UNIVERSIDAD PRIVADA DE TRUJILLO

FACULTAD DE DERECHO

CARRERA PROFESIONAL DE DERECHO

TESIS PARA OPTAR EL TITULO PROFESIONAL DE

ABOGADO

TRANSACCIONES FRAUDULENTAS Y DELITOS INFORMATICOS

COAUTORES:

ABAD HARO JAIME HUMBERTO

REYES CORCINO MARITZA JOVANNA

ASESOR:

MG. WALTER RAFAEL LLAQUE SANCHEZ

Trujillo – Perú

2022

PRESIDENTE

SECRETARIO

VOCAL

DEDICATORIA:

Esta Tesis esta dedicada a Dios, por dar la fuerza para continuar a pesar de las

adversidades; a mi familia quienes me

apoyan sin importar las circunstancias.

AGRADECIMIENTO:

Agradezco a Dios por cada día de vida, a

mi familia quienes con un granito de arena han apoyado este reto académico.

INDICE DE CONTENIDOS

Páginas

El presente trabajo de investigación fue desarrollado en la facultad de Derecho de la Universidad Privada de Trujillo. Su objetivo principal es determinar cómo es que las transacciones fraudulentas y delitos informáticos afectan el derecho patrimonial de los consumidores en los soportes virtuales. Para alcanzar este objetivo se realizó un estudio con los abogados penalistas especialistas en la materia.

El tipo de estudio es orientado al cambio y toma de decisiones, el diseño de estudio es Fenomenológico. La investigación cuenta con la variable independiente: Transacciones fraudulentas, y la variable dependiente: Delitos informáticos.

Se trabajó con un total de 10 participantes que son abogados especialistas en la materia; se ha empleado un cuestionario de preguntas cerradas. El estudio permitirá

entender el fenómeno social complejo que se aborda, así como comprender posibles aspectos a mejorar en nuestro ordenamiento jurídico nacional.

Se concluye que la manera en que las transacciones fraudulentas y los delitos informáticos afectan los derechos de autor en soportes virtuales, es porque la herramienta virtual del internet brinda a los consumidores la obtención de contenido gratuito de los cuales se han creado o se han destinado para tener un enriquecimiento hacia las empresas que son dueños de ese contenido por los derechos de autor que los protege, siendo así que de esa manera es que se transgrede los derechos de autor de las empresas en los soportes virtuales.

Palabras clave: Transacción, delito informático, consumidor, soporte virtual.

ABSTRACT

This research work was developed at the Law School of the Private University of Trujillo. Its main objective is to determine how fraudulent transactions and computer crimes affect the economic rights of consumers in virtual media. To achieve this objective, a study was carried out with criminal lawyers specializing in the matter.

The type of study is oriented to change and decision making, the study design is Phenomenological. The investigation has the independent variable: Fraudulent transactions, and the dependent variable: Computer crimes.

We worked with a total of 10 participants who are lawyers specialized in the matter; a closed question questionnaire has been used. The study will allow us to understand the complex social phenomenon that is being addressed, as well as to understand possible aspects to improve in our national legal system.

It is concluded that the way in which fraudulent transactions and computer crimes affect copyrights in virtual media is because the virtual tool of the internet provides consumers with obtaining free content of which they have been created or have been destined for have an enrichment towards the companies that own that content due to the copyright that protects them, being so that in this way it is that the copyright of the companies in virtual media is violated.

Keywords: Transaction, computer crime, consumer, virtual support.

I. INTRODUCCION

1.1. Realidad Problemática

Las últimas generaciones se han visto envueltas en un entorno globalizado, y, sobre todo, con una fuerte influencia por el internet. Las compras y servicios de todo tipo ahora son más sencillas gracias a las transacciones mediante plataformas virtuales que facilitan el comercio de los consumidores. Por lo que, en teoría, también sería más sencillo la inseguridad, el cometimiento de infracciones y los delitos.

Investigar el delito desde cualquier perspectiva es una tarea compleja; de eso no hay duda. Las dificultades que surgen al tratar de aplicar el método científico a la Delincuencia Transnacional y al Crimen Organizado en buena parte ya fueron establecidas en estudios anteriores, pero enfrentar este tipo de delincuencia a todo nivel es la tarea a la que se ve avocada le

Ministerio Público por mandato constitucional y por disposición legal. (Acuario, 2015). Asimismo, Acuario menciona que:

El fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados delitos Informáticos.

Cuando se logra entender esto, nos vemos en el otro plano a tratar, las transacciones. Ahora, los métodos de pago en internet logran juntar dinero de velozmente, disminuir el trabajo y costo operativo asociado, lo cual, provoca a ser eficaces en procesos internos y dar un servicio mejorado y transparente.

No obstante, los consumidores de estas plataformas no suelen tener el conocimiento de cómo funciona la política de cada empresa que permite el cobro de sus servicios a través de internet, como tampoco conocen la seguridad de una entidad bancaria, y mucho menos conocen los límites de la seguridad brindada en este medio virtual. Esto significa tener problemas culturales y de administración, requieren integrar sistemas legados con el sistema del mundo moderno, por lo que las aplicaciones móviles y las más importantes deben generar confianza a los usuarios, cualquiera que sea la plataforma de pago principal.

Los datos colocados en estos medios son cada vez mayores, desde información personal hasta número de cuentas. Por ejemplo, las dos estafas concurridas suelen ser: Phishing y los robos de identidad, directamente relacionadas con el otro tema mencionado.

La primera, radica en usar mensajes con datos o información maliciosa solicitando un pago o cobro, dando a conocer una promoción o accediendo a una dirección o link de internet infectado con programas troyanos o virus (generalmente para robar o destruir información, los infractores utilizan

diferentes técnicas de la informática para atacar a los consumidores conectados, aquí usan este conocimiento buscando recopilar la información de la gente, ya sea como datos personales, datos también de sus de sus tarjetas o usuario y contraseña.

Con esta información, el delincuente realiza transferencias a cuentas del mismo banco, por ejemplo, o transferencias a cuentas de otro banco, pagos a terceros en cuanto a deudas, servicios, permisos, etc.

Es decir, compras o pagos por internet a través de una tarjeta de crédito, suelen ser, los métodos más comunes y cómodos de cómo acceder a servicios en el mundo moderno. Qué hacer, a quién reclamar y quién es culpable puede ser una cuestión del caso en concreto, pero que a grandes rasgos se resuelve con las grandes ideas principales del derecho. Es aquí donde nace el interés y la necesidad de encontrar una respuesta a un entorno cada vez más tecnológico.

Es elemental recaudar información valiosa para pronunciarse sobre el tema como la Opinión Consultiva No. 01-2018-JUS/DGTAIPD (2018) que expone lo siguiente:

Un uso ilegal de la información de una tarjeta de crédito sin el conocimiento del titular real de la tarjeta acredita a disputar el cargo poniéndose en contacto con su banco. El banco o la empresa de tarjetas de crédito realizarán una investigación y le devolverá el dinero al titular de la tarjeta.

El tema del contrato por internet viene con mucha fuerza, la mayoría de transacciones se ejecutan mediante un “contrato por adhesión” donde brindan simplemente el lugar o plataforma en la que se realiza la actividad comercial, donde, sin embargo, no se cuenta con una seguridad jurídica.

De igual manera, cuando se habla de delitos informáticos, se entiende que ahora la forma de cometerlos en mucho más sencilla, el delito más común

es el tráfico ilegal de datos, fraudes informáticos, accesos ilícitos y una violación contra los derechos de autor.

Ahora, uno de los problemas más comunes que recibe INDECOPI, son los consumos fraudulentos mediante tarjetas de crédito, servicios que brindan los bancos, lo mismo para los cobros de membresía, incluido también el tema de los consumidores quienes se adhieren a este tipo de servicios buscando facilidades, pero no lo hacen tomando en cuenta la información necesaria que consta no solamente de derechos sino también de deberes.

Entonces existe una delgada línea entre saber si la desinformación acarrea una responsabilidad en el consumidor por la "duda", o si es la entidad bancaria quien necesita brindar absoluta seguridad y protección a sus consumidores, ya que, teniendo en cuenta la fuerte influencia del internet, y lo relativamente sencillo que es cometer un delito informático, es necesario brindar una seguridad jurídica.

Se entiende que el derecho debe evolucionar al igual que la tecnología, de ser el caso en contrario, sobre todo con la fuerte influencia de este medio de comunicación, la ley no estaría contemplando muchos supuestos en los que las personas estarían siendo víctimas de muchas y nuevas formas.

Mediante este trabajo de investigación se busca proyectarse al futuro, asumiendo que estas nuevas formas de afectaciones están muy cerca y esta modalidad requiere una regulación, ya que el eterno conflicto de intereses es difícil de determinar, por ser un tema poco tratado, para el esclarecimiento del tema, se ha querido realizar el presente trabajo de investigación.

1.2. Formulación del problema:

¿De qué manera las transacciones fraudulentas y los delitos informáticos afectan el derecho patrimonial de contratar, de los consumidores en los soportes virtuales?

1.3. Justificación

La justificación teórica del trabajo, se sustenta en diversas teorías y estudios sobre las transacciones fraudulentas y los delitos informáticos, como la Teoría del Riesgo Provecho, el Riesgo Creado y el Riesgo Profesional de Rodríguez Zárate, fundamentándose en la responsabilidad objetiva, subjetiva y las fallas del mercado, estableciendo que no existe claridad en torno a la posibilidad de determinar un régimen de responsabilidad objetiva basándose en la teoría de los riesgos, por lo que el régimen de responsabilidad objetiva bajo este panorama no resulta ser la solución más eficiente.

Por lo que, al no existir una claridad, y a la urgencia de tenerla debido al aprovechamiento de estas deficiencias, que son los delitos informáticos, siendo sustentando en este trabajo en la Teoría de la Criminalidad de los Delitos Informáticos, por Acuario del Pino. Se parte tomando en cuenta que estos aportes doctrinarios y teóricos, nacionales e internacionales, indican que hace falta en la legislación peruana una respuesta que logre minimizar los riesgos y organizar mejor el control de estas prácticas, siendo también un fin de la investigación el aporte al conocimiento ya existente sobre el tema abordado.

La justificación practica para este trabajo de investigación es que tanto como el derecho patrimonial como el derecho a la propiedad se encuentran vulnerados al momento de realizar compras o prácticas en internet, al utilizar la compra en línea, se logra así una serie de inconvenientes en los consumidores de estos productos, generando una deficiencia en la sociedad; por ende, se cree conveniente la protección jurídica que se le debe dar a los consumidores ante este tipo de prácticas tecnológicas.

1.4. Objetivos

1.4.1. Objetivo General:

Determinar cómo es que las transacciones fraudulentas y delitos informáticos afectan el derecho patrimonial de los consumidores en los soportes virtuales

1.4.2. Objetivo Especifico:

a. Analizar cómo es que las transacciones fraudulentas y los delitos informáticos afectan el derecho de contratar

b. Analizar cómo es que las transacciones fraudulentas y los delitos informáticos afectan los derechos de autor en soportes virtuales

1.5. Antecedentes.

Internacional

Laura Mayer Lux (2017) en su artículo de investigación titulado "El bien jurídico protegido en los delitos informáticos" en la Revista Chilena de Derecho, vol. 44 Nº 1, concluyó:

La funcionalidad informática es un presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su servicio en un Estado democrático de derecho. Esta, se identifica con aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo. El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. En ese contexto, la funcionalidad informática constituye, por una parte, un interés cuyo sentido y alcance debe precisarse dinámicamente, así como en atención a la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre los individuos. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados.

José Santiago Rendón Vera (2007) en su trabajo de grado titulado "Responsabilidad Civil Contractual por fraudes con tarjeta de crédito en

Colombia" sustentado en la Universidad EAFIT Escuela De Derecho Medellín, concluye:

Para que el sistema pueda enfrentar los riesgos por fraude es necesario que las partes cooperen en el desarrollo de la actividad y para que la tarjeta de crédito pueda cumplir su finalidad. Como derivados del principio de cooperación surgen para cada participante, la obligación de desplegar unas conductas de prevención de fraudes".

Daniela Salas Peña (2010) en su tesis de grado titulada "Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos" sustentada en la Universidad de Costa Rica, concluye que:

A la par de las ventajas que proporciona la Banca por Internet se encuentras las herramientas que se han desarrollado con el fin tomar partido, de forma ilícita, de este moderno instrumento. Se desarrollan así una serie de delitos informáticos a través de los cuales los delincuentes cibernéticos pretenden obtener un beneficio patrimonial ilegítimo, defraudando al consumidor de servicios bancarios por Internet. Los más comunes, por su nivel de afectación al cliente, han sido el Pishing, el Pharming, el Malware, los Keyloggers y los Troyanos o Caballos de Troya, entre otros.

Nacional

Katia Silvana Peñaloza Vassallo (2018) en su trabajo de investigación titulado "¿Cómo educar al consumidor financiero y no morir en el intento?" sustentada en la Pontifica Universidad Católica del Perú, concluye que:

La implementación de la educación financiera como herramienta de protección al consumidor financiero evidencia un gran obstáculo y es que el sujeto destinatario de los programas educativos no busca información ni reconoce que la educación financiera le genera beneficios, como adoptar mejores decisiones de consumo no solo al momento de contratar un bien o servicio, sino también

durante la ejecución de la prestación. Por ello, no basta con obligar a los proveedores a brindar más información, debido a que los consumidores no la demandan, es decir, no la consultan. Por tanto, para efectos de instituir una política eficaz es igual de importante identificar qué información brindar, así como la manera de hacerlo de forma atractiva para el público objetivo.

Chávez Rodríguez Elías Gilberto (2018) en su tesis titulada "El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de lima norte, 2017" sustentada en la Universidad Federico Villareal recomienda que:

El Estado a través del poder judicial brinde capacitaciones constantes a los operadores del derecho de la Corte Superior de Justicia de Lima Norte en relación a los principios generales de protección de la información pública y privada (información sensible, de control, limitación a la información personal, a la verdad actualizada, seguridad personal, indemnización civil), esto con la finalidad de garantizar la protección de los derechos fundamentales a la intimidad personal y familiar por actos ilícitos cometidos utilizando la informática.

Local

Winnie Yennifer Balcázar Díaz (2017) en su tesis titulada "Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito" sustentada en la Universidad Privada Antenor Orrego, concluye:

Asimismo, los principales mecanismos de seguridad en las tarjetas de crédito y tarjetas de débito son las claves secretas; con la que se obtiene total acceso, permitiendo el uso de las mismas; en esta línea, el INDECOPI, al requerir la información de todos los documentos de las transacciones realizadas por el supuesto "titular"; la entidad bancaria o financiera, entrega los reportes Tándem y Journals correspondientes a las operaciones generadas; sin embargo, esta información solo indicará que las operaciones se realizaron de manera habitual

porque se digitó la clave secreta correctamente; la misma que, ya no es suficiente para verificar si se trata de operación veraz o de una operación no reconocida.

1.6. Bases Teóricas

CAPÍTULO I: DELITOS INFORMATICOS

1. DEFINICIÓN

Esta manera delictiva de actuar se puede definir, citando a Callegari (citado por Telles, 1996) como "aquel que se da con la ayuda de la informática o de técnicas anexas". Lo negativo de esta definición es que la autora no tiende a considerar como medio de comisión de esta clase de delitos a la informática, olvidándose que también que lo informático puede ser el objeto de la infracción

Por lo que, Davara Rodríguez (1995) que define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o

telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Siguiendo la idea del autor precedente, este señala que, en algún sector de la doctrina, se subrayará que el delito informático, más que una forma de delito, supone un conjunto de modalidades delictivas relacionadas con la informática y las computadoras.

Asimismo, se puede indicar que el delito informático debe utilizarse en forma plural, pues se utiliza para designar un conjunto de hechos ilícitos y no consta de carácter general, por lo que se hablará de delito informático siempre y cuando se refieran a una conducta o modalidad en particular, que se valga de la informática para cometer un acto ilícito penal.

Se concluye, que, para poder definir el contenido de los delitos informáticos, hay que tener en cuenta que se caracteriza por una denominación de carácter general y flexible, puesto que se relaciona con la delincuencia informativa. Por lo que se los define como toda conducta ilícita que tiene como finalidad alterar, modificar, destruir o manipular maliciosamente cualquier aspecto del sistema informático, causando daño al bien jurídico protegido.

2. BIEN JURÍDICO PROTEGIDO

Según el autor Acurio del Pino (2015), indica que “el bien jurídico protegido es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico; y finalmente por los sistemas que la procesan”.

Asimismo, su contenido está formado por los siguientes bienes jurídicos especificados en el Código Penal Peruano, como:

- El patrimonio, puesto que el fraude o tráfico financiero tiene por finalidad obtener el dinero, o los productos que han enajenado otras personas a través de un servicio financiero electrónico.

- La reserva, la intimidad y confidencialidad de los datos, puesto que también tiene la modalidad de robo de identidad o información de los datos de las personas inscritas en el sistema financiero virtual.

- La seguridad o fiabilidad del tráfico jurídico y probatorio.

- El derecho de propiedad.

Asimismo, el carácter delictivo de esta figura ilícita es pluriofensivos, pues como se ha mencionado anteriormente afecta a diferentes bienes jurídicos protegidos al momento de su comisión.

3. SUJETOS

En el derecho penal, toda conducta ilícita supone la existencia de dos sujetos, uno que comete el acto delictivo, y el otro que se encuentra se afectado por este; empero eso significa que no solamente puede ser un sujeto que comete la acción, puesto que pueden ser varios, y también no solamente un sujeto puede ser el afectado con el delito, sino también varios sujetos, pudiendo ser entidades financieras, consumidores, etc.

Por ende, los sujetos se clasifican de la siguiente manera:

a) Sujeto activo.

Según el autor Garrido (citado por Jijena, 1993) refiere que, se entiende a todo sujeto activo, "por quien realiza toda o una parte de la acción descrita por el tipo penal". Las personas que infringen la ley, cometiendo delitos informáticos, son las que no poseen el común denominador de los infractores, pues tienen habilidades para el manejo de los sistemas informativos, y generalmente su status laboral es alto, por lo que así evitan ser descubiertos.

Con la evolución del tiempo, se ha podido observar que los autores de este tipo de delitos son variados, por ejemplo, al momento que un empleado de un banco desvía

fondos de la cuenta de los clientes, para beneficio propio; o cuando se ingresa al sistema de datos de un banco, para robar la identidad de los clientes que se encuentran registrados ahí. Son diferentes las formas en las que puede actuar el sujeto activo del hecho punible.

b) Sujeto pasivo.

Aquí en estos casos, el sujeto pasivo es la persona a quien se le ha vulnerado el bien jurídico protegido, puesto que es el titular, se le puede denominar como víctima del delito, porque es el sujeto en quien recae la conducta de acción u omisión que realiza el sujeto activo.

En el especifico caso, de los delitos informáticos, los sujetos pasivos, pueden ser:

- Individuos.
- Instituciones crediticias.
- Gobiernos.
- Otros que usan sistemas automatizados de información, generalmente conectados a otros.

4. CLASES

a) Extravío o hurto.

Esta forma es una de las más típica al momento de realizar una operación en una entidad financiera, en la utilización de tarjetas de crédito y tarjeta de débito, pues en ellas se suele producir por pérdida, robo o sustracción.

Este acto sucede cuando un tercero malicioso (sujeto activo) con la tenencia de la tarjeta suplanta la identidad del titular, imitando su firma, su rúbrica, logrando así adquirir bienes y/o servicios, a costa de la propiedad del sujeto pasivo. O también sucede en los casos cuando se adquieren los datos de una tarjeta de crédito o débito, tales como: número de tarjeta, nombre del titular, y todos los datos que se requieren

al momento de realizar una transferencia virtual, puesto que es muy fácil hacer compras mediante internet suplantando la identidad del titular.

Lo que procede a realizarse es: bloquear la tarjeta y denunciar la compra como no reconocida, así el banco o entidad financiera realizará una investigación para reconocer en que momento especifico sucedió la compra, en qué lugar, en que entidad, y a qué hora, para verificar si quien la realizó no era titular.

b) Clonación o Skimming.

Es un delito informático, que consiste en la duplicación maliciosa, fraudulenta, y no autorizada de datos personales que s encuentran en el registro que posee la tarjeta de crédito o debido; su procedimiento se realiza a través de un móvil llamado

"skimmer", que copia todos los datos de las tarjetas al servidor de la persona quien realiza este acto delictivo.

Se le puede denominar también como la falsificación de la misma tarjeta, pues existe una simulación de modo que induce a error sobre la autenticidad a quien admite la tarjeta como un medio de pago, generando que el límite de crédito que contiene la tarjeta sea totalmente despilfarrado, pudiendo aumentar el crédito de la tarjeta, o retirar todo el monto, entre otros supuestos más.

c) Phishing

Es un delito informatico, utilizado por los conocidos "hackers" mediante el cual se obtiene datos confidenciales de forma maliciosa. Es así que, el estafador se hace pasar por una empresa de confianza y mediante el envío de un correo electrónico de la empresa del sistema financiero afectada, obtiene información de sus usuarios: número de tarjeta y clave secreta. En el contenido engañoso del correo electrónico se indica:

- Que la cuenta será deshabilitada si es que no se actualiza los datos del titular.

- Que el cliente ha sido ganador de un premio y lo invitan a ingresar sus datos para poder reclamar dicho premio.

Después de ser ingresada la información (número de cuenta clave secreta y otros), ésta es almacenada y utilizada para suplantar al cliente, efectuando compras o transferencias de su dinero.

d) Pharming

Los pharmers utilizan sitios web falsos, casi idénticos a los originales, para robar información confidencial de víctimas. Es más difícil detectarlos ya que no necesitan que la víctima acepte un mensaje falso. En lugar de depender de que los usuarios hagan clic en vínculos engañosos de correo electrónico, el pharming redirige a sus víctimas a sitios web falsos, aún incluso si uno escribe correctamente la dirección web. (Banco de Crédito del Perú, 2017)

e) Shishing

El smishing es una modalidad de phishing que consiste en el envío de mensajes (SMS) que llegan a las víctimas, indicando que el banco ha dado de alta un determinado servicio, y que se le cobrará cierta cantidad a menos que cancele su petición llamando al número de teléfono indicado. Para la cancelación del servicio, y su 40 correspondiente reembolso, piden que la víctima comparta su clave y contraseña. (Banco de Crédito del Perú, 2017)

f) Vishing.

Es un delito informático que se deriva del phising pero no ofrece un enlace para que la víctima haga clic en él, sino que le ofrece un número de teléfono. En un teléfono aparentemente corporativo, lo espera una persona que se hace pasar por un empleado de banco, quien le solicitará sus datos personales. Para lograrlo, el funcionario indica que como la tarjeta ha sido clonada, necesita la clave para anular la tarjeta en el sistema. (Banco de Crédito del Perú, 2017)

g) Spyware.

Es una aplicación que los delincuentes han conseguido introducir en el ordenador de la víctima, al ingresar a páginas web infestadas con virus. Una vez que el "troyano", como se le conoce al virus que se introduce en nuestra PC, se aloja en el ordenador, este comienza a enviar datos del equipo informático, relativos a claves de acceso, al ordenador del delincuente cibernético, quien lo utiliza para acceder a las claves financieras. (Banco de Crédito del Perú, 2017)

5. TRANSACCIONES FRAUDULENTAS

Son órdenes y compras realizadas con tarjetas de crédito y cuentas bancarias que no pertenecen al comprador.

En realidad, ninguna de las herramientas y tecnologías revisadas por un estudio puede por sí misma eliminar el fraude, cada técnica agrega valor a la habilidad de detectar el fraude, y postula que una buena práctica ha sido la combinación de varias de ellas, por ejemplo revisar el uso múltiple de una tarjeta en diferentes sitios físicos o virtuales durante un corto período de tiempo, Existe todo un conjunto de técnicas implementadas por los software de detección de fraude, de todas ellas, están las reglas de asociación.

6. DERECHO PATRIMONIAL

Se considera parte de una de las ramas que comprende el derecho de autor y propiedad intelectual, puesto que, permite al autor obtener una retribución económica por el uso de su obra por parte de terceros, por lo que les otorga el derecho a impedir que estos terceros la utilicen en contra de su voluntad o sin su autorización.

Asimismo, le permite al autor obtener ventajas de su creación, permitiendo a otras personas, a través de permisos o licencias, su utilización; además también puede ceder su derecho patrimonial de manera que el tercero adquiriente lucre y genere ingresos con esta obra.

Es por ello, que se puede definir al derecho patrimonial del autor como un derecho totalmente cesible y transferible. Este derecho está a cargo de una persona natural,

la cual se le denomina titular del derecho de autor, teniendo así la capacidad intelectual de la obra, y de ceder o transferir su propiedad a un tercero, así sea este una persona jurídica.

Por lo que, se puede definir a este derecho como "aquellos que tienen por objeto el provecho económico por el autor mediante la explotación de la obra". (ONG Derechos Digitales, 2015).

Se entiende, que el derecho patrimonial del autor, está compuesto por derechos que son de titularidad del autor creador de la obra. Estos derechos forman parte del patrimonio que ostenta de titularidad, es decir, sus creaciones o sus obras, son su patrimonio.

CAPÍTULO II: TEORIAS DOCTRINARIAS

1. TEORIA DE LA RESPONSABILIDAD CIVIL FRENTE AL CLIENTE POR DELITOS INFORMATICOS

Se desarrolló por Daniela Salas Peña, en el año 2010 en su tesis de grado titulado "La Responsabilidad Civil Bancaria frente al cliente por los Delitos Informáticos" en donde se sostiene:

Se debe recoger la responsabilidad objetiva, como criterio de impugnación, se menciona que ha sido desarrollándose más dentro de las legislaciones últimamente, con el fin de reparar los daños sufridos por las personas víctimas que se quedaban fuera del ámbito de protección del sistema de responsabilidad subjetiva.

Tomando en cuenta esto, vemos las atractivas vías de acceso para una amplia gama de transacciones desde el celular o computadora, lo que resulta ideal para el consumidor, como, por ejemplo, la Banca por Internet. Aquí, se mueven cantidades considerables de dinero que no resultan seguras a día de hoy, otorgándoles un valor agregado a la Banca Online.

Sin embargo, para acceder a este servicio, se realiza un contrato de adhesión, es decir, sin negociación, regido por las leyes civiles y mercantiles, porque mantiene los mismos principios para su elaboración, validez y eficacia. Esto supone, a la par una desventaja, porque brinda la posibilidad de tomar partido, de forma ilícita de estos instrumentos, como el Pishinig, Pharming, Malware, et, que buscan obtener los datos confidenciales de los clientes.
Se considera el perfil del consumidor de servicios informáticos como una persona deficiente en información y en conocimiento técnico sobre el uso correcto y seguro de las páginas WEB de los bancos, y estos, tampoco brindan de forma correcta la capacitación necesaria para que el cliente interiorice los conceptos básicos y sea consciente de los riesgos.

Por lo que aquí, el criterio de impugnación que establecerá que los Bancos se encuentran obligados a responder civilmente por los daños que lleguen a surgir como el resultado de su actividad, pero esto siempre y cuando se logre demostrar la existencia de un nexo causal entre la conducta y el daño. Por lo que, los Bancos tendrían la posibilidad de demostrar que el daño fue ajeno cuando ellos logren probar que existió algina de las eximentes de culpabilidad que la ley prescribe.

En conclusión, esta teoría respalda que existe una responsabilidad objetiva en el caso de los delitos informáticos afectados en consumidores de entidades bancarias, pero habrá la posibilidad de exonerarse de la responsabilidad cuando se compruebe: la

fuerza mayor, la culpa de la víctima o hecho de un tercero. Por consiguiente, se toma como recomendación que sean revisados los contratos de adhesión elaborados por los bancos para que llegue a eliminarse cualquier cláusula abusiva que perjudique a los consumidores un abuso de poder.

2. TEORIA DEL RIESGO PROVECHO, EL RIESGO CREADO Y EL RIESGO PROFESIONAL

Esta teoría fue desarrollada por Rodríguez Zárate, publicado en el año 2014 en su artículo "Análisis Económico de la Responsabilidad Bancaria frente a los Fraudes

Electrónicos: El Riesgo Provecho, El riesgo Creado y el Riesgo Profesional" donde sostiene:

Recoger la responsabilidad objetiva, subjetiva y las fallas del mercado, porque podemos establecer que no existe claridad en torno a la posibilidad de determinar un régimen de responsabilidad objetiva basándose en la teoría de los riesgos, todo esto bajo el ordenamiento jurídico colombiano.
Es decir, la responsabilidad civil no estipula de una manera expresa ninguna disposición de la que puedan concluirse que al menos en materia bancaria la responsabilidad por fraudes electrónicos es objetiva, por lo que el régimen de responsabilidad objetiva bajo este panorama no resulta ser la solución más eficiente (Rodríguez, 2014).

Aquí es donde se hace necesario una serie de ajustes en el régimen planteado que permitan eliminar los problemas del riesgo moral o las asignaciones de las cargas, porque no resultan viables.

Por lo tanto, el riesgo moral se entenderá como la conducta que genera un impacto en otro agente, que no cuenta con el mecanismo necesario para desarrollar un monitoreo y control sobre la conducta del primero, entonces, bajos las restricciones normativas actuales, la solución más eficiente sería mantener el régimen subjetivo de responsabilidad bajo la culpa presunta, porque distribuye de mejor manera los riesgos.

Finalmente, para esta teoría ante las mencionadas transacciones fraudulentas, órdenes y compras realizadas por tarjetas de crédito la forma de establecer la responsabilidad en estas prácticas será determinándose bajo el régimen subjetivo de responsabilidad contractual de culpa presunta.

3. TEORIA DE LA TUTELA JURÍDICA DEL CONSUMIDOR FRENTE A LA RESPONSABILIDAD CIVIL Y ADMINISTRATIVA DE LOS BANCOS

Esta teoría fue desarrollada por Espinoza Espinoza, en su artículo jurídico titulado "La tutela Jurídica del consumidor frente a la responsabilidad civil y administrativa de los bancos" donde sostiene:

En el Perú, se da en dos niveles, uno administrativo y otro judicial, frente a esta teoría la actividad bancaria ante el consumidor está protegida bajo esos niveles.

Sin embargo, no requiere acudirse la vía administrativa para acudir al Poder Judicial, ya que, cuando sea materia administrativa, tenemos al órgano de la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección a la Propiedad Intelectual, estos tienen competencia primaria para conocer las infracciones a la Ley de Protección al Consumidor.

Entonces, aquí tenemos el primer planteamiento de la teoría, donde el cliente no asume la responsabilidad por el uso irregular o fraudulento que pueda haberse hecho con tarjetas, si éste fue realizado con posterioridad a la comunicación cursada a el Banco, porque en estos casos se encontraría cubierto por el seguro Y mecanismo de cobertura contra fraude implementado por la entidad financiera.

4. TEORIA DE LA CRIMINALIDAD INFORMÁTICA Y EL ABUSO INFORMÁTICO

Esta teoría fue desarrollada por Acuario del Pino (2015) en su libro "Delitos Informáticos: Generalidades" donde sostiene que:

La delincuencia informática como todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos, y como ya se sostenía antes, es necesario llevar a cabo una respuesta rápida y adecuada armonización legislativa para contrarrestar estas prácticas.

Aquí, no solamente están todos los requisitos del delito, sino que el instrumento del crimen es el elemento informático, puede vulnerarse los derechos de un titular de algún elemento informático, hardware o software. Además, se entiende que esta clase de delitos no solo consideran como medio de comisión el elemento informático, sino que también lo informático puede ser el objeto de la infracción.

Entonces, ya se va entendiendo que el delito informático más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con las computadoras, por lo que existe una multiplicidad de conductas ilícitas.

5. TEORIA SOBRE LOS ASPECTOS JURÍDICOS PENALES SOBRE LOS DELITOS INFORMÁTICOS

Esta teoría fue desarrollada por Costa Hoevel, en el año 2006 en su libro titulado "Delitos Informáticos. Aspectos jurídico-penales a la luz de la teoría del delito" donde sostiene que:

Los sistemas informáticos ofrecen nuevas y sumamente complicadas formas de violar la ley, creándose la posibilidad de cometerse delitos tradicionales y no tradicionales, sumándole el hecho de que se reproducen con mayor rapidez que en el mundo real, se debería establecer su configuración específica como delito.

El primer aspecto del delito informático, sería de analizar la conducta desde la óptica de la informática, es decir, se requiere un análisis interdisciplinado. Para poder comprender conceptos, y establecer entonces los parámetros y posteriores tipificaciones de conductas ilícitas, se debe recurrir como auxilio a los conocimientos que solo brinda la ciencia informática.

El segundo aspecto jurídico, sería que el bien jurídico a tutelar podría variar de un instante a otro, porque existe un sin número de conductas que son imposibles de enumerar de forma taxativa debido a su constante aumento y evolución en sus formas de operación. (Costa, 2006)

Aquí, a diferencia de la teoría anterior, se hace una diferenciación sobre la conceptualización de los delitos informáticos, ya que se excluyen algunos elementos informáticos cuando son involucrados, por no ser estrictamente elementos informáticos. Por ejemplo, el contrabando de hardware o software porque son objetos de ilícitos como cualquier otro objeto material, por ser bienes muebles que pueden ser pasibles en robos, hurtos, daños, etc.

1.7. Definición de Términos Básicos Delito

informático

la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (Davara Rodríguez, 1995)

Transacciones fraudulentas

Son órdenes y compras realizadas con tarjetas de crédito y cuentas bancarias que no pertenecen al comprador

Derecho patrimonial

Se considera parte de una de las ramas que comprende el derecho de autor y propiedad intelectual, puesto que, permite al autor obtener una retribución económica por el uso de su obra por parte de terceros, por lo que les otorga el derecho a impedir que estos terceros la utilicen en contra de su voluntad o sin su autorización.

1.8. Hipótesis:

1.8.1. Planteamiento de la hipótesis:

La manera en que las transacciones fraudulentas y los delitos informáticos afectan el derecho de propiedad y el derecho patrimonial en soportes virtuales son: la asimetría informativa al contratar, el aprovechamiento delictivo producto de la facilidad y la desprotección en la industria lícita, las medidas de seguridad ineficientes para la protección de los derechos de autor, y la falta de una determinación clara en la responsabilidad contractual haciendo difícil el comercio.

1.8.2. Variables:

1.8.2.1. Variable independiente:

Transacciones fraudulentas

1.8.2.2. Variable dependiente:

Delitos informáticos

II. MATERIALES Y MÉTODOS

2.1. Materiales

DESCRIPCIÓN	UNIDAD	CANTIDAD
Papel bond A4/75g	Millar	3
Lapicero	Unid.	2
Memoria – USB	Unid.	2
Lápiz	Unid.	10
Borrador	Unid.	10
Tajador	Unid.	2
Corrector	Unid.	5
Regla	Unid.	2
Engrapador	Unid.	1
Perforador	Unid.	1
Folder Manilla A4	Unid.	25

Clips x 200 unidades	Ciento	2
Grapas Estándar 26/6	Millar	1
CD’s	Unid.	10
Computadora y equipos periféricos	Unid.	1
Fotocopias	Millar	5
Impresión	Millar	2
Internet	Mes	4
Empastado	Unid.	2

2.2. Material de estudio

2.2.1. Población

Según la plataforma INE (s/f) define a la población como el conjunto de personas que habitan una determinada área geográfica.

En estadística, según la plataforma de Educación Recursostic (s/f) la define como un conjunto de todos los elementos que verifican una característica que será objeto de estudio.

En esta presente tesis, la población está comprendida por los siguientes profesionales: Abogados defensores.

2.2.1.1.Muestra

Según Lalangui (2017) precisa que la muestra es la parte de la población que se selecciona para la obtención de la información. En ella se realizará las mediciones u observaciones de las variables de estudio. En la presente tesis, la muestra está conformada por lo siguiente:

TECNICAS	**UNIDAD**	**S.S**	**POBLACIÓN**	**MUESTRA**
Encuesta	Abogados	10	10	10
		TOTAL	**10**	**10**

2.3. Técnicas, procedimientos e instrumentos.

2.3.1. Para recolectar datos

Tabla N°01

Técnicas e instrumentos del Análisis documental

Técnicas	Instrumentos
Análisis documental	Fichas de análisis del marco teórico, de la legislación, doctrina y jurisprudencia

Fuente: Investigación propia

Elaborado por: NOMBRE DE ALUMNO. (2021).

Tabla N°02

Técnicas e instrumentos de Observación

Técnicas	Instrumentos
Entrevistas	Guía de entrevista. Elaborado en base a un conjunto de preguntas y se aplica a abogados defensores.

Fuente: Investigación propia

Elaborado por: NOMBRE DE ALUMNO (2021)

2.3.2. Para procesar datos

Siendo la finalidad realizar el análisis de la información obtenida, se realizó un estudio inicial de las respuestas obtenidas por los profesionales involucrados, a fin

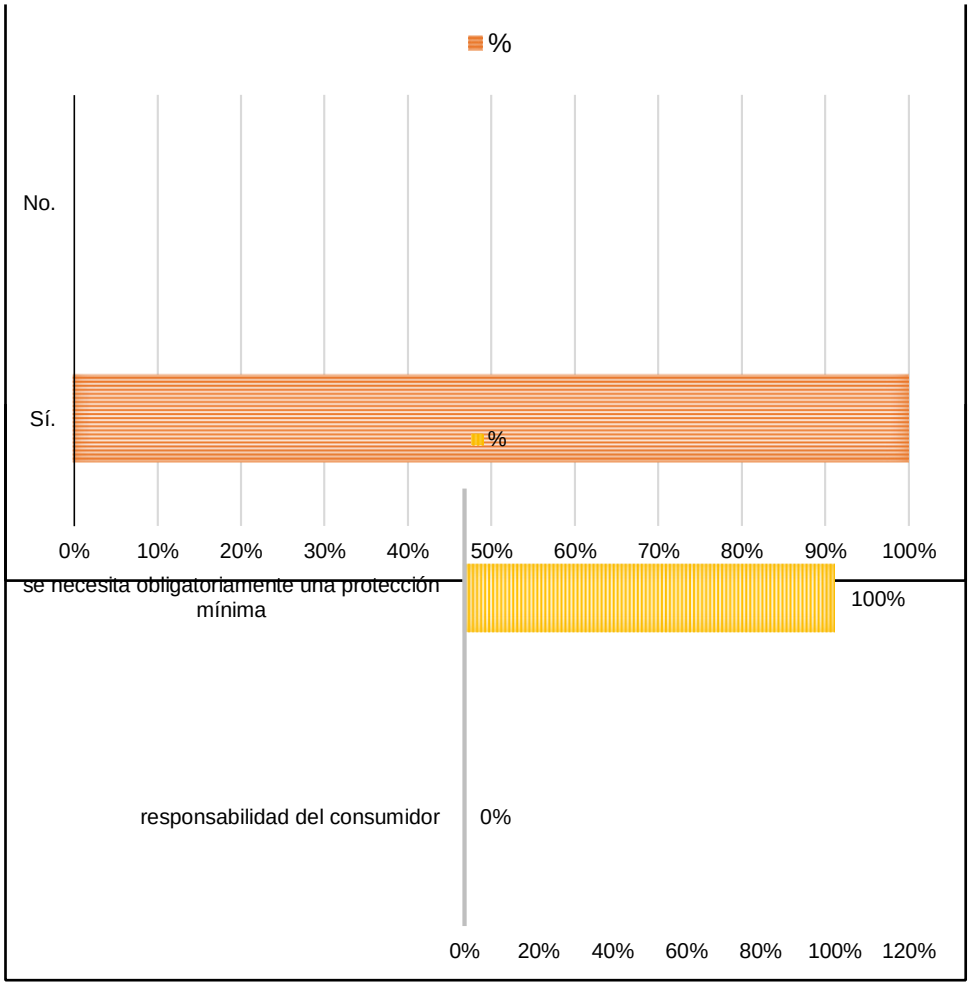
de poder determinar las definiciones más pertinentes y significativas, respecto al clima organizacional, de acuerdo a las categorías señaladas.

III. RESULTADOS

En el siguiente acápite se realizó una entrevista a 10 abogados especializados en Derecho Penal, cuya experiencia se encuentra basada en Delitos Informáticos, de conformidad con las variables de estudio y los objetivos específicos de la investigación. Es por ello, que después de haber realizado las entrevistas, se obtuvo los siguientes resultados:

Análisis de la entrevista practicada.

¿Considera que existen modalidades en las que se puede considerar "fraudulento la pérdida de un bien, límites y excepciones?

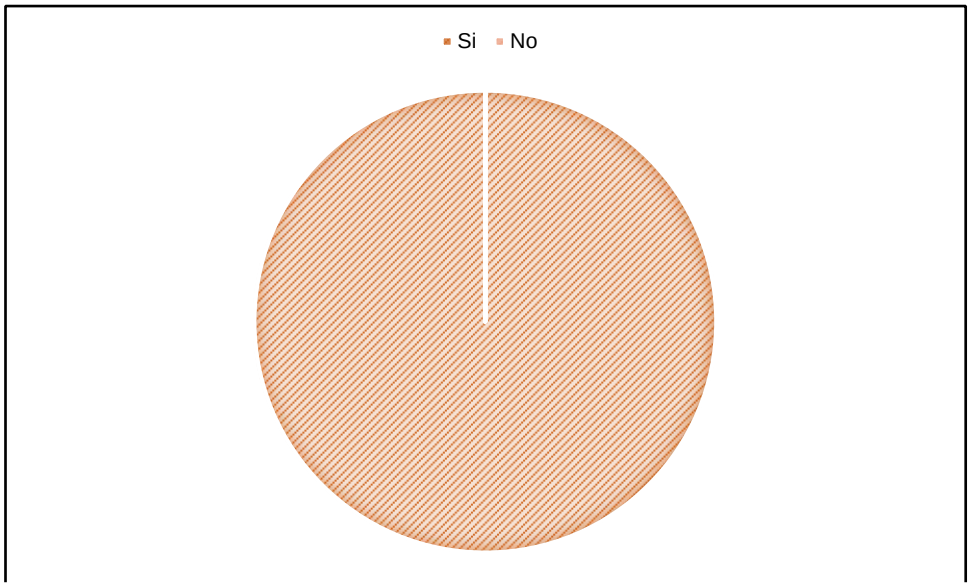


Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que existen modalidades en las que se puede considerar "fraudulento la pérdida de un bien, límites y excepciones".

¿Es responsabilidad del consumidor tener una cultura informada en cuanto a cómo gestiona sus gastos y donde decide comprar, o se necesita obligatoriamente una protección mínima en estos medios?

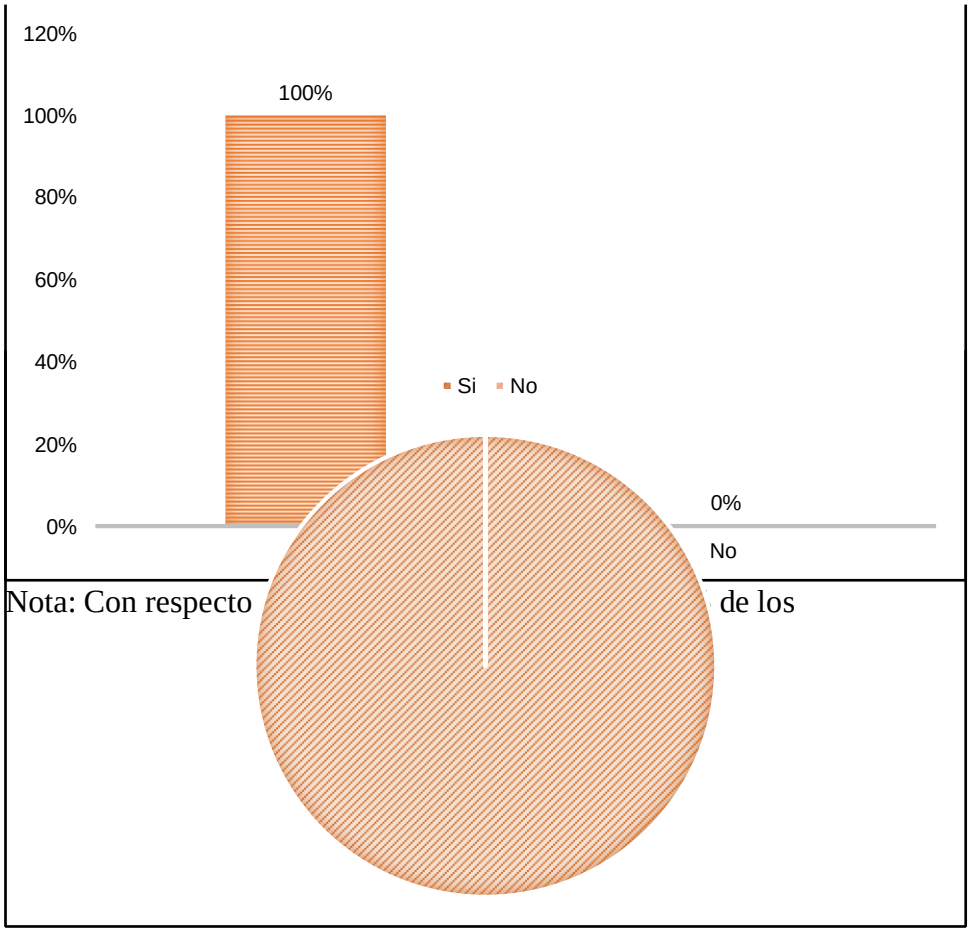
Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron como alternativa correcta que se necesita obligatoriamente una protección mínima para que tenga una cultura informada en cuanto a cómo gestiona sus gastos y donde decide comprar, dejando de lado así la alternativa siguiente.

¿Se debe contrarresta un delito informático si cada vez se hace más evidente la "guerra de la tecnología" desde un punto de vista jurídico?



Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que se debe contrarresta un delito informático si cada vez se hace más evidente la "guerra de la tecnología" desde un punto de vista jurídico.

¿Se necesita una interpretación diferente en cuanto a la comisión de estos delitos?



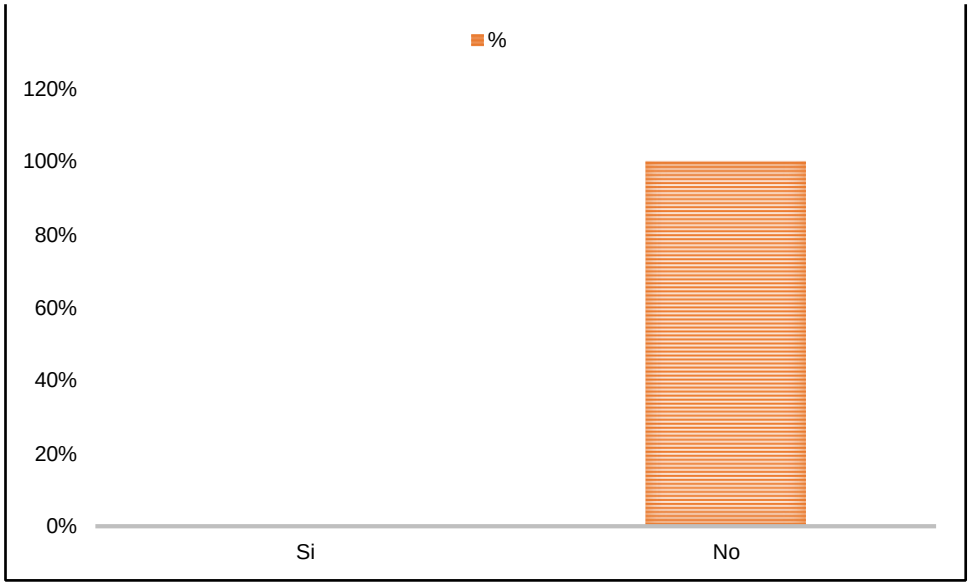
Nota: Con respecto de los entrevistados consideraron que si se necesita una interpretación diferente en cuanto a la comisión de estos delitos informáticos que vulneran el derecho patrimonial de los consumidores.

Si son los bancos, las entidades y los prestadores de servicio quienes tienen la información de sus limitaciones al momento de brindar su servicio, ¿deben poner esta información al público?

Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que los bancos, las entidades y los prestadores de servicio deben poner esta información al público al momento de brindar su servicio.

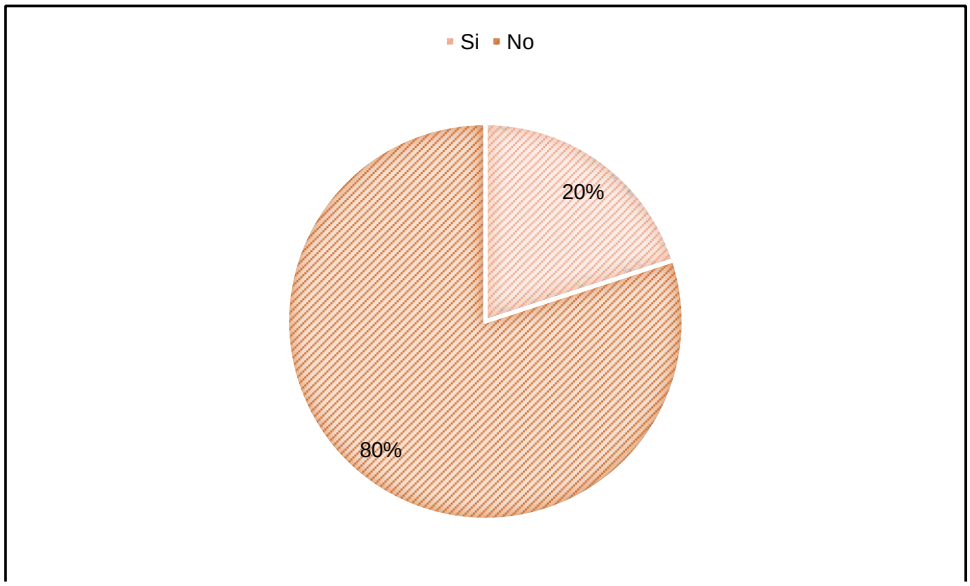
¿Es posible que se haga la libre la información de las empresas dando más

“tranquilidad” a los consumidores, no afectando los derechos de autor y la gestión empresarial para poder subsistir?



Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que no es posible que se haga la libre la información de las empresas dando más “tranquilidad” a los consumidores, puesto que esto afecta los derechos de autor y la gestión empresarial para poder subsistir.

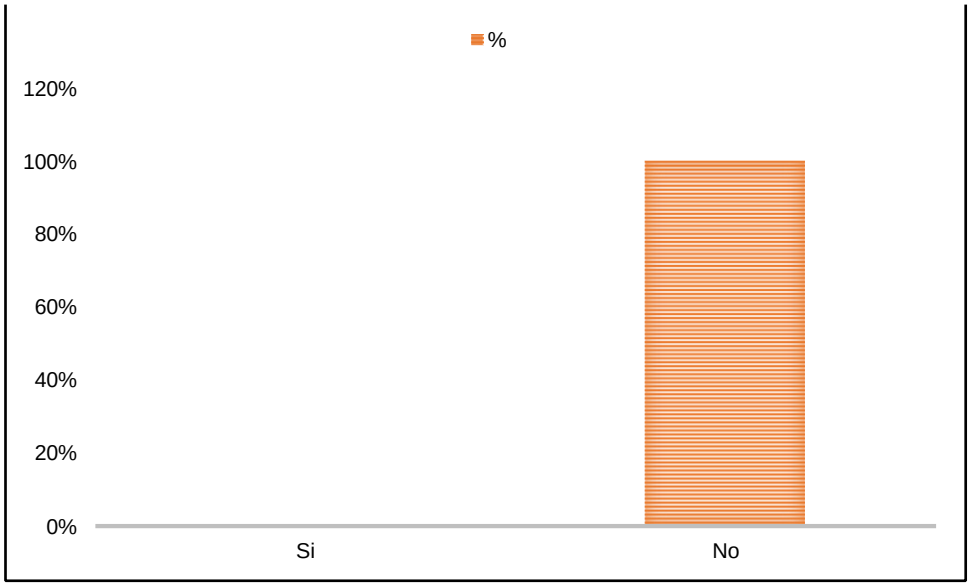
¿Existe los modelos jurídicos contractuales pertinentes y adecuados, para que una persona al realizar una compra-venta por internet?



Nota: Con respecto a los resultados obtenidos, el 80% de los entrevistados consideraron que no existen modelos jurídicos contractuales pertinentes y adecuados, para que una persona al realizar una compra-venta por internet; sin embargo, el 20% de los entrevistados, si consideran que existen modelos jurídicos contractuales pertinentes y adecuados, para que una persona al realizar una compraventa por internet.

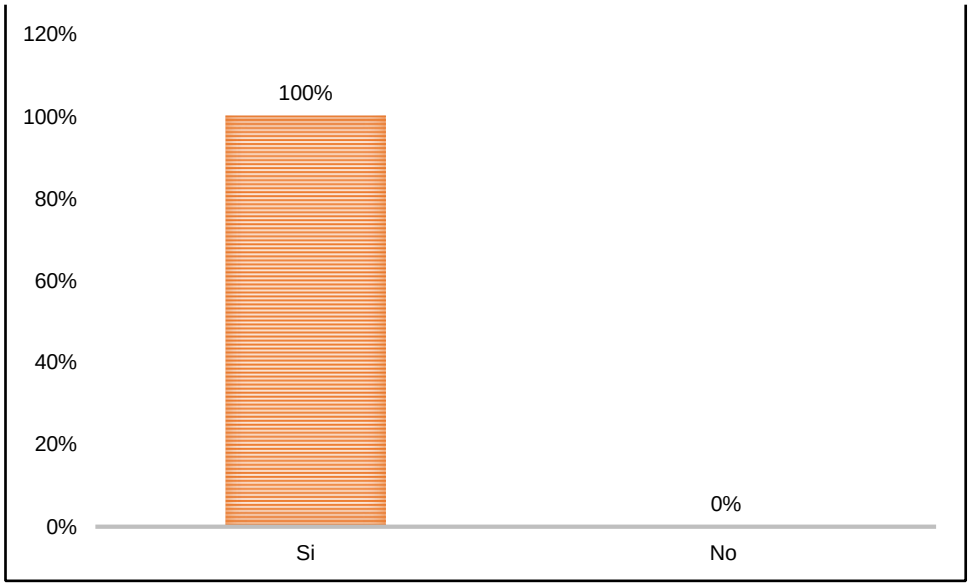
Los delitos informáticos pueden afectar a una empresa al punto de su quiebre. ¿Existen acciones legales que puede tomar la empresa?

Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que no existen acciones legales que puede



tomar la empresa, en los casos que se cometan delitos informáticos que puedan afectarla al punto de su quiebre.

¿El estado debería financiar implementaciones y estándares de seguridad en las empresas que sean susceptibles o blanco de mira para los delitos informáticos?



Nota: Con respecto a los resultados obtenidos, el 100% de los entrevistados consideraron que el estado debería financiar implementaciones y estándares de seguridad en las empresas que sean susceptibles o blanco de mira para los delitos informáticos.

IV. DISCUSION

Con respecto al resultado N° 01, se evidenció que, los abogados especializados en Derecho Penal, opinaban que las transacciones fraudulentas y los delitos informáticos afectan el derecho de contratar. Esto se relaciona con lo establecido por Daniela Salas (2010) en su tesis titulada "Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos", en la cual sostiene que:

Se desarrollan así una serie de delitos informáticos a través de los cuales los delincuentes cibernéticos pretenden obtener un beneficio patrimonial ilegítimo, defraudando al consumidor de servicios bancarios por Internet. Los más comunes, por su nivel de afectación al cliente, han sido el Pishing, el Pharming, el Malware, los Keyloggers y los Troyanos o Caballos de Troya, entre otros.

En cuanto al resultado N° 02, se verificó que, los abogados especializados en Derecho Penal, consideraban que las transacciones fraudulentas y los delitos informáticos afectan el derecho de ejercer toda industria lícita. Esto concuerda con lo señalado por Winnie Balcázar (2017) en su tesis titulada "Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito", en donde concluye que:

Asimismo, los principales mecanismos de seguridad en las tarjetas de crédito y tarjetas de débito son las claves secretas; con la que se obtiene total acceso, permitiendo el uso de las mismas; en esta línea, el INDECOPI, al requerir la información de todos los documentos de las transacciones realizadas por el supuesto "titular"; la entidad bancaria o financiera, entrega los reportes Tándem y Journals correspondientes a las operaciones generadas; sin embargo, esta información solo indicará que las operaciones se realizaron de manera habitual porque se digitó la clave secreta correctamente; la misma que, ya no es suficiente para verificar si se trata de operación veraz o de una operación no reconocida.

Referente al resultado N° 03, se evidenció que, los abogados especializados en Derecho Penal, opinaban que las transacciones fraudulentas y los delitos informáticos afectan el derecho de comerciar. Esto se asemeja con lo mencionado

por José Rendón (2007) en su trabajo de grado titulado "Responsabilidad Civil Contractual por fraudes con tarjeta de crédito en Colombia", en donde concluye:

Para que el sistema pueda enfrentar los riesgos por fraude es necesario que las partes cooperen en el desarrollo de la actividad y para que la tarjeta de crédito pueda cumplir su finalidad. Como derivados del principio de cooperación surgen para cada participante, la obligación de desplegar unas conductas de prevención de fraudes".

Finalmente, con respecto al resultado N° 04, los abogados especializados en Derecho Penal, consideraron que las transacciones fraudulentas y los delitos informáticos afectan los derechos de autor en soportes virtuales. Esto concuerda con lo establecido por Daniela Salas (2010) en su tesis titulada "Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos", en la cual sostiene que:

Se desarrollan así una serie de delitos informáticos a través de los cuales los delincuentes cibernéticos pretenden obtener un beneficio patrimonial ilegítimo, defraudando al consumidor de servicios bancarios por Internet. Los más comunes, por su nivel de afectación al cliente, han sido el Pishing, el Pharming, el Malware, los Keyloggers y los Troyanos o Caballos de Troya, entre otros.

V. CONCLUSIONES

- Concluido el trabajo de investigación, es menester señalar que, se confirma la hipótesis propuesta, la manera en que las transacciones fraudulentas y los delitos informáticos afectan el derecho de propiedad y el derecho patrimonial en soportes virtuales, en el departamento de La Libertad en el periodo de 2019-2020 son: la asimetría informativa al contratar, el aprovechamiento delictivo producto de la facilidad y la desprotección en la industria lícita, las medidas de seguridad ineficientes para la protección de los derechos de autor, y la falta de una determinación clara en la responsabilidad contractual haciendo difícil el comercio.

- Asimismo, se concluye que la forma en que las transacciones fraudulentas y los delitos informáticos afectan el derecho de contratar, es que actualmente, todas las personas realizan contratos virtuales, lo que genera que sea muy fácil realizar un fraude o algún delito informático, por lo que se necesita una mayor protección legal para esos casos, lo cual se podría reducir si en los contratos de compraventa virtual se coloquen clausulas informando a los consumidores de los riesgos de contratas por internet.

- De la misma manera, se concluye que la forma en que las transacciones fraudulentas y los delitos informáticos afectan el derecho de ejercer toda industria lícita, puesto que existe un enriquecimiento ilícito y pirata de parte de los consumidores, lo que genera que las empresas no puedan llegar a masificarse o a extenderse o tener mayores ingresos; entonces cuando existe esa facilidad de trasgredir la actuación de las empresas, es que estas suelen tener cláusulas abusivas con sus consumidores, logrando ejercer la ilicitud.

- De la misma forma, se concluye que la manera en que las transacciones fraudulentas y los delitos informáticos afectan el derecho de comerciar, pues los consumidores realizan un método evasivo de pagos, generando que se vea vulnerado la retribución que tienen los dueños del contenido, puesto que

los consumidores no pagan, pues realizan transacciones fraudulentas para obtenerlos.

- Finalmente, se concluye que la manera en que las transacciones fraudulentas y los delitos informáticos afectan los derechos de autor en soportes virtuales, es porque la herramienta virtual del internet brinda a los consumidores la obtención de contenido gratuito de los cuales se han creado o se han destinado para tener un enriquecimiento hacia las empresas que son dueños de ese contenido por los derechos de autor que los protege, siendo así que de esa manera es que se transgrede los derechos de autor de las empresas en los soportes virtuales.

VI. REFERENCIAS BIBLIOGRAFICAS

- Opinión Consultiva No. 01-2018-JUS/DGTAIPD (2018). Lima. https://www.minjus.gob.pe/wp-content/uploads/2018/10/O-C01_OCTUBRE.pdf
- Santiago Acuario del Pino (2015) Derecho Penal Informático. Ecuador https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Balcazar, W. (2017) ¿Cómo educar al consumidor financiero y no morir en el intento? http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/13087
- Sobre la tutela jurídica del consumidor frente a la responsabilidad civil y administrativa de los bancos. http://repositorio.pucp.edu.pe/index/handle/123456789/108032
- Sobre el bien jurídico protegido en los delitos informáticos, https://scielo.conicyt.cl/pdf/rchilder/v44n1/art11.pdf
- Sobre la Responsabilidad Contractual por fraudes con tarjeta de crédito en Colombia: https://repository.eafit.edu.co/bitstream/handle/10784/457/JoseSantiago_RendonVera_2007.pdf;jsessionid=3789A5F45FA7BF91 EDCF940A18EE 52 08?sequence=1
- Sobre los Delitos Informáticos en general: http://www.hfernandezdelpech.com.ar/14)-PP%20Informatico%20(9a_parte)%20Delitos%20Informaticos.pdf
- Sobre el estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación. https://es.scribd.com/document/180922473/Meza-Alayo-PaolaConsumidor-Clonacion
- Sobre el Delito informático y su problemática en la cooperación internacional. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321
- Sobre la Estafa Informática del Artículo 248.2 del Código Penal. https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y

- Sobre la teoría de delitos informáticos. http://www.justiniano.com/revista_doctrina/delitoinformatico.htm