumidores, debido a que envés de facilitar las transacciones comerciales originan un riesgo al patrimonio del usuario, además que generan desconfianza e inseguridad para contratar servicios que ofrecen los bancos.

RECOMENDACIONES

5.1. En mérito a las conclusiones descritas, se recomienda que en el "Reglamento de Tarjetas de Crédito y Débito" se amplíe un párrafo en el artículo 2 inciso 5) incorporando los diversos factores mínimos que no corresponden a patrones de consumo del usuario cuando se realiza operaciones por internet para que la entidad bancaria considere como señales de alerta para que notifique al usuario, cuando:

- Se realiza una operación por internet por primera vez
- Se realice una compra más grande de lo habitual
- Se realice compras de artículos iguales en gran cantidad.
- Se realice compras de artículos que tengan un costo elevado.
- Se realice varias transacciones con la misma tarjeta en un plazo corto.
- Se realice operaciones en un país del extranjero
- Se realice compras con envío a una dirección internacional.
- Se realice operaciones en una ciudad distinta al lugar de residencia del usuario.

5.2. Además, se recomienda que en el artículo 17 inciso 5) del "Reglamento de Tarjetas de Crédito y Débito" se establezca que, para realizar operaciones por internet con tarjetas de crédito, las entidades bancarias deben aplicar un método de autenticación de datos, como por ejemplo un código de autenticación que será enviado por correo electrónico o mensaje de texto del usuario para brindar adecuadas condiciones de seguridad.

REFERENCIAS

Arana, M. (Sf). Contrato de consumo: Cláusula Abusiva. Revista de la competencia y la propiedad intelectual N° 10, 60-61. Recuperado de http://revistas.pucp.edu.pe/index.php/forojuridico/article/download/18415/18655/

Balcazar, W. (2017). Medidas de seguridad que deberían de implementarse a fin de evitar operaciones no reconocidas en tarjetas de crédito. (Tesis de licenciatura). Universidad Privada Antenor Orrego, Trujillo. Recuperado de http://repositorio.upao.edu.pe/bitstream/upaorep/3314/1/RE_DERE_WINNIE.BALCAZAR_MEDIDAS.DE.SEGURIDAD_DATOS.PDF

Bellido, Y. (2018). La idoneidad en las tarjetas de crédito: a propósito de las denuncias ante los órganos competentes de Indecopi durante los años 2013-2015. (Tesis para optar el grado de magister en Derecho). Universidad Nacional Mayor de San Marcos, Lima. Recuperado de http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/9681/Bellido_ay.pdf?sequence=1&isAllowed=y

Cabrera, N y Lombana, M. (2016). Fraude financiero con tarjetas en Colombia 2010 a 2015: ilustración de su evolución y prevención. Recuperado de http://repository.lasalle.edu.co/bitstream/handle/10185/29024/17101047_2016.pdf?sequence=1&isAllowed=y

Conoce los fraudes del comercio electrónico. [Editorial]. (21 de octubre de 2018). *Perú21*. Recuperado de https://peru21.pe/economia/conoce-fraudes-comercio-electronico-435852

Castro, R. (2014). Responsabilidad en los fraudes con las tarjetas de pago. Universidad de La Laguna. Recuperado de https://riull.ull.es/xmlui/bitstream/915/372/1/Responsabilidad+en+los+fraudes+con+tarjetas+de+pago..pdf

¿Cuándo presentar un reclamo ante una entidad financiera y cómo hacerlo? [Editorial]. (05 de julio de 2017). RPP. Recuperado de https://rpp.pe/campanas/contenido-patrocinado/cuando-presentar-un-reclamo-ante-una-entidad-financiera-y-como-hacerlo-noticia-1062416

Defensoría del cliente financiero.(2020,19 y octubre). Obtenido de URL. https://dcf.bancaparatodos.com.pe/

Diaz, S; Angulo, J y Barboza, M. (2018). Análisis del delito de fraude electrónico: modalidad tarjeta de crédito. Universidad Cooperativa de Colombia Sede Montería. Recuperado de https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

Flores, E; Pilco, M y Haro, P. (2015). El uso de las tarjetas de crédito y débito en la sociedad actual. *Revista Caribeña de ciencias sociales*¸ 6. Recuperado de https://www.eumed.net/rev/caribe/2015/08/tarjetas-credito.zip

Gabaldón, L. (2006). Fraude electrónico y cultura corporativa. *Cuaderno CRH* (47), 195-213. Recuperado de https://www.redalyc.org/pdf/3476/347632169004.pdf

Guarnizo, P y Segura, M. (2018). Responsabilidad de las entidades financieras en eventos de fraudes electrónicos. *Revista Nueva Época* (40), 99-126. Recuperado de https://www.researchgate.net/publication/331720115_Responsabilidad_de_las_entidades_financieras_en_eventos_de_fraudes_electronicos

Herrera, J. (2015). Análisis jurídico de las cláusulas abusivas en los contratos de consumo. (Tesis para optar el título profesional de abogado). Lima: Universidad Nacional de San Agustín. Recuperado de http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/2210/DEhepajl.pdf?sequence=1&isAllowed=y

Javato, A. (2012). Tarjetas de crédito y débito. Aspectos penales. Universidad de Salamanca. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4498460

Ley 29571- INDECOPI. *Código de Protección y Defensa del Consumidor* (setiembre 01, 2010). Art. IV "Definiciones". Recuperado de https://www.indecopi.gob.pe/documents/20195/177451/CodigoDProteccionyDefensaDelConsumidor%5B1%5D.pdf/934ea9ef-fcc9-48b8-9679-3e8e2493354e

Ley 29571- INDECOPI. *Código de Protección y Defensa del Consumidor* (setiembre 01, 2010). Art. 18: "Idoneidad". Recuperado de página web https://www.indecopi.gob.pe/documents/20195/177451/CodigoDProteccionyDefensaDelConsumidor%5B1%5D.pdf/934ea9ef-fcc9-48b8-9679-3e8e2493354e

Ley 26702. *Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros* (diciembre, 1996). Artículo 282: "Definiciones". Recuperado de

http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/8CEF5E01E937E76105257A0700610870/$FILE/26702.pdf

Lineamientos de Protección al Consumidor – Indecopi (2016). Obtenido de https://www.indecopi.gob.pe/documents/20182/747822/CC1+y+CPC+-+ILN+-.pdf/cd9a32a6-4aab-4b60-993c-8bb3a202ad89

Martínez, M (2006). La investigación cualitativa (Síntesis conceptual). Revista IIPSI (9), 123- 146. Recuperado de http://sisbib.unmsm.edu.pe/bvrevistas/investigacion_psicologia/v09_n1/pdf/a09v9n1.pdf

Meza, P. (2012). El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación. (Tesis de para obtener bachiller). Pontificia Universidad Católica del Perú. Perú. Recuperado de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/1668/MEZA_ALAYO_PAOLA_CONSUMIDOR_CLONACION.pdf?sequence=1&isAllowed=y

Molano, Y y Correa, Y. (2016). Predicción del fraude con tarjetas para una entidad financiera a través del modelo arimax. (Tesina). Universidad de Los Libertadores Recuperado de https://repository.libertadores.edu.co/bitstream/handle/11371/760/MolanoD%C3%ADazYulyAlexandra.pdf?sequence=2&isAllowed=y

Nuevo récord de fraudes de dominio en internet en el 2018, con 3,447 casos [Editorial]. (18 de marzo de 2019). *Gestión*. Recuperado de https://gestion.pe/tecnologia/nuevo-record-fraudes-dominio-internet-2018-3-447-casos-261610

Ñaupas, C (2016). Minería de datos aplicada a la detección de fraude electrónico en entidades bancarias. (Para optar Título de ingeniero de sistemas). Universidad Nacional Mayor de San Marcos, Lima. Recuperado de http://cybertesis.unmsm.edu.pe/handle/20.500.12672/5080

Paz, S (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. *Revista de Derecho Privado* (35), 261-289. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7013328

Porco, A. (2015). Modelos computacionales y metodologías utilizadas en la detección del fraude de las tarjetas de crédito. (Tesis de licenciatura). Universidad Nacional de la Plata, Argentina. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/71300/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017 [Editorial]. (10 de agosto de 2017). *Gestión.* Recuperado de https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411

Perú. Superintendencia de Banca y Seguros . Resolución S.B.S N°6523-2013: Reglamento de tarjetas de crédito y débito. (30 de octubre de 2013). Recuperado de https://intranet2.sbs.gob.pe/dv_int_cn/718/v3.0/Adjuntos/6523-2013.pdf

Perú. Superintendencia de Banca y Seguros. Resolución S.B.S N° 5570-2019: Modifican Reglamento de Tarjetas de Crédito y Débito, el Reglamento para la Administración del Riesgo de Sobre Endeudamiento de Deudores Minoristas, el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Crédito y otros dispositivos legales. (27 de noviembre de 2019). Recuperado de https://busquedas.elperuano.pe/normaslegales/modifican-reglamento-de-tarjetas-de-credito-y-debito-el-reg-resolucion-no-5570-2019-1831401-1/

Procedimiento de atención BBVA. (2020,19 y octubre). Obtenido de URL. https://www.bbva.pe/personas/canales-de-atencion/procedimiento.html

Procedimiento de atención de consultas y reclamos-BCP. (sf). Obtenido de URL. http://ww3.viabcp.com/Connect/Contacto%20al%20cliente/Procedimiento%20de%20atencion%20de%20consultas%20y%20reclamos.pdf

Reclamos y consultas- Scotiabank Perú. (2020, 18 y octubre). Obtenido de URL. https://www.scotiabank.com.pe/Acerca-de/A-Tu-Servicio/Canales-de-atencion/reclamos-y-consultas

Rodríguez, A. (2014). Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional. *Universitas,* (128), 285-314. Recuperado de http://www.scielo.org.co/pdf/vniv/n128/n128a10.pdf

Sánchez, G. (2012). Delitos en internet: Clases de Fraudes y estafas y las medidas para prevenirlos. *Boletín de información N° 324.* Recuperado de https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

Sampieri, R (2014). Metodología de la investigación. México (Sexta Edición). Recuperado de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Sarmiento, C. (2015). Motores de riesgo transaccionales ¿Solución eficaz para reducir agresivamente el fraude electrónico? *Universidad Piloto de Colombia*, 1-6. Recuperado de http://polux.unipiloto.edu.co:8080/00002059.pdf.

Soto, E. (2015). Uso malicioso de una tarjeta comercial hurtada robada o extraviada. *Ars Boni et Aequi* (11), 203-220. Recuperado de https://dialnet.unirioja.es/descarga/articulo/5853819.pdf.

Superintendencia de Banca y Seguros. Guía del docente. Recuperado de https://www.sbs.gob.pe/portals/3/educacion-financiera-pdf/Guia%20del%20docente%202017.pdf

Vodanovic, L (2013). La dinámica entre la regulación prudencial del sistema financiero y la protección del consumidor. En Rivera, C (2017). Replanteando Roles: Análisis del modelo de regulación y supervisión bancaria en el Perú en materia de protección al consumidor financiero. (pp 17), Lima: Pontificia Universidad Católica del Perú. Recuperado de http://textos.pucp.edu.pe/pdf/4899.pdf

ANEXOS

ANEXO I: PROPUESTA DE PROYECTO DE RESOLUCIÓN

PROYECTO DE RESOLUCIÓN N° XXXX/2020-EF

Proyecto de Resolución: Propone Resolución que modifica el artículo 2.5 y artículo 17.5 Resolución N°6523-2013, "Reglamento de tarjetas de crédito y débito".

CONSIDERANDO:

Según el "Reglamento de Tarjetas de Crédito y Débito", Resolución N° 6523-2013, define que el comportamiento habitual de consumo del usuario hace referencia al tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros que pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa. Así también, con respecto a operaciones con tarjetas se debe requerir al usuario que se utilice un mecanismo de autenticación de múltiple factor.

Dicha definición limita el comportamiento habitual señalando factores mínimos que no corresponden a patrones de consumo del usuario cuando realiza operaciones, además que no se señala el mecanismo de autenticación de múltiple factor que se debe establecer para operaciones por internet con tarjetas de crédito.

Que, es necesario regular a través de un reglamento, que se establezca el comportamiento habitual y se mencione los diversos factores mínimos que no corresponden a patrones de

consumo del usuario cuando se realiza operaciones por internet para que la entidad bancaria considere como señales de alerta para que notifique al usuario

Que, es necesario que, para realizar operaciones por internet con tarjetas de crédito, las empresas deben aplicar un método de autenticación de datos, como por ejemplo un código de autenticación que será enviado por correo electrónico o mensaje de texto del usuario para brindar adecuadas condiciones de seguridad.

Por las consideraciones expuestas, se propone a la Superintendencia de Banca y Seguros el siguiente Proyecto de Resolución:

RESOLUCIÓN QUE MODIFICA LA RESOLUCIÓN N° 6523-2013, REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO

Artículo 1.- Alcance

La presente Resolución tiene por objeto modificar el artículo 2 inciso 5) y artículo 17 inciso 5) de la Resolución N° 6523-2013, Reglamento de Tarjetas de Crédito y Débito.

Artículo 2.- Modificación del Artículo 2.5° de la Resolución N° 6523-2013, "Reglamento de Tarjetas de Crédito y Débito".

Modifíquese los artículos 2.5°, Resolución N°6523-2013, incorporando un párrafo, en los siguientes términos:

> "Artículo 2.- Definiciones
>
> (…)
>
> 2.5. No corresponden a patrones de consumo del usuario cuando se realiza operaciones por internet para que la entidad bancaria considere como señales de alerta para que notifique al usuario, cuando:

a) Se realiza una operación por internet por primera vez

b) Se realice una compra más grande de lo habitual

c) Se realice compras de artículos iguales en gran cantidad.

d) Se realice compras de artículos que tengan un costo elevado.

e) Se realice varias transacciones con la misma tarjeta en un plazo corto.

f) Se realice operaciones en un país del extranjero

g) Se realice compras con envío a una dirección internacional.

h) Se realice operaciones en una ciudad distinta al lugar de residencia del usuario.

Artículo 3.- Modificación del artículo 17.5° de la Resolución N° 6523-2013, Reglamento de Tarjetas de Crédito y Débito.

Modifíquese el artículo 17.5° de la Resolución N°6523-2013, Reglamento de Tarjetas de Crédito y Débito en los siguientes términos:

"Artículo 17.- Medidas de Seguridad respecto al monitoreo y realización de las operaciones

(…)

17.5. Para realizar operaciones por internet con tarjeta de crédito, las empresas deben aplicar un método de autenticación de datos, como por ejemplo un código de autenticación que será enviado por correo electrónico o mensaje de texto del usuario para brindar adecuadas condiciones de seguridad.

Trujillo, ……

ANEXO II

CUESTIONARIO DE PREGUNTAS

La presente encuesta se desarrolla en el marco de la investigación para determinar si las Entidades Bancarias cumplen con el deber de idoneidad en el fraude electrónico con tarjetas de crédito y débito en los clientes de las entidades financieras de la Región La Libertad, 2020. Para tal efecto se precisará los siguientes términos:

- **Deber de idoneidad:** Es el principio mediante el cual el consumidor espera recibir el producto o servicio, en función de la información que el proveedor le ha brindado al momento de adquirir el bien o servicio.

- **Fraude electrónico:** Conducta que es realizada por un tercero ajeno al titular de la tarjeta de crédito o débito, que realiza transacciones por conductos electrónicos y que le causa un perjuicio.

1. ¿Usted cuenta con tarjeta de crédito y/o débito?

( ) SÓLO CRÉDITO
( ) SÓLO DÉBITO
( ) AMBAS
( ) NINGUNA

2. ¿De qué Banco usted adquirió la tarjeta de crédito o débito?

( ) Scotiabank S.A. ( ) BCP (Banco de Crédito del Perú S.A.)

( ) Interbank S.A. ( ) BBVA S.A.

( ) Otro (especifique)_____

3. ¿Al momento de adquirir su tarjeta, el Banco le informó sobre la habilitación de compras por internet?

( ) SI ( ) NO

4. ¿Realiza compras por internet con su tarjeta de crédito y/o débito?

( ) SI ( ) NO

5. ¿Ha sido víctima alguna vez de fraude electrónico con su tarjeta de crédito y/o débito?

( ) SI ( ) NO

6. En el caso que haya sido víctima de fraude electrónico con su tarjeta de crédito o débito ¿El banco tomó algunas de las medidas de seguridad que se muestran a continuación para evitar dicho fraude?

( ) ME MANDARON UN MENSAJE DE TEXTO A MI CELULAR

( ) ME MANDARON UN CORREO ELECTRÓNICO NOTIFICANDOME DE LA OPERACIÓN

( ) NO TOMARON NINGUNA MEDIDA DE SEGURIDAD

( ) NO FUI VICTIMA DE FRAUDE ELECTRÓNICO

7. En el caso de que el Banco no tomó medidas de seguridad para evitar que se cometiera el hecho ilícito ¿UD reclamó ante el Banco por haberse efectuado operaciones con cargo a su tarjeta por el fraude electrónico?

( ) SI

( ) NO

( ) NO FUI VICTIMA DE FRAUDE

8. ¿De cuánto fue el importe que se le cargo a su tarjeta de crédito o débito por la operación que se efectúo a causa del fraude electrónico?

( ) S/5- S/50 ( ) S/ 51- S/500

( ) S/ 501- S/1001 ( ) S/ 1001-S/5000

( ) Más de S/5001 ( ) NO FUI VICTIMA DE FRAUDE

9. ¿Ud. cree que se le estaría causando un perjuicio económico al efectuarse las operaciones no reconocidas a causa del fraude electrónico con su tarjeta de crédito o débito?

( ) SI

( ) NO

( ) NO FUI VICTIMA DE FRAUDE ELECTRÓNICO

10. ¿Ud. cree que se estaría vulnerando el deber de idoneidad al momento de que el banco no cumple con las medidas necesarias para evitar el fraude electrónico con las tarjetas de crédito o débito?

( ) SI ( ) NO