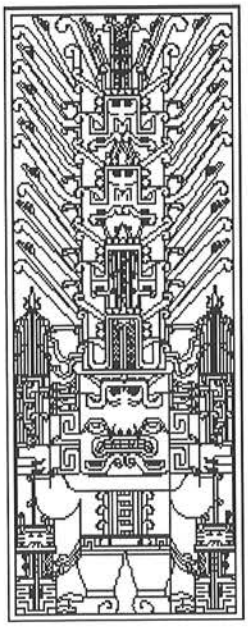
UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

ESCUELA UNIVERSITARIA DE POSGRADO



TESIS

"EL DELITO INFORMATICO Y SU INCIDENCIA EN LA EMPRESA BANCARIA"

PRESENTADO POR:

Abog. BLOSSIERS MAZZINI, JUAN JOSÉ

PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN DERECHO EMPRESARIAL

LIMA - PERÚ

2018

Dedicatoria

A las cualidades de mis padres,

Al Abogado y Catedrático Juan José Blossiers

Y la Profesora de Historia Carmela Mazzini

Por ser como son,

Sin lo cual yo no sería lo que soy.

Agradecimiento

Agradezco a Sylvia mi querida esposa, por su cariño y amor constante su invaluable colaboración, sin los cuales no hubiera sido posible este trabajo de investigación

ÍNDICE

RESUMEN

El presente trabajo de investigación, trata sobre los delitos cibernéticos y su impacto en las empresas bancarias, para lo cual debemos incidir, que con el pasar de los años las tecnologías informativas se han ido desarrollando a manera que se crea una nueva fuente de delitos, la criminalidad cibernética, para lo cual es necesario la tutela de parte del estado, y criminalizar o tipificar esta nueva modalidad de delincuencia.

En ese sentido, es que se hace una descripción de la realidad problemática, y consecuencia de ello se formula en forma de interrogante los problemas generales y específicos; partiendo de estas interrogantes, es que se determinan los objetivos, por los cuales se guiara la investigación.

El marco teórico, parte con los referentes de los delitos informáticos, y los derechos a la intimidad que se pueden afectar, así como otros temas de mayor interés, conforme al problema, haciendo uso de información física como virtual, que coadyuven a nuestra investigación.

Asimismo se hizo uso de la más adecuada metodología de investigación, que ayude no solo a describir el problema, sino que también describa de manera coherente la información analizada. En ese sentido es que también se realiza en análisis de las encuestas, en la que se idearon cuadros informativos y gráficos en forma de tablas; que ayudan a demostrar gráficamente la información obtenida.

La investigación finaliza, con las conclusiones y recomendaciones.

ABSTRACT

This research work deals with cybercrimes and their impact on banking companies, for which we must emphasize that over the years information technologies have been developed in a way that creates a new source of crime, the cybernetic crime, for which it is necessary the protection of part of the state, and to criminalize or typify this new modality of delinquency.

In that sense, it is that a description of the problematic reality is made, and as a consequence the general and specific problems are formulated in a questioning way; starting from these questions, is that the objectives are determined, by which the investigation will be guided.

The theoretical framework, part with the referents of computer crimes, and the rights to privacy that can be affected, as well as other topics of greater interest, according to the problem, making use of physical information as virtual, that contribute to our research.

Likewise, the most appropriate research methodology was used, which helps not only to describe the problem, but also to describe in a coherent manner the information analyzed. In this sense, it is also carried out in the analysis of the surveys, in which informative tables and graphs were created in the form of tables; that help to graphically demonstrate the information obtained.

The investigation ends, with the conclusions and recommendations.

INTRODUCCIÓN

En nuestro país, con el pasar del tiempo se han ido emitiendo leyes, que tiene como finalidad prevenir las conductas ilícitas, así como sancionarlas, de ello no se ha escapado el cibercrimen, o delitos informáticos, que tiene como supuesto afectar sistemas y base de datos virtuales, que afecten bienes jurídicos, tales como el patrimonio, la libertad sexual y la fe pública.

En caso de las empresas bancarias, o entidades financieras, se ven afectas por el cibercrimen, cuando personas ajenas a las empresas bancarias, con la finalidad de obtener beneficios propios o para terceros, de manera ilegal infringe los sistemas de seguridad virtuales, para recabar información secreta, clonar tarjetas, o asumir identidades que no les pertenecen, y ocasionan daños al patrimonio propio de la empresa bancaria o a sus clientes.

Si bien es cierto la globalización ha traído consigo la modernización de diferentes sistemas públicos y privados, siendo uno de esos, de los que se generan las operaciones financieras en segundos o minutos, situaciones que hace años no se hubieran imaginado; realizándose operaciones desde diferentes partes del mundo, desde un solo lugar, dejándose así de lado las fronteras, y asumiéndose el papel propio de la globalización.

Es así, que los robos a los bancos se han dejado de lado, pues ya no es necesario ingresar a un a punta de armas, sino que ahora se utilizan mecanismos electrónicos que no ponen en riesgo, ni la vida, ni la libertad y mucho menos la identidad de quien ejerce el delito.

En general, se tratara de desarrollar, temas como ¿Qué son los delitos informáticos? ¿Cuáles son las características de los delitos informáticos?, asimismo se buscara desarrollar, temas relacionados a la intimidad, y como se ven afectos con la comisión de los delitos informáticos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Antecedentes

Luego de realizar una búsqueda en los repositorios de diferentes universidades de la capital, así como de universidades de provincias, sean nacionales o privadas, hemos podido encontrar los siguientes antecedentes, que nos darán una idea de lo que buscamos en el desarrollado de la tesis y su problemática.

VEGA AGUILAR J. A. (2010) quien presento la tesis titulada "LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL" ante la Universidad Católica de Santa María, con la finalidad de optar el grado académico de Maestro en Derecho Penal; el autor del trabajo mencionado, pudo concretar las siguientes conclusiones relacionadas a nuestro tema:

- El avance científico y tecnológico han acarreado aspectos positivos e importantes en nuestra sociedad en los últimos tiempos, motivo por el cual la interpretación tradicional de los delitos en nuestro código penal

han quedado desfasados ante la aparición de estos delitos de nueva data como es la criminalidad informática.

- Actualmente no existe una definición unánime de los "Delitos Informáticos", por parte de los juristas nacionales y extranjeros, motivo por el cual a nuestro parecer la denominación más apropiada a estos delitos de nueva data es la de "Criminalidad Informática", debido a que estos ilícitos son una nueva forma de criminalidad.
- Que, estos delitos de nueva data son delitos pluriofensivos, debido a que afectan a más de un bien jurídico protegido, con son el patrimonio, el honor, la intimidad, el pudor, el orden económico, la libertad informática, la vida el cuerpo entre otros, los cuales afectan gravemente el normal desenvolvimiento y desarrollo de nuestra sociedad.
- Nos parece poco acertada la inclusión de los "Delitos Informáticos" como un Capítulo dentro del Título de los Delitos Contra el Patrimonio en nuestro Código Penal, lo cual permite colegir que solo existen Delitos Informáticos Contra el Patrimonio, no ajustándose a la realidad, debido a que la gama esta nueva forma de criminalidad afecta a diversos bienes jurídicos protegidos como el patrimonio, el honor, la intimidad, el pudor, la libertad Informática, la vida el cuerpo y la salud, etc.
- La naturaleza virtual e intangible de esta nueva forma de criminalidad, origina confusión al momento efectuarse su tipificación, al realizar las investigaciones por parte de la Policía Nacional; asimismo en la actualidad los jueces y fiscales, cuentan con poco conocimiento y

experiencia en el manejo de esta área del Derecho Informático con la finalidad de enfrentar a esta nueva forma de criminalidad.

- Finalmente hemos podido apreciar que en la actualidad son escasos los procesos penales relacionados con los delitos informáticos, los mismos que se encuentran tipificados en nuestro Código Penal vigente en los artículos 207º "A", 207º "B" y 207º "C" los cuales fueron incorporados en nuestro Código Penal vigente mediante Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000, motivo por el cual cabría la derogatoria de los artículos antes mencionados y que se efectúe un estudio minucioso de los tipos penales que pueden ser realizados por medios informáticos del Código Penal vigente, los cuales deben ser agravados debido al impacto que ocasiona en nuestra sociedad.

TENORIO ROJAS J. y TUESTA GÓMEZ M. (2012), quienes presentaron la tesis titulada "LEGISLACIÓN DEL SECRETO BANCARIO Y SU RELACIÓN CON EL DELITO DE HURTO INFORMÁTICO DE DINERO MEDIANTE LA VIOLACIÓN DE CLAVES SECRETAS, IQUITOS- 2010", ante la Universidad Nacional de la Amazonia Peruana, con la finalidad de que cada uno opte el grado académico de Maestro en Derecho y Ciencias Penales. Del trabajo mencionado, se pudieron extraer las siguientes conclusiones:

- La legislación del secreto bancario en el Perú, no está acorde con el avance tecnológico y el incremento de la criminalidad cibernética, porque la Ley 26702 - Ley General del Sistema Financiero, del Sistema

de Seguros y Orgánica de la Superintendencia de Banca y Seguros, que lo regula, es una ley que tiene más de una década y en ese tiempo la tecnología y la informática han avanzado mucho y la delincuencia cibernética también.

- El secreto bancario representa un obstáculo en la investigación del delito de hurto de dinero, mediante la violación de claves secretas, porque solo se levanta a petición de los jueces y tribunales en un proceso concreto, en el cual sea parte el cliente de la empresa financiera, más no lo puede solicitar el Fiscal Provincial.
- El secreto bancario ha influido en la impunidad de los autores de hurto de dinero, mediante la violación de claves secretas en !quitos, durante el año 201 O, porque de la investigación se ha determinado que las personas afectadas al no conocer el nombre de los presuntos autores no denunciaron a la Policía o Fiscalía, sino recurrieron mayoritariamente a Indecopi, interesados en recuperar el dinero hurtado; asimismo en ninguna Comisaría de !quitos se presentó denuncia por este tipo de delito y, los bancos informan que no presentan denuncia ante la policía o fiscalía, lo cual genera impunidad porque los autores quedan en el anonimato.
- Los Bancos, Abogados, la Policía Nacional e Indecopi, no tienen información estadística que registre los casos de hurto de dinero de las cuentas de los clientes de las entidades financieras, en la modalidad de violación de claves secretas, que contribuya en la investigación y al mejoramiento de la seguridad de las transacciones financieras.

- El secreto bancario contribuye en el incremento del delito de hurto de dinero, mediante la violación de claves secretas, debido a que las entidades financieras amparadas en esta institución no brindan la información al Fiscal Provincial, para que identifique a los presuntos autores y proceda con la investigación de este delito.

1.2. Descripción y formulación del problema

1.2.1. Descripción del Problema

Los bancos son las víctimas predilectas de los delincuentes informáticos, sobre todo por el desarrollo de la banca electrónica-empresarial a nivel internacional. En el ámbito nacional se observa que el progreso de esta modalidad de banca es paulatino, debido entre otros factores a la desconfianza del público y el bajo nivel de bancarización. Desde hace varios años, los bancos peruanos ofrecen transacciones por Internet, motivados básicamente por ser operaciones más sofisticadas lo cual los hacen más competitivos, beneficiando al cliente y a la institución financiera. De este modo, las operaciones son más económicas en Internet que por ventanilla, el horario de atención pasa de seis horas diarias, de acuerdo a la Ley General del Sistema Financiero y de Seguros, a 24 horas durante los 365 días del año, ahorrando considerablemente tiempo y dinero, brindando comodidad a sus clientes, quienes pueden realizar operaciones desde su casa u oficina. (BLOSSIERS MAZZINI, 2008, pag. 39)

Sin embargo todo esta sofisticación que nos traen las nuevas tecnologías de información son empañadas por los delitos informáticos que pese a estar legislados en nuestro texto punitivo en sus artículos 207-A, 207-B Y 207-C, aún la criminalidad informática sigue socavando el sistema financiero lo que ha motivado que la Empresa Bancaria, ponga a la palestra la situación de la seguridad informática para contrarrestar el avance de este tipo de delincuencia del siglo XXI. He allí, el problema central de nuestra investigación.

1.2.2. formulación del Problema

Problema General

- ¿Cuál es el impacto de los delitos informáticos en la Empresa Bancaria?

Problemas Específicos

- ¿En qué medida se encuentran tipificados los delitos informáticos, que afecten directamente a las Empresas Bancarias?

- ¿Existe una clasificación adecuada de los delitos informáticos que afecten a las empresas Bancarias?

- ¿De qué manera la Empresa Bancaria es blanco de los delincuentes informáticos?

1.3. Objetivos

1.3.1 Objetivo General

- Determinar cuál es el impacto de los delitos informáticos en la Empresa Bancaria.

1.3.2 Objetivos Específicos

- Evaluar en qué medida se encuentran tipificados los delitos informáticos, que afecten directamente a las Empresas Bancarias.

- Evaluar si existe una clasificación adecuada de los delitos informáticos que afecten a las empresas Bancarias.

- Determinar de qué manera la Empresa Bancaria es blanco de los delincuentes informáticos.

1.4. Justificación e importancia

1.4.1. Justificación

La elaboración del presente estudio, concedería a la Dirección de delitos de Alta Tecnología de la Policía Nacional del Perú, Superintendencia de Banca y Seguros y Órganos Jurisdiccionales encargados de velar por los derechos esenciales de los clientes del sistema financiero a poseer un documento idóneo que les permita vislumbrar cual es la verdadera dimensión de los Delito Informático y su incidencia en la Empresa Bancaria.

1.4.2. Importancia

a) Carácter Técnico

Nuestro plan de Tesis, pretende colaborar de modo efectivo al discernimiento de la necesidad ineludible de establecer una nueva tipología de delitos informáticos que amenazan y sucumben actualmente al sistema financiero, llamando la atención a las autoridades administrativas de control y jurisdiccionales y por supuesto a la sociedad civil que reclama protección informática en la realización de sus transacciones en la Empresa Bancaria.

b) Carácter legal

El referido estudio se sustenta reglamentariamente, porque se desarrolla en observancia de las disposiciones académicas vigentes y requeridas por la Escuela Universitaria de Post Grado de la Universidad Nacional Federico Villarreal, en el marco de las obligaciones imperativas para obtener el Grado académico de Maestro en Derecho Empresarial.

c) Carácter practico

El uso aplicativo del reseñado estudio por parte de los órganos administrativos de control, jurisdiccionales y de la sociedad civil, conlleva asentar nuestra investigación, motivando la atención de quienes tienen la toma de decisiones en la elaboración de un política empresarial que observe nuestro circunspecto trabajo de exploración en aras de encontrar un mejor tratamiento del Delito Informático y su incidencia en la Empresa Bancaria.

1.5. Limitaciones de la investigación

Es preciso indicar, que no se tuvieron inconvenientes al momento de realizar el desarrollo de la investigación, puesto que la información que se requería fue de fácil accesibilidad; asimismo es posible indicar la accesibilidad que mostraron los encuestados, siempre que se guarde en secreto la identidad de los mismos.

CAPÍTULO II

MARCO TEÓRICO

2.1 Bases teóricas

Dado que la mirada central del presente trabajo de investigación estará puesta en el recurso de casación, será necesario plantear algunos parámetros que sirvan de ejes conceptuales. Para empezar, se brindarán antecedentes para luego desarrollar el tema en virtud a la problemática planteada.

Las bases teóricas relacionadas con las variables de la investigación que se presentan son las columnas vertebrales de la investigación, las mismas que merecen ser presentadas desde la óptica de varios autores que se citaran a continuación.

2.1.1. El Delito Informático

El derecho y la sociedad siempre están en constante van cambio, por lo que es el Derecho quien se adecúa a todo lo que la necesidad necesita. Se puede señalar que los principales cambios se han dado por el progreso o la constante actualización de la tecnología y en particular a todo lo concerniente a la tecnología informática, la misma que está presente en diferentes aspectos de la vida social.

Por lo mismo, es que van surgiendo una serie de comportamientos ilícitos denominados de manera genérica "delitos informáticos", en cual el sujeto activo mediante acciones dolosas provoca afectación a otro sujeto pasivo dañando y vulnerando su privacidad, intimidad, y el patrimonio. En esta oportunidad abarcaremos el tema de los Delitos Informáticos, y para ello es necesario saber que la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales, los cuales deben contar con la capacidad de cumplir tres tareas básicas: entrada (captación de la información), procesamiento y salida (transmisión de los resultados). El conjunto de estas tres tareas se conoce como algoritmo. (Fernández Villegas, Vivanco Quinto, & Vara Morocco, 2018)

Teniendo en cuenta la Teoría del Delito, se podría definir a los Delitos Informáticos como toda acción ilícita que se realice en un entorno informático, la cual se encuentra sancionada con una pena. Para el tratadista en Derecho Penal, de nacionalidad italiana, Carlos Sarzana, están referidos a "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

2.1.1.1. Código Penal Peruano- Delitos Informáticos

En nuestro Código Penal, en su artículo 207-A, define a los delitos informáticos como el que utiliza o ingresa indebidamente a una base de datos, sistema p red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con

prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas. [1]

Tenemos como ejemplo que se desprende de esta premisa, a aquellos fraudes que se cometieron en perjuicio de las instituciones bancarias o de cualquier empresa por personal del área de sistemas que tienen acceso a los tipos de registros y programas utilizados. También se encuadra el fraude efectuado por manipulación informática, es decir, cuando se accede a los programas establecidos en un sistema de información y se les manipula para obtener una ganancia monetaria. (Fernández Villegas , Vivanco Quinto , & Vara Morocco , 2018)

Tenemos también a la falsificación informática, la misma que se configura con la operación de aquellos datos que específicamente son confidenciales por la importancia que tienen, como la repetición de programas que ameritan ser guardados bajo seguridad absoluta, por el derecho que tienen sus propios autores, acreditada como piratería,

Así mismo, su artículo 207-B, hace referencia a la alteración, daño, y destrucción de datos, sistema, red o programa de computadoras, donde se señala que aquel que maneja, integra, ilegalmente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de

[1] Código Penal Peruano de 1991

libertad no menor de tres ni mayor de cinco años y con setenta a noventa días de multa.[2]

En este caso, podemos señalar que este artículo hace referencia al manejo o al hecho de integrar de manera ilícita determinados datos que más adelante serán dañados o de alguna manera tratar de beneficiarse con aquella información obtenida, utilizándolos para un fin que perjudica a terceras personas.

Se puede señalar que existe, la Ley 27309, la misma que añade los delitos informáticos al Código Penal en el que específicamente solo se ha señalado dos aspectos en general, los mismos que cuentan con diversas características. Por lo mismo es que el legislador, tiene como fundamento primordial, el uso de la computadora como herramienta para cometer los delitos informáticos.

Esta Ley de delitos informáticos, establece especialmente penas para atentados contra la integridad de datos informáticos, sistemas informáticos, proposiciones a niños y adolescentes con fines sexuales, incitación a la discriminación, contra la intimidad y el secreto de las comunicaciones como el tráfico ilegal de datos, la interceptación de datos informáticos, suplantación de identidad, abuso de mecanismos y dispositivos informáticos y el fraude informático. El aumento de la criminalidad informática en el Perú y a nivel mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son

[2] Código Penal Peruano de 1991

denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción. (Dávila Laguna, 2017)

En la mayoría de los delitos informáticos, el delincuente cibernético, es la persona que tiene conocimientos informáticos y de sistemas lo que le permitiría acceder sin autorización a terminales públicas o privadas (acceso ilícito), quebrando o transgrediendo todos los sistemas de seguridad. En los delitos informáticos, el fin es impedir el acceso e imposibilitar el funcionamiento del sistema, este es el principal propósito y debe existir dolo (conocimiento y voluntad de ejecutar el delito). En los delitos informáticos se va a valorar el daño y en este caso se sanciona el uso indebido de las tecnologías de la información. (Dávila Laguna, 2017).

Es de vital importancia, señalar que popularizar de información y más aún si esta es íntima, no sería considerado como delito informático, sino cabria en los delitos de violación a la intimidad, por ende su pena es hasta cuatro años.

2.1.1.2. La tipicidad en los Delitos Informáticos

La aplicación temporal o vigencia temporal de la ley penal constituye el conjunto de principios o reglas que tratan de conflicto entre diferentes leyes penales en el tiempo en relación a un hecho imputado.

Como ya sabemos, ya ley es una expresión dinámica al cambio que se genera en la sociedad, tal como lo afirma Peña Cabrera "la ley es la expresión fragmentaria de la cultura siempre cambiante". (Peña Cabrera, 1997). Algunas leyes se vuelven inoperantes y, por ende, dejan de cumplir una necesidad social. Esta situación de actualización origina que las leyes innecesarias sean

reemplazadas por otras que son consideradas eficaces en relación a las nuevas situaciones sociales.

El periodo que media entre el final de la publicación y su entrada en vigencia se denomina vacatio legis.

La tipificación de un delito, tiene que ver con la descripción de actos ilegales que puedes ser por acción u omisión, que son considerados como delitos.

Suele afirmarse que un acto es típico cuando se puede encuadrar o encajar en un tipo penal, en virtud del principio de legalidad, si un acto encaja en lo tipificado como delito, se considerar como tal.

Grisanti, señala que "gráficamente se ha llamado a la tipificación encuadrabilidad, para poner de manifiesto que un acto es típico, cuando encuadra a la perfección en algún molde delictivo, en alguna figura delictiva, es decir, en algún tipo legal o penal". (Grisanti A., 1989)

La tipificación de los delitos informáticos, es necesaria, toda vez que se ha evidenciado que si estas conductas no están establecidas dentro del marco normativo, sea dentro del Código Penal o en una ley especial, las conductas ilegales no podrán ser objeto de sanción, conforme a la vigencia del principio de legalidad.

En ese sentido, es que la Ley de Delitos informáticos, tipifica primigeniamente el acceso ilícito, que no es otra cosa, que acceder deliberadamente e ilegalmente a un sistema información, afectando las medidas de seguridad; tendrá una pena no menor de 1 ni mayor de cuatro años de pena privativa de libertad. Como podemos observar lo que se persigue es el acceso a un sistema informático de manera ilegal; lo cual de ingresar a un sistema

informático de una empresa bancaria, pondría en riesgo la seguridad de los clientes, en su medida poder ver afectado su patrimonio.

En ese sentido, procederé a señalas, algunos artículos de la Ley N° 30096, que guarden íntima relación con nuestro tema de investigación:

*"**Artículo 8.** Fraude informático El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.*

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social." (Ley de Delitos Informaticos, 2013)

El delito antes mencionado, guarda relación con la afectación a las empresas bancarias, es decir aquellas del sistema financiero, al menos al momento de determinar la clonación de datos informáticos, toda vez que el sujeto al clonar la información, podrá hacerse acreedor del patrimonio del posible agraviado.

No consideramos que exista mayores delitos que guarden relación con las posibles afectaciones a la empresa bancaria, consecuencia de ello, es que las empresas bancarias, penalmente se encuentran desprotegidas, en ese sentido susceptible de la comisión de algún delito contra su patrimonio o de aquel que se encuentra bajo su cuidado y tutela.

Los delitos informáticos, de usual comisión en nuestro país, son el fraude y el hack; así como el envió de software que contienen virus, así como la suplantación de identidad; el más común dentro del sistema financiero, es aquel que con el propósito de obtener información privada, como claves de cuentas bancarias así como correos electrónicos, hacen llamadas a los usuarios/clientes o envían correos maliciosos. Asimismo se tiene el espionaje a las empresas, los fraudes bancarios, el robo de datos de propiedad intelectual, la clonación de tarjetas, siendo el tipo más común, que infringe no solo a la entidad bancaria, sino también al cliente de la entidad bancaria, pudiendo extraer ahorros de toda una vida.

La criminalidad informática, sigue en aumento y consecuencia de ello, es que se general perdidas económicas, frente a la infinidad de fraudes cometidos, no solo por una persona o grupo reducido de personas, sino por organizaciones delictivas, que no son denuncias por no se encontrar a los culpables, o es que las transacciones se llevaron fuera del país.

El sujeto activo de los delitos informáticos, seria aquella persona que ejerce un amplio conocimiento informático y de sistemas, que accede sin autorización a sistemas públicos o privados, es decir accede a estos de manera ilícita, sin permiso, haciendo vulnerables sus sistemas de seguridad.

Es posible que por común acuerdo de países, los delitos informáticos, se trabajen de manera conjunta, pues no solo importa a un solo país, como lo indicamos, los delitos no necesariamente se realizan en un país, sino en diferentes países y desde diferentes países, conforme a lo señalado en el

Convenio de Budapest o denominado también como Convenio sobre la ciberdelicuencia.

2.1.1.3. Características de los Delitos Informáticos

Según el autor mexicano Téllez J. las características de los delitos informáticos son las siguientes:

- Conductas criminales de cuello blanco
- Acciones ocupacionales
- Acciones de oportunidad
- Provocan serias pérdidas económicas
- Ofrecen posibilidades de tiempo y espacio
- Muchos casos y pocas denuncias
- Proliferación continúa
- Ilícitos de impunidad ante la ley.
- Delitos informáticos que genera fraude o robo por medios de tarjetas de crédito.
- Registros magnéticos transitorios
- Sistemas impersonales
- En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir.
- En el centro de cálculo hay un personal muy inteligente
- El error y el fraude son difíciles de equiparar.

2.1.2. EL DERECHO A LA INTIMIDAD EN LA INFORMACION COMPUTARIZADA

Es ineluctable precisar que entre los derechos de la personalidad, establecidos por el Código Civil Peruano promulgado por Decreto Legislativo N° 295 de 24 de julio de 1984, está el llamado derecho a la intimidad, en sus artículos 14°,16° y 18°, que cobran vigencia en la sociedad contemporánea por las múltiples formas que existen para transgredirlo fácilmente. Es tal su importancia, que ha sido considerado como uno de los derechos vertebrales que sustentan el sistema democrático. (BLOSSIERS MAZZINI, 2008)

En la actualidad, el hombre se encuentra expuesto para que esta esfera de privacidad que la reserva para sí y su familia, sea vulnerada. La era "tecnotrónica" facilita que particulares y el Estado mismo penetre en esta esfera privada, perturbando la tranquilidad y obstaculizando el libre desarrollo de la personalidad.

Muchas veces solemos pensar que en circunstancias como las nuestras (países subdesarrollados) existen problemas prioritarios, como el hambre, la miseria, la falta de empleo, y en general el deterioro de las condiciones de vida, problemas sociales que requieren de voluntad política, de modo que los problemas relativos al ser humano, enfocados desde una perspectiva individualista, aparecen como de segundo orden. Primero ocupémonos del hambre, y luego de la vida privada, o del honor, o de la libertad de las personas, por ejemplo, o en todo caso lo segundo está

supeditado al primero. Esta concepción debe ser superada, y la historia así lo demuestra, como hacen lo propio los tiempos actuales.

Un enfoque sociológico de estos derechos (partiendo del principio aristotélico que el ser humano es un ser social) nos permite puntualizar que el tratamiento debe ser paralelo; que condicionar uno a otro, nos llevará a conclusiones erradas para la humanidad. Tan importante es luchar contra el hambre y la miseria, como lo es la defensa de los demás derechos fundamentales del ser humano.

A continuación, revisaremos brevemente algunos aspectos sociológicos existenciales de la intimidad: Persona, intimidad y sociedad. (BIDART CAMPOS, 1988)

La palabra persona tiene como significado etimológico el de máscara, que servía al actor para «representar» los personajes en las obras teatrales en Roma, este significado constituye una real metáfora, pues en verdad el ser humano desempeña un papel en la vida social, pero detrás de dicha representación (máscara) se encuentra el verdadero ser, su vida íntima, personal o familiar.

La vida íntima, personal, la individualidad, entra en una relación dialéctica dinámica y conflictiva con la sociedad. El ser humano proyecta su personalidad en dos dimensiones, una social, exógena, y otra de regreso hacia sí mismo; y es que el ser humano es individuo y es sociedad; y esta relación dialéctica constituye todo un problema existencial permanente de la humanidad que cobra especiales características en el hombre contemporáneo.

Los conflictos del hombre a través de la historia han sido por la libertad; la lucha contra todo aquello que oprimía y oprime al ser humano, impidiéndole el desenvolvimiento y desarrollo integral de su personalidad; las grandes revoluciones tuvieron en mente liberar al hombre, aun cuando la historia nos demuestra que, posteriormente, los grupos sociales o clases sociales que encabezaron dichos procesos, fueron creando mecanismos de opresión, en función a la defensa de sus propios intereses que entraban en conflicto con los intereses de los otros grupos sociales.

La historia también nos demuestra que la humanidad se ha desarrollado poniendo el acento, en unas etapas, en la individualidad y otras, en el aspecto social del ser humano. En la era contemporánea, apreciamos que con el triunfo de la revolución francesa se puso el acento en el individuo, como una reacción frente al absolutismo imperante. Se pensó que al fin el ser humano alcanzaba la posibilidad de un desarrollo libre de su personalidad; la libertad, fue el valor convertido en derecho que encabezó la lucha contra el poder imperante. No obstante, el individualismo fue engendrando su propia destrucción, ya que ha resultado pernicioso para la humanidad, motivando que desde fines del siglo pasado se produjera una reacción hacia lo social.

Y es así que el siglo XXI apreciamos en el mundo, luego de las experiencias de los socialismos autoritarios, una reacción para poner de relieve los derechos personales, respetándose al ser humano en su individualidad. La esperanza es que se logre un justo equilibrio entre el individuo y la

sociedad, ya que los extremos han sido negativos porque atentan contra la naturaleza del ser humano.

Este equilibrio sólo será posible en la medida que se respete el ámbito que el ser humano reserva para sí mismo, el ámbito de la creación, de la seguridad y que se convierte en el sustento y resorte de impulso para el desarrollo de los demás derechos del ser humano; por ello se afirma que el derecho a la vida privada es la expresión del derecho a la libertad.

El derecho a la intimidad de configuró en el derecho sustantivo recién en el siglo pasado, y es que si bien, anteriormente, ha existido la protección a ciertos ámbitos propios de la intimidad como es el domicilio, lo cierto del caso es que la autonomía la adquiere desde fines del siglo XIX, cuando el adelanto de la ciencia y tecnología ponen en evidencia la facilidad con que se puede penetrar en el ámbito de la vida privada de las personas; cuando los medios de comunicación masiva adquieren papel preponderante en la comunidad y pueden poner al descubierto hechos que las personas no desean que se divulguen; cuando las técnicas de espionaje son cada vez más sofisticados.

A estos avances de la ciencia y la tecnología, debe agregarse algunos fenómenos sociales propios de la era contemporánea como la masificación social, que significa la pérdida de la individualidad para convertirse en "hombre-masa".

Es cierto que en la actualidad los fines de la sociedad están destinados a forjar seres humanos carentes de individualidad, dóciles, con falta de sentido crítico, con pensamientos uniformes, conformistas con el orden

establecido, donde ser diferente resulta una suerte de indecencia. Este proceso de socialización que se inicia desde la niñez, que lo impone el medio familiar, el grupo social la educación y los medios de educación masiva, fundamentalmente la televisión, se convierte en un bombardeo permanente que pretende aniquilar la posibilidad que el ser humano piense por si mismo. ¿De qué nos sirve la libertad de expresión si carecemos de pensamientos propios? Tener pensamientos propios no significa tener ideas originales que nunca nadie las haya pensado, sino que los mismos hayan sido consecuencia de proceso interno nuestro, de nuestra propia actividad.

Este proceso de masificación es un fenómeno universal que se encuentra presente en la sociedad contemporánea sin distingos de clases de sociales. El hombre- masa existe en oriente y occidente, en las clases sociales altas e inferiores obedece a una característica especial ya señalada por Ortega y Gasset.

Otro fenómeno social que ha complicado la vida privada del hombre contemporáneo es la concentración urbana, que se inicia en los países desarrollados con la revolución industrial y que provoca el aumento de las interrelaciones sociales. En el caso nuestro, y como fenómeno que se acentúa a partir de la década del cincuenta, con el éxodo rural, y consecuentemente la migración urbana que ha originado una fuerte concentración en las ciudades principales de la costa con los consiguientes problemas de convivencia y de acciones sociales que determinan una disminución del ámbito de la vida privada de las personas.

En suma, el panorama que se nos presenta es sumamente peligroso para la persona, y por ello la necesidad de otorgar la protección Jurídica al ámbito de la intimidad, resultando ser la expresión máxima del derecho a la libertad y la posibilidad de un desarrollo armonioso de la persona en la colectividad y con la injerencia del Internet no sólo hablamos del mundo del futuro sino del presente donde se vulnera una y otra vez la intimidad de las personas, situación que el derecho debe afrontar. (ARMAGNAGUE, 2002)

A) Aspectos jurídicos del derecho a la intimidad.

La intimidad como bien jurídico autónomo data de fines del siglo XIX, cuando en 1890, Samuel Warren, comerciante y abogado, escribió conjuntamente con su socio Luis Brandeis, también abogado, el artículo "El derecho a la intimidad", publicado en el Harvard Law Review, donde se vislumbra ya el contenido autónomo del derecho mencionado, por lo que puede considerarse como la semilla que ha ido germinando hasta la actualidad, para convertirse en un derecho de la personalidad base, sobre el que se desarrollan los demás derechos del hombre. (Warren & Brandeis, 1981)

La apreciación anterior, en efecto, reconoce que con anterioridad, el ámbito de la vida privada ha sido protegido de una u otra forma, aun cuando sumergida dentro de otros derechos. Novoa Monreal refiere que el respeto a la vida privada era un valor tradicional en la Edad Media.

Podemos afirmar que en el Derecho Romano el hogar doméstico (la casa – la domus) juega un papel importantísimo en la vida de los romanos, con un contenido moral y jurídico trascendental. Era, como lo es actualmente,

el lugar del recogimiento y la protección de la persona del mundo exterior. La protección de la casa ha sido reconocida a través del derecho a la inviolabilidad del domicilio. El dueño de la casa, el pater familias, no sólo era el jefe del hogar, con potestades amplias sobre toda la familia, sino que era también el Juez, el sacerdote, es decir, el ámbito de la lasa estaba bajo su imperio; todas las divergencias eran resueltas por él, sin que autoridad alguna pudiera intervenir.

El concepto de domicilio en Roma, no coincidía necesariamente con el de casa o residencia, ya que la nota fundamental para ello era que el lugar se convierta en el centro de las actividades o intereses de la persona, a pesar que etimológicamente domicilio deriva de dos vocablos latinos DOMUS y COLO, que a su vez significa DOMUN COLERE que significa HABITAR UNA CASA. Pero, es evidente que, ya en Roma existía la protección a este espacio destinado al desarrollo de la intimidad de la persona y su familia.

Luego de este breve recuento de la evolución jurídica del derecho a la intimidad, podemos señalar que cuando se trata de su naturaleza jurídica, esta no es ajena al debate suscitado al mismo, no siendo ajeno al debate suscitado respecto a los derechos de la personalidad. ¿El derecho a la intimidad como uno de los derechos de la personalidad es realmente un derecho subjetivo o es sólo un bien jurídicamente protegido?. La respuesta que demos a esta interrogante tiene consecuencias en el sistema jurídico, por cuanto si se trata de derechos subjetivos, su trascendencia rebasa al derecho positivo; en cambio, sí se trata de bienes jurídicamente protegidos, simplemente debemos limitarnos a la protección que brinde la ley a ciertos

derechos. Bien sabemos que en lo que se refiere a los derechos de la personalidad, se trata de hechos subjetivos que deben estar en la conciencia de la humanidad, para la protección integral de la persona, por lo que su motivación además de jurídica es fundamentalmente ética trascendiendo el marco de la norma.

Los adversos a considerar la existencia de derechos de la personalidad y por ende a la intimidad, sustentan su posición en base al concepto de derecho subjetivo, que supone un poder o señorío atribuido a la voluntad, un objeto sobre el cual versa y un deber correlativo a cargo de otro u otros sujetos contra los cuales se ejerce la pretensión del titular y finalmente sostienen de estos pretendidos derechos no tienen modos de adquisición, transferencia o extinción. Podemos mencionar a Ennecerus, Kipp y Wolf, y Alfredo Orgaz.

a) El señorío de la voluntad: El derecho subjetivo es la expresión de la voluntad individual; el atributo principal, como lo señala Messineo es el estar fundado sobre intereses autónomos. En el caso del derecho analizado, no existe facultad alguna a favor de las personas, ni «un interés autónomo», ya que no existe nada que dependa de la voluntad de la persona; sin embargo, el mismo Messineo se encarga de refutar esta posición, indicando que estos derechos de la personalidad.

b) El objeto: Se ha considerado que la persona humana siendo sujeto de derecho no puede ser objeto a su vez de la relación jurídica; sin embargo, existe confusión en tanto que lo que constituiría objeto de la relación jurídica no es el hombre en cuanto a ser ontológico, sino aquellas categorías

existenciales que sirven para que el ser humano se desarrolle como tal, y que si bien son circunstanciales a él pueden ser agredidas, inclusive puede verse privado de ellas, por lo que es separable del sujeto, siendo necesaria su protección normativa.

c) El deber correlativo: El derecho subjetivo implica la voluntad del individuo, un objeto determinado y un deber por parte de otra persona, quien se convierte en sujeto pasivo. Los derechos de la personalidad no requieren de un sujeto pasivo inmediato y específico, ya que está encuadrado dentro de los derechos absolutos y por ende todos son sujetos pasivos en cuanto tienen el deber de respetar tal atribución, exactamente de la misma forma como ocurre con el derecho de propiedad, en la que el propietario es el sujeto activo que tiene la facultad y todo el mundo se convierte en sujeto pasivo, pues, tienen el deber de respetar dicha propiedad. El derecho a la intimidad, como derecho de la personalidad, al igual que el derecho de propiedad, son derechos absolutos y, por ende, oponibles erga omnes.

d) Tratamiento dogmático: Se señala que la legislación no dispone los modos de adquisición, transferencia, extensión, etc. de estos supuestos derechos y por lo tanto ello genera incertidumbre en su contenido y límites. Debemos indicar que está de por medio nuestra concepción del Derecho, en el sentido de colocar en el centro de la preocupación al ser humano, y no a la propiedad o al el contrato. Después de todo, si somos conscientes que estos derechos son transgredidos permanentemente, es necesario protegerlos normativamente.

B) La Confidencialidad en la Información Computarizada

Núñez nos explica "A fines del siglo pasado el Derecho a la intimidad se definía como "el derecho a ser dejado a solas", sin embargo, las nuevas dimensiones aportadas al problema de la defensa de la intimidad, en especial por la difusión del uso de los computadores u ordenadores obligan a una reformulación del concepto entendido ahora como "el derecho del individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal".

"El desarrollo del fenómeno informático en nuestra sociedad ha traído consigo una mayor vulnerabilidad de las libertades del Individuo y la invasión frecuente de su esfera privada. La intimidad, el ámbito íntimo, o el "right to privacy" (por utilizar la terminología anglosajona), es un concepto moderno que alcanza un reconocimiento implícito, a través de la libertad de conciencia, en las declaraciones de derechos que se promulgan con el advenimiento del Estado liberal y tendrá su reflejo en la tradición constitucionalista occidental de nuestro siglo".

La información computarizada de carácter personal y privado contenida en las bases de datos puede ser "accesada" u obtenida sin consentimiento por medios informáticos y telemáticos, lesionando el derecho de la intimidad tratándose de personas naturales y el derecho a la confidencialidad tratándose de personas jurídicas. Ante esta realidad el Derecho ha examinado mecanismos que permitan proteger jurídicamente de manera eficiente la información de carácter privado, uno de estos mecanismos es

el Habeas Data. El Derecho de la información tiene dos aristas: Es el derecho que todos tenemos de ser informados de lo que sucede y puede interesamos y también, es el derecho a informar a los "profesionales de la comunicación" sobre los acontecimientos. Sin embargo, el ejercicio de este derecho no debe vulnerar otros derechos, como es el derecho a la intimidad, sin que esto signifique en ningún caso menoscabo del ejercicio del derecho de información."

Asimismo, debe tenerse en cuenta que en la doctrina, "El derecho a la intimidad, tradicionalmente es definido como un derecho esencialmente negativo, adquiere hoy por hoy contornos nuevos y distintos: ya no solo se refiere a un derecho delimitador de no interferencia, sino que vendrá a definirse con un contenido abiertamente positivo. Frente al derecho a la información, caracterizado por su doble vertiente de derecho a informar y a ser informado, el individuo de la sociedad tecnológica afirmará su derecho primario a controlar el flujo de informaciones que sobre su vida privada puede existir en las base de datos. La intimidad se perfila así como derecho o facultad de autodeterminación informativa y encontrará su expresión legislativa a nivel internacional, entre otras normas, en el Convenio Europeo para la Protección de datos personales".

El nuevo enfoque del derecho de la intimidad, influye también en la nueva dimensión del derecho a la confidencialidad de las personas jurídicas, que en nuestra legislación está protegida por figuras jurídicas como el secreto de producción. En efecto, el artículo 83° del Decreto Ley 26017 establece que "El Estado protege al titular de un secreto de producción contra el

aprovechamiento ilícito de su empleo, divulgación o comunicación, siempre que el titular haya tomado las medidas necesarias para preservar su carácter secreto y que sea efectivamente novedoso" (Ley General de Propiedad Industrial , 1992) o por la competencia desleal, al establecer el artículo 6° del Decreto Ley 26122 que se "considera acto de competencia desleal y, en consecuencia ilícito y prohibido, toda conducta que resulte contraria a la buena fe comercial, al normal desenvolvimiento de actividades económicas y, en general, a las normas de corrección que deben de regir en las actividades económicas". (Ley sobre Represión de la Competencia Desleal, 1992)

De otro lado, el desarrollo tecnológico expone cada vez más numerosos problemas Jurídicos en los que la aplicación de las normas Jurídicas citadas puede tornarse deficiente. Verbigracia: la comunicación teleinformática y los correos electrónicos se están trasformando en un instrumento bastante favorable y sumamente productivo para las empresas, a consecuencia de sus irrefutables provechos: obteniendo gran rapidez, y logrando mayor performance en sus comunicaciones. Ahora bien, en este campo de las comunicaciones de información computarizada han surgido nuevos problemas jurídicos en torno a la confidencialidad de las empresas.

Verbigracia; en los Estados Unidos, se han producido varios casos jurídicos en relación al problema de la vulneración de la confidencialidad de las empresas, a través del uso de los correos electrónicos y de la comunicación teleinformática de información computarizada. Entre ellos podemos citar el

litigio Borland/Symantec en el que "recientemente se acusó a Eugene W., ex vicepresidente de Borland International de pasar documentos confidenciales de la compañía utilizando correo electrónico (que también se le conoce como E- mail a uno de los principales rivales de Borland; Symantec Corporation. Después de que Eugene W. Dejó a Borland por un puesto en Symantec, la gerencia de Borland examinó la cuenta del correo electrónico de Eugene W. Y descubrió evidencia probatoria suficiente que condujo, inclusive, a que el presidente de Symantec, también fuera acusado en el caso.

En nuestro país existe un aumento sin precedentes en la utilización de las nuevas tecnologías por parte de las empresas. En la actualidad se haya correos electrónicos, redes electrónicas de datos, base de datos interconectadas, que hacen estimar que se manifestarán variadas dificultades legales circunscritas a estas actividades. Verbigracia podemos puntualizar que la SMV ha expresado nuevas disposiciones referentes al Mercado de Valores, por las cuales se obliga a las Sociedades Agentes de Bolsa a tener un sistema automatizado de recepción y registro de órdenes, que sea inviolable y asegure la continuidad del servicio. El plan deberá posibilitar a la sociedad observar las órdenes e instrucciones de sus clientes y asignar sus operaciones a través de sistemas computarizados y de comunicación que dificulte la intromisión o alteración alguna que desvirtúe la intención del cliente. Lo que ha de implicar manejo de información computarizada y la adopción de sistemas de seguridad de datos que han de tener consecuencias jurídicas. De otro lado debe tenerse en cuenta, por citar un ejemplo, que se han establecido servicios como

Dataline que brindan facilidades para intercomunicarse con otros usuarios de computadoras poseedores de base de datos utilizando modem, la red telefónica y la red de conmutación de paquetes MEGAPAC. Como vemos, la confidencialidad de la información computarizada necesita, ineludiblemente, de la asunción de dichas medidas que salvaguarden la integridad de la información

2.1.3. DEFENSA DE LOS DATOS PERSONALES

Marie Iasoni nos explica que la protección de la privacidad constituye un problema central para las transacciones que se realicen a través de la red, ya que el usuario estará expuesto con frecuencia a suministrar sus datos personales, y estos serán registrados de múltiples maneras y utilizados para fines muy diversos, que incluyen aspectos tan variados como el marketing, el control de la vida privadas, la persecución política, o la discriminación. (IASONI, 2002, pág. 95)

Sin duda que en el marco de un sitio de comercio electrónico el usuario será a menudo, el más solicitado para que transmita sus datos personales sin los cuales, en efecto, ninguna transacción electrónica sería posible.

Por lo tanto, el usuario que desee contratar en línea, suministrará al vendedor informaciones personales como el nombre, dirección, teléfono, etc.

El Perú no dispone de una ley especial de protección de los datos personales, contrariamente a la mayor parte de los países de Europa y de los EE.UU.

Sólo existe protección en la legislación común a través del recurso constitucional de "Habeas Data". (ABALOS, ABBIATI, & OTROS, 2002, pág. 76)

En consecuencia, en el ejercicio de la Acción de Habeas Data un ciudadano puede exigir que cualquier autoridad, funcionario o persona que quebrante o amenace los derechos a que se refiere el artículo 2°, inciso 5 de la Constitución, cese estos actos, situación que hemos tratado oportunamente.

De otro lado, el secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado:

Inciso 6: A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar. (Congreso Constituyente Democrático , 1993)

Inciso 7: Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propia. (Congreso Constituyente Democrático , 1993)

En conclusión, "toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley". (Congreso Constituyente Democrático , 1993)

Por tanto, si en la práctica la acción constitucional de Habeas Data funciona como un instrumento protector de la privacidad, así como una norma de acceso a la información pública para el ciudadano, no parece una herramienta efectiva para el control de los datos personales.

En efecto, el Habeas Data es una herramienta procesal que es efectiva, solamente, cuando existe una trasgresión o amenaza contra la privacidad.

Ahora bien, el interés de las leyes de protección de los datos personales es presentar un carácter preventivo y establecer normas especiales para el manejo de los datos personales, resaltando una real responsabilidad de las empresas que tratan este tipo de información.

Así, las empresas deberán poner cierta diligencia en el manejo de los datos recogidos, es decir, adoptar y seguir una verdadera política de protección.

Como señala Iasoni, aunque el Perú no dispone todavía de una ley especial que obligue a las empresas del país a divulgar una política de protección de los datos personales, en relación con el comercio electrónico, creemos que es fundamental que las empresas, que se dedican a actividades de comercio electrónico por Internet, desarrollen desde ahora una verdadera política de protección de estos datos. (IASONI, 2002, pág. 96)

2.1.4. CONVENIO DE BUDAPEST

Perú a la fecha no forma parte del Convenio de Budapest, si bien es cierto ha sido invitado para que pueda adherirse, nuestro legisladores aún se encuentran en el análisis de si es viable o no, pese a que el objeto del convenio es combatir el delito informático y fomentar la cooperación entre los países.

El convenio en mención, determina la necesidad de aplicar, una política de común acuerdo, a fin de proteger a la sociedad de la ciberdelicuencia, adoptando legislación adecuada, en cooperación internacional.

La armonización de las leyes, con el convenio, haría frente a los delitos informáticos, y en consecuencia habría un avance en las técnicas de investigación del delito, ello en cooperación internacional.

El convenio de Budapest, el 28 de octubre de 2010, donde 30 estados firmaron el convenio, ratificándolo y adhiriéndose a la convención, mientras que otros 16 solo la rubricaron, más no la ratificaron.

Lo más resaltante, en cuanto a delitos es:

> *Artículo 7. Falsedad informática Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Los Estados podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.* (Convenio de Budapest, 2001).
>
> *Artículo 8. Estafa informática Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como*

infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a. *la introducción, alteración, borrado o supresión de datos informáticos,*
b. *cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.* (Convenio de Budapest, 2001).

Ambos artículos señalados, insisten en que los estados deben de asumir y adoptar medidas necesaria, para determinar los delitos del crimen informático, entendiendo que existen posturas, de que el derecho penal, tiene una finalidad preventiva, y al tipificar los delitos, no se cometan tales accionares.

El Convenio sobre la ciberdelincuencia (o Convenio de Budapest) persigue dos objetivos fundamentales: por un lado, homogeneizar las definiciones sobre ciberdelito; por el otro, establecer las bases para la cooperación internacional y el intercambio de información en lo que respecta a estos ilícitos. Dado que el país se encuentra próximo adoptarlo, tres expertos detallan sus implicancias. (Motessi, 2017)

La primera observación que realizan los especialistas es que el Convenio requiere que los estados miembros adapten sus legislaciones nacionales a los estándares mínimos que estipula. "Si bien incorporarnos no es lo peor que podría suceder, cuando se legisla en materia penal es necesario tomar la

mayor cantidad de precauciones posibles", asegura Enrique Chaparro, secretario general de Fundación Vía Libre. (Motessi, 2017)

2.1.5. IMPACTOS EN LA EMPRESA BANCARIA.

Las operaciones financieras, se encuentran reguladas normativamente en todos los países.

Los impactos legales que se generarían ante la comisión de delitos informáticos, se daría ante la violación cometidas por las instituciones financieras, respecto de las normas que regulan el sistema financiero; aunado a ello se incluye las afectaciones que surtirían el incumplimientos de las obligaciones asumidas por las entidades financieras, tanto contractuales, como fiscales y otras.

Usualmente de suele dar el denominado blanqueo de dinero, lo cual constituye una violación a régimen normativo penal y tributario, y es cometido no solo por entidades nacionales, sino también internacionales.

La reputación es un elemento esencial de las entidades financieras, toda vez que parte de ella la confianza que puede generar a sus clientes y quienes postulen como sus nuevos clientes.

La percepción que se tiene es de suma importancia en la realidad bancaria, pues no solamente se debe de ser integro, dedicado y competente, sino que debe aparentarse ello; la percepción y la realidad deben de ir de la mano.

En ese sentido, la comisión de algún delito informático, guardaría íntima relación con un posible fraude bancario, lo cual incidiría en la reputación de la entidad bancaria, dañándose su imagen.

Se dice que los fraudes cometidos en el comercio electrónico, en todo América Latina y el Caribe, suman por los menos los US$430,000,000.00 al año, siendo el país más afectado Brasil.

Como mencionamos el país más afectado es Brasil, sin embargo los siguen países como México, Colombia, Chile y Argentina, causando gran preocupación en los gobiernos de esta parte del mundo, pues los ataques cada vez son más sofisticados, causando graves daños a la población.

Según una publicación en el Diario Gestión "Las autoras de la investigación advirtieron que uno de los delitos digitales de mayor impacto económico, el phishing (la suplantación de la identidad de una persona para hacerse con las contraseñas de sus tarjetas de crédito o cuentas bancarias) ha aumentado en la región 20% más de lo que ha crecido a nivel global". (Redacción Gestión, 2014); Asimismo señalan que "El informe agrega que América Latina cuenta con 80,000 bots, robots digitales que pueden enviar archivos maliciosos. Un 44% de los bots se encuentran en Chile, 15% en Perú y 11% en Argentina, señaló el documento." (Redacción Gestión, 2014)

Según una publicación de México, "...los bancos pierden hasta 93 millones de dólares anuales solo en fraude en línea" (Chavez, 2014)

Se refiere que "Alemania es el más afectado económicamente por la ciberdelincuencia, (cyberkriminlitat) pues es también uno de los más avanzados en términos de adopción de tecnología y penetración de Internet. El impacto a su economía representa 1.6% de su Producto Interno Bruto (PIB),

seguido de los Países Bajos con 1.5% de su PIB y en tercer lugar Estados Unidos con 0.64%." (Chavez, 2014).

2.2. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **ARCHIVO.-** Conjunto de datos almacenados bajo un solo nombre, tal como una lista de direcciones, lista de fechas o facturas por cobrar que pueden ser procesadas por un computador.
- **BACK UP.-** Copia de respaldo de archivos o programas de datos que es conservada para ser usada solamente si el archivo inicial es destruido.
- **BAUD RATE.-** Velocidad de transmisión de caracteres en una línea conectada usualmente por impresoras, terminales y módem. Su nombre deriva de Emil Baudot quien fuera un pionero en telegrafía impresa.
- **BANCA ELECTRONICA:** Es una red de cajeros automáticos que ofrece gran cantidad de servicios relacionados al manejo de dinero, como tarjetas de débito, transferencias electrónicas, servicios de pago, etc. Su principal competidor en el mercado financiero es Red Link.

  Esta red de cajeros automáticos se complementa con el sistema de banca electrónica Pago mis cuentas es usada principalmente por bancos privados. Por el contrario, Link es usada principalmente por bancos estatales.

  Es el conjunto de instituciones encargadas de la circulación del flujo monetario y cuya tarea principal es canalizar el dinero de los ahorristas

hacia quienes desean hacer inversiones productivas. Las instituciones que cumplen con este papel se llaman "Intermediarios Financieros" o "Mercados Financieros".

- **BANCARIZACION:** Bancarización significa utilizar intensivamente al sistema financiero para facilitar las transacciones efectuadas entre los agentes económicos. Este proceso permite evitar el uso del dinero físico.
- **BEAT-** Abreviatura de dígito binario, unidad básica de información utilizada por una computadora.
- **BYTE.-** Secuencia de ocho bytes tratados como unidad. Es el menor elemento direccionable en el computador usualmente utilizado para almacenar un carácter.
- **CAPACIDAD.-** Cantidad de información que quiere decir que puede almacenarse en una unidad magnética (diskette) usualmente descrita el K Bytes o Kilo Bytes, donde un kilo bytes representa 1,024 bytes.
- **CARÁCTER.-** Una letra, signo especial, dígito numérico.
- **CARGA DEL SISTEMA OPERATIVO.-** Leer el sistema operativo del área reservada al mismo en el diskette.
- **CLIENTES:** Es el conjunto de actividades interrelacionadas que ofrece un suministrador con el fin de que el cliente obtenga el producto en el momento y lugar adecuado y se asegure un uso correcto del mismo.
- **COMANDO.-** Instrucción ingresada por el usuario mediante el teclado o Mouse para dirigir la acción del computador.

- **COMPATIBILIDAD.-** Habilidad de un computador para aceptar y procesar datos producidos por otro computador sin ninguna modificación en los discos o diskettes en los que los datos son transferidos.
- **CONFIGURACIÓN.-** Conjunto de equipos tales como impresoras, unidad de discos conectados a un computador que han sido programados para operar como un sistema
- **COMERCIOELECTRONICO:** El **comercio electrónico**, también conocido como e-commerce (electronic commerce en inglés) o bien negocios por Internet o negocios online, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas.
- **CPU.-** Unidad Central de Procesos, es el llamado cerebro del computador donde se interpretan y procesan las instrucciones y los datos a través del microprocesador.
- **CRIMINALIDAD INFORMATICA:** La realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).
- **CURSOR.-** Indica la posición activa en la pantalla de la terminal. Generalmente es una línea, en forma horizontal o vertical.
- **CHIPS.-** Pequeño elemento de silicio que contiene la lógica del computador, los circuitos para el procesamiento de datos, la memoria

principal, la entrada y salida de la información. Los chips están soldados sobre una plaqueta de circuito impreso para formar el computador.

- **DATOS.-** Los números, letras, símbolos procesados o producidos por una computadora.
- **DELITO INFORMATICO:** "Delitos informáticos" son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático El Delito Informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.
- **ENTRADA.-** Datos ingresados en el computador mediante un periférico.
- **ENTRADA / SALIDA.-** Aceptación o transferencia de datos desde y hacia un computador.
- **EMPRESA:** Una empresa es un sistema que interacciona con su entorno materializando una idea, de forma planificada, dando satisfacción a unas demandas y deseos de clientes, a través de una actividad económica.

  Requiere de una razón de ser, una misión, una estrategia, unos objetivos, unas tácticas y unas políticas de actuación.

Se necesita de una visión previa y de una formulación y desarrollo estratégico de la empresa.

Se debe partir de una buena definición de la misión. La planificación posterior está condicionada por dicha definición.

- **EMPRESA BANCARIA:** Es la organización que reúne capital y trabajo y la visión del negocio o el objeto de la sociedad u objeto social.
  En el caso de empresa bancaria es la organización debidamente autorizada por la Superintendencia de Banca y Seguros, para operar con dinero del público "intermediación financiera", vale decir, recibir dinero del publico poner su propio capital y prestarlo.

  Constituye una organización dedicada a intermediar financieramente con autorización del estado por operar con dinero del público. Se denomina bancaria es porque se dedica a la intermediación autorizada por la Ley. (26702).

- **FIRMWARE.-** Conjunto de instrucciones o programas habitualmente almacenados en la memoria de lectura (ROM) del computador. Generalmente contiene las instrucciones para la carga del sistema operativo o para la realización de funciones específicas para control del periférico del sistema.
- **FRAUDE INFORMATICO:** La informática es una ciencia o técnica que ha permitido simplificar y agilizar una gran variedad de actividades en diferentes áreas. La informática se hace cada día más imprescindible, ya que estamos viviendo una época en la cual la tecnología juega un papel sumamente importante.

- **FORMATEAR.-** Acción de preparar la inicialización de la estructura de un diskette sobre el cual corre el sistema operativo.
- **HARDWARE.-** Se trata de la parte física del computador, sus componentes duros tales como elementos mecánicos o magnéticos.
- **LENGUAJE.-** Mecanismo de expresión y codificación de instrucciones al computador, definido y gobernado por un conjunto de reglas y convenciones. Para el funcionamiento práctico debe existir al menos un intérprete o compilador que traduzca la instrucción del lenguaje propio del computador a otro accesible.
- **MENÚES.-** Mecanismo de ingreso de órdenes mediante teclado para dirigir la acción del computador. Los menúes están generalmente conformados por una serie de opciones o una letra asociada a ella. A diferencia de los comandos son necesarios datos adicionales para completar la especificación de la orden.
- **MÓDEM.-** Contracción de modulador. Equipo de comunicación que permite la transmisión de información entre computadoras por medio de líneas telefónicas.
- **OPERACIONES EN LINEA:** Habilita su tienda virtual a recibir múltiples opciones de pago para la venta de sus productos y/o servicios.
- **PROGRAMA DE APLICACIÓN.-** Conjunto de instrucciones sistematizadas que permiten al computador realizar tareas específicas.
- **SEGURIDAD INFORMATICA:** Podemos entender como seguridad un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los

resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

Integridad: La información sólo puede ser modificada por quien está autorizado.

a) **Confidencialidad**: La información sólo debe ser legible para los autorizados.

b) **Disponibilidad**: Debe estar disponible cuando se necesita.

c) **Irrefutabilidad**: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en seguridad lógica y seguridad física.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea robada.

- **SISTEMA BANCARIO:** Lo constituyen todas las instituciones financieras de depósito de un país, como los bancos, las cajas de ahorro, la banca oficial, las cooperativas de crédito y el banco central.
- **SISTEMA CREDITICIO:** Es el conjunto de instituciones de un país autorizadas y capacitadas para conceder créditos. En España está integrado por el Banco de España, el sistema bancario, y las entidades de crédito oficial.

- **SISTEMA FINANCIERO:** Así se define al conjunto de regulaciones, normativas, instrumentos, personas e instituciones que operan y constituyen el mercado de dinero y el mercado de capitales de un país. El sistema financiero está conformado por el conjunto de Instituciones bancarias, financieras y demás empresas e instituciones de derecho público o privado, debidamente autorizadas por la Superintendencia de Banca y Seguros, que operan en la intermediación financiera (actividad habitual desarrollada por empresas e instituciones autorizada a captar fondos del público y colocarlos en forma de créditos e inversiones
- **SISTEMA MONETARIO:** Tiene como función regular la liquidez de una economía, y está formado por el conjunto de instrumentos, instalaciones y reglas que rigen el mercado monetario de uno o varios países.
- **SISTEMA OPERATIVO.-** Conjunto de instrucciones que permiten la interacción entre el computador y el usuario. Controla el funcionamiento del computador, interpretando y ejecutando los comandos recibidos, dirigiendo la información a su destino.
- **SOFTWARE.-** Programa que controla el funcionamiento del computador y permite que el hardware realice las instrucciones dadas.

CAPÍTULO III

HIPÓTESIS

3.1 Hipótesis general

- Existe un impacto en las Empresas Bancarias, producto de los delitos informáticos.

3.2 Hipótesis específicas

- No encontramos una adecuada tipificación de los delitos informáticos, que aguarden íntima relación con las Empresas Bancarias?
- No Existe una clasificación adecuada de los delitos informáticos que afecten a las empresas Bancarias.
- La Empresa Bancaria es blanco de los delincuentes informáticos.

3.3. Variables e Indicadores

Variable Independiente:

Delitos Informáticos

Indicadores

- Acceso a una base de datos;
- Sabotaje Informático;
- Agravantes

Variable Dependiente:

Empresa Bancaria

Indicadores

- Derecho Bancario y Monetario;
- Los Contratos Empresariales Modernos;
- Derecho Penal Común y de la Empresa;
- Derecho Constitucional Económico.

3.4. Operacionalización de las variables

Variables	Definición conceptual	Definición Operacional	Indicadores	Escala de medición
Variable Independiente: Delitos Informáticos	Se considera como aquel acto tipificado, que se desarrolla por la utilización ilegal de medios informáticos, con la finalidad de abatir posibles sistemas de seguridad, de aparatos cibernéticos, computadoras.	Comisión de un delito, por uso de medios cibernéticos.	• Acceso a una base de datos; • Sabotaje Informático; • Agravantes	Nominal Nominal Nominal
Variable Dependiente: Empresa Bancaria	Entidad bancaria que asume la administración de dinero (clientes o usuarios) para otorgarla en préstamo a terceros; asimismo hace uso de mecanismos de seguridad, para dar garantías del dinero resguardado	Entidad financiera, que resguarda el dinero de terceros, para terceros, que debe de dar tanto seguridad material, como informática, conforme a los avances de la tecnología.	• Derecho Bancario y Monetario; • Los Contratos Empresariales Modernos; • Derecho Penal Común y de la Empresa; • Derecho Constitucional Económico.	Nominal Ordinal Ordinal Nominal

CAPÍTULO IV

METODOLOGÍA

4.1 Tipo de la investigación

La presente investigación, es elementalmente de tipo básica - descriptivo, puesto que nos conllevara a poder conocer con exactitud la problemática planteada, respecto del impacto que surte sobre las empresas bancarias, respecto de los delitos informáticos.

El enfoque que se le dará, es el cuantitativo, toda vez que se recolectara información, que pueda probar la hipótesis realizada.

4.2 Nivel de la investigación

El nivel de la presente investigación, según el tipo y enfoque, será de nivel descriptivo de enfoque cuantitativo; al determinarse esta metodología, se recolectaran datos que puedan describir la problemática planteada, respecto

del impacto que surten las empresas bancarias, con la comisión de delitos informáticos.

4.3 Método y diseño

4.3.1 Método de Investigación

El método utilizado fue el método dogmático porque se buscó hacer un análisis doctrinario del problema planteado, sobre los delitos informáticos, y su incidencia en las empresas bancarias; asimismo se hizo uso del método analítico, la realizarse un análisis del problema ante mencionado.

4.3.2 Diseño de la Investigación

La presente investigación, fue de diseño documental, toda vez que se hizo un análisis e interpretación de las fuentes de información mencionadas, que sirvieron de fundamento para la investigación planteada.

4.4 Población y Muestra.

Población:

La población está conformada por los fiscales y jueces de la Corte Superior de Justicia de Lima.

Muestra:

Por ser una población relativamente pequeña, se considerara a 40 personas, entre jueces y fiscales como muestra; se debe tener en cuenta que la muestra señalada es no probabilística.

Muestreo:

El tipo de muestro, se realizó a modo de muestra enfocada, es decir a los jueces y fiscales de la Corte Superior de Justicia de Lima.

a. Jueces Penales : 20
b. Fiscales Penales : 20

4.5 Técnicas e instrumentos de recolección de datos

4.5.1 Técnicas de recolección de datos:

Técnica de encuesta

La misma que se utilizó para recabar información de manera anónima. La finalidad de la encuesta, es obtener datos de diferentes personas. Es necesario indicar que las encuestas fueron realizadas de modo impersonal, pues no se designas los datos de los encuestados, toda vez que ello no es de suma importancia.

Técnica documental

Por medio de la cual se hizo un análisis de documentos, libros, trabajos, revistas y otros, que contienen información importante, sobre nuestro tema de investigación.

4.5.2 Instrumentos de recopilación de datos:

Técnica de cuestionario

Por medio de la cual, se elabora un cuestionario íntimamente relacionado por las hipótesis planteadas, hipótesis general, e hipótesis específicas, en un orden adecuado, a fin de poder realizar un análisis correspondiente.

Ficha bibliográfica

Por medio de la cual, se hace un esquema de los datos obtenidos, sean estos físicos o digitales, y en consecuencia, poder realizar las citas correspondientes.

4.5.3. Técnicas de análisis y procesamiento de datos

Es preciso indicar, que el método de análisis de datos, fue el de análisis cuantitativo; a través de un programa de computo.

Técnicas de análisis de datos: Una vez obtenidos los datos finales, estos serán transmitidos a una matriz u guardada en un archivo digital; los cuales fueron analizados de manera manual, y computarizada, haciendo uso al programa EXCEL.

Asimismo se hizo uso de análisis documental, por medio de cual se hizo un análisis de documentos físicos y virtuales, que coadyuvaron a poder validar las hipótesis planteadas.

Técnicas de procesamiento de datos: es específico, fue utilizado el programa Excel, que por medio de formular, coadyuvo a identificar los datos y porcentajes, a fin de realizar una adecuada interpretación.

4.6. Presentación de Datos.

La presentación de datos se efectuara de la siguiente manera:

Cuadros estadísticos

Mediante los cuales, se presenta datos de manera ordenada, facilitando su lectura y análisis.

Gráficas y barras rectangulares

Que demuestran de manera dinámica, los porcentajes obtenidos.

CAPITULO V

RESULTADOS DE LA INVESTIGACIÓN

5.1 Análisis e interpretación

Fundamentadas las bases teóricas, y metodológicas, respecto del impacto que pueda surtir a las empresas bancarias, respecto de los delitos informáticos, que usualmente son víctimas, como parte del presente trabajo de investigación, es necesario someter a validación nuestras hipótesis planteadas.

Como lo indicamos en el punto, universo, población y muestra, correspondió realizar 40 encuestas, entre jueces y fiscales especializados en derecho penal, con competencia en la Corte Superior de Justicia de Lima.

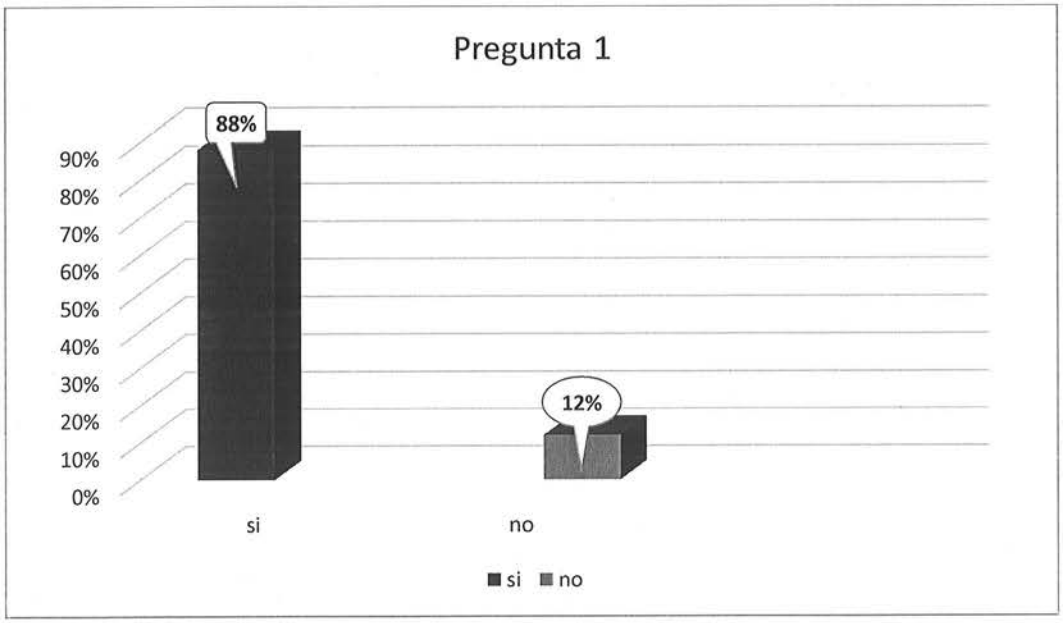
En ese sentido, los siguientes cuadros y gráficos, presentaran los resultados obtenidos, una vez aplicada la encuesta, que estarían confirmando las hipótesis planteadas, tanto la general, como las específicas; conforme a las interpretaciones que pudieron realizarse.

5.2 Análisis de estadísticas

Pregunta 1

¿Conoce Ud. que los impactos que puedan tener la comisión de delitos informáticos, respecto de las empresas bancarias?

Item	Frecuencia	Porcentaje
Si	35	88%
No	5	12%
Total	40	100%

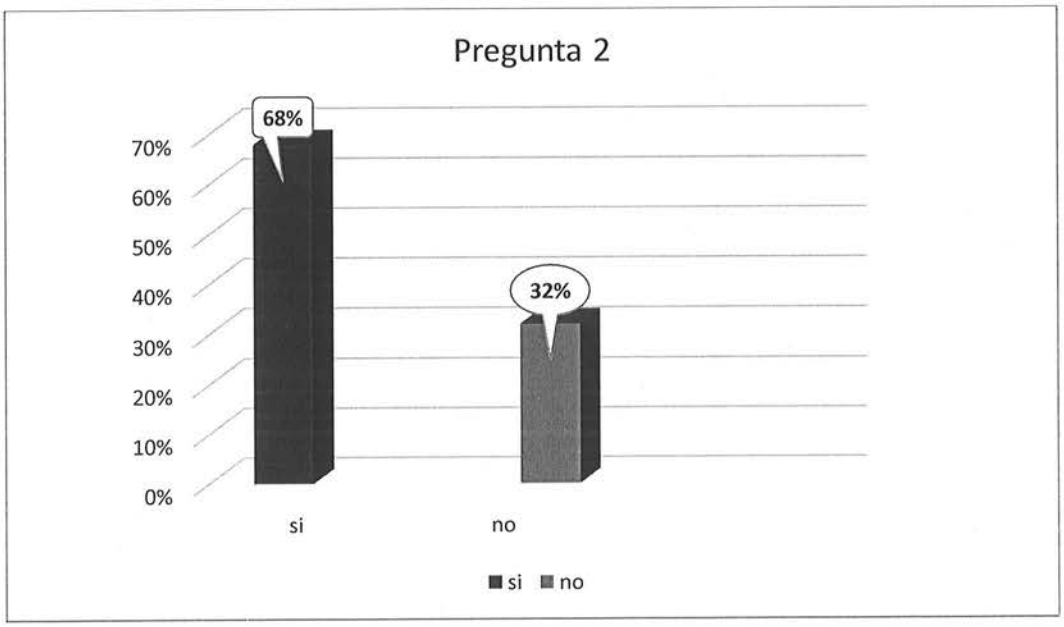


Del total de encuestados, 35 (88%) creen de que existen serios impactos a la empresa bancaria, la comisión de delitos informáticos, mientras que 5 (12%) considera que no es así.

Pregunta 2

¿Considera Ud. que la comisión de delitos informáticos, generan impactos económicos, respecto de las empresas bancarias?

Item	Frecuencia	Porcentaje
Si	27	68%
No	13	32%
Total	40	100%

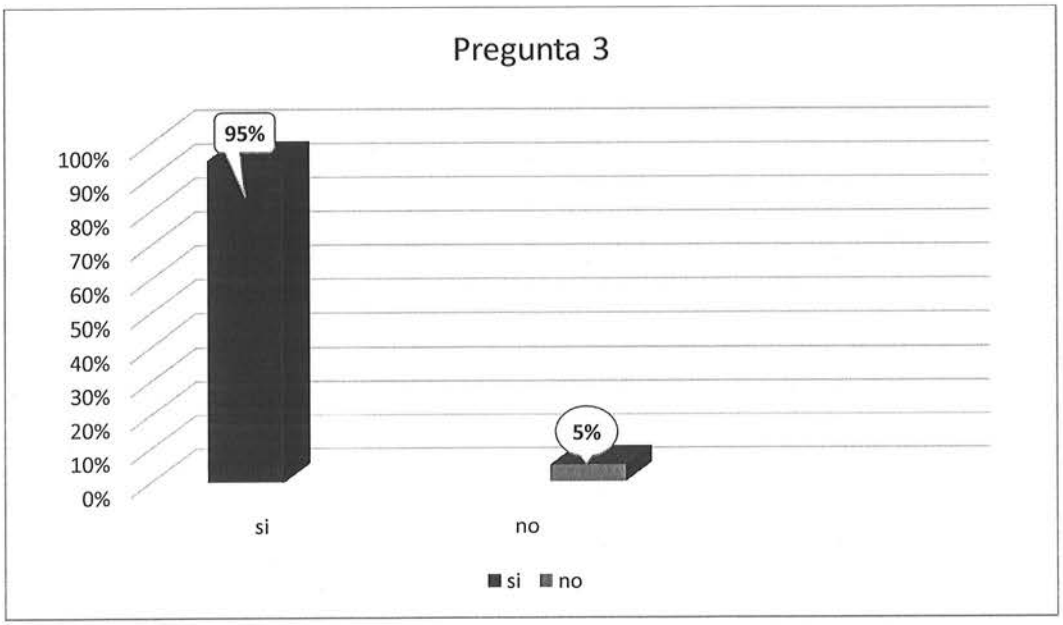


Del total de encuestados, 27 (68%) creen de que la comisión de delitos informáticos generan serios impactos económicos a la empresa bancaria, mientras que 13 (32%) considera que no es así.

Pregunta 3

¿Considera Ud. que la comisión de delitos informáticos, ejerce impactos sociales, respecto de las empresas bancarias?

Item	Frecuencia	Porcentaje
Si	38	95%
No	2	5%
Total	40	100%

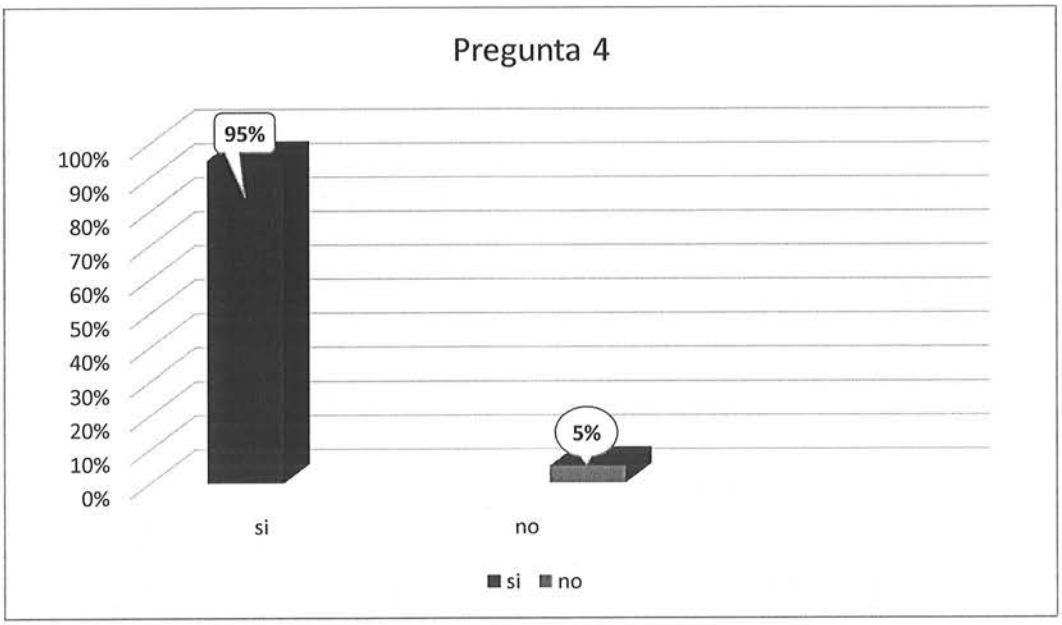


Del total de encuestados, 38 (95%) creen de que la comisión de delitos informáticos generan serios impactos sociales a la empresa bancaria, mientras que 2 (5%) considera que no es así.

Pregunto 4

¿Considera Ud. que la comisión de delitos informáticos, ejercería un impacto en la estabilidad jurídica de la empresa bancaria?

Item	Frecuencia	Porcentaje
Si	35	88%
No	5	12%
Total	40	100%

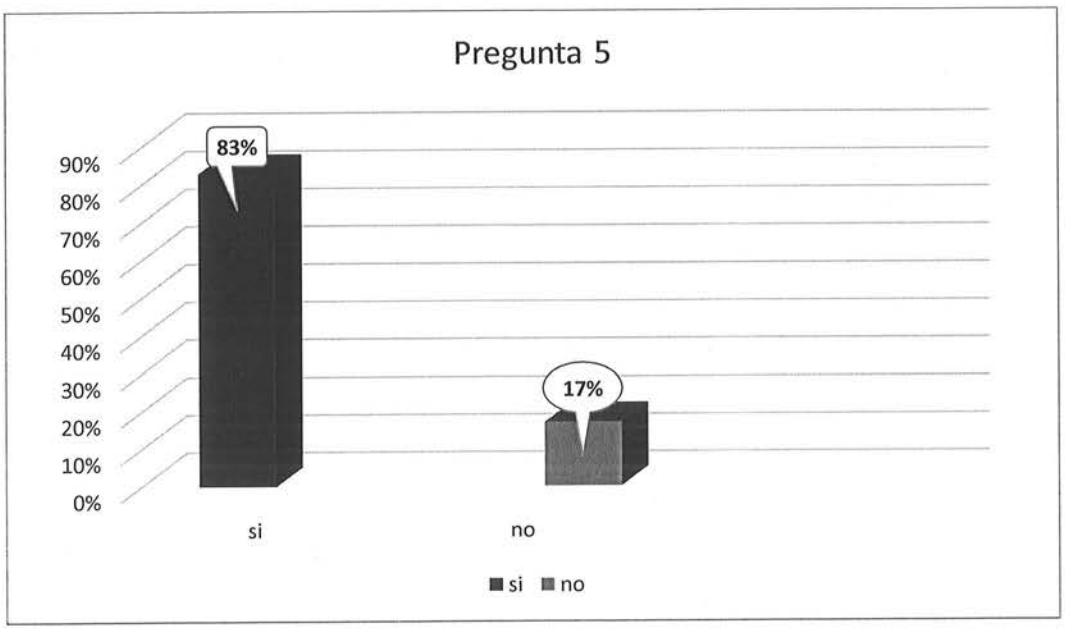


Del total de encuestados, 38 (95%) creen de que la comisión de delitos informáticos generan serios impactos sociales a la empresa bancaria, mientras que 2 (5%) considera que no es así.

Pregunta 5

¿Considera Ud. que la comisión de delitos informáticos, ejercería un impacto en la estabilidad económica de la empresa bancaria?

Item	Frecuencia	Porcentaje
Si	33	83%
No	7	17%
Total	40	100%

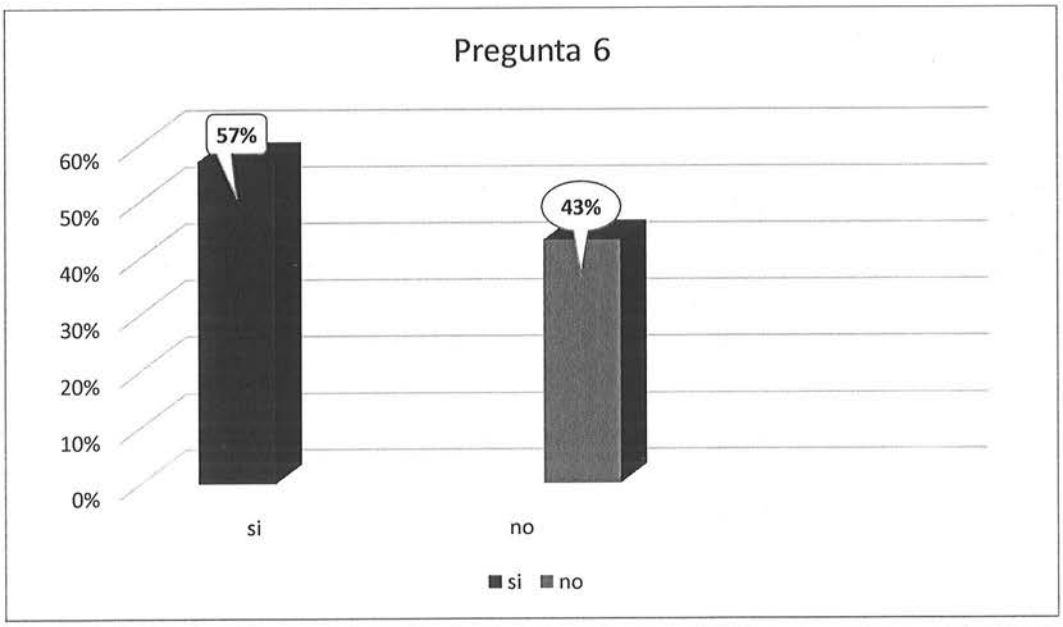


Del total de encuestados, 33 (83%) creen de que la comisión de delitos informáticos ejercería un impacto en la estabilidad económica de la empresa bancaria, mientras que 7 (17%) considera que no es así.

Pregunta 6

¿Cree Ud. que la tipificación de los delitos informáticos, coadyuvan a una defensa efectiva de bien jurídico protegido?

Item	Frecuencia	Porcentaje
Si	23	57%
No	17	43%
Total	40	100%

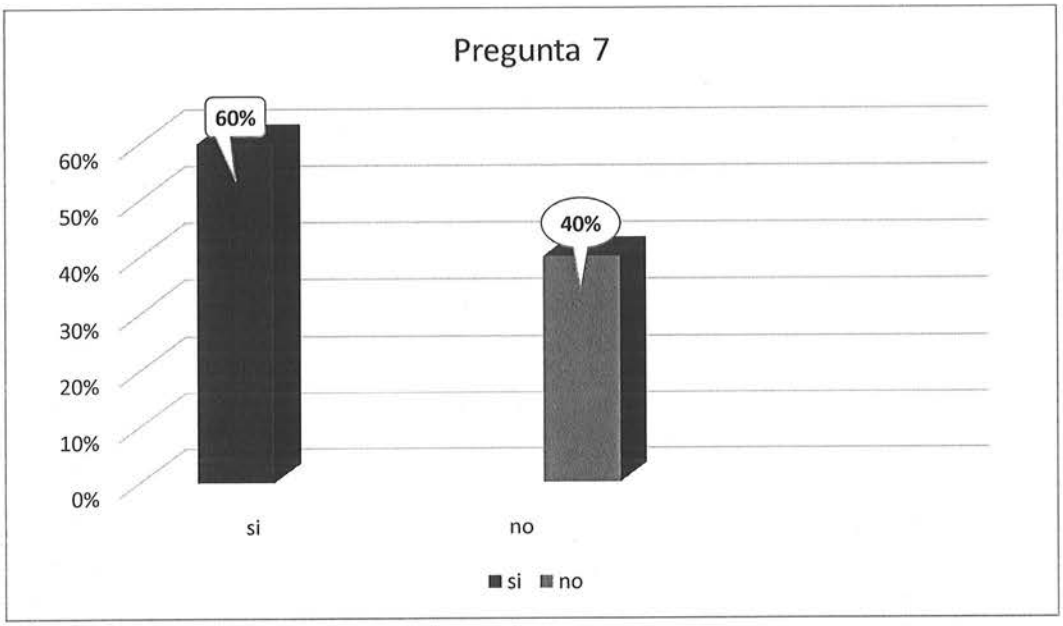


Del total de encuestados, 23 (57%) creen de que la tipificación de los delitos informáticos coadyuvan a una defensa efectiva de los bienes jurídicos protegidos, mientras que 17 (43%) considera que no es así.

Pregunta 7

¿Considera Ud. que la tipificación de los delitos informáticos, son utilizados válidamente por el persecutor del delito (Ministerio Publico - Fiscal)?

Item	Frecuencia	Porcentaje
Si	24	60%
No	16	40%
Total	40	100%

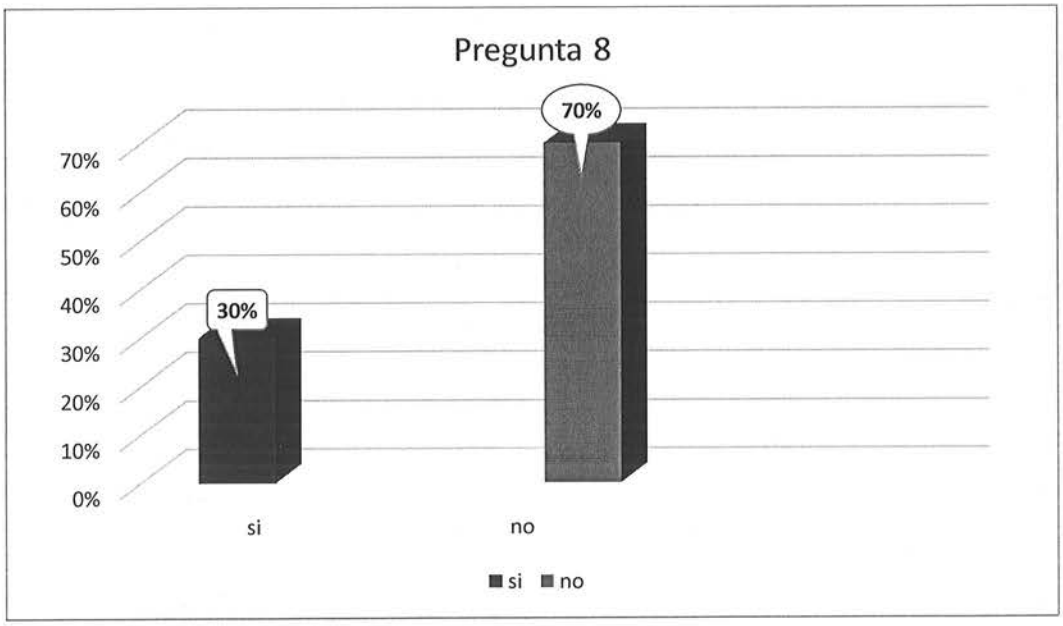


Del total de encuestados, 24 (60%) creen de que la tipificación de los delitos informáticos, son utilizados válidamente por el persecutor del delito (Ministerio Publico - Fiscal), mientras que 16 (40%) considera que no es así.

Pregunta 8

¿Cree Ud. que existe una adecuada clasificación de los delitos informáticos que afecten a las empresas bancarias?

Item	Frecuencia	Porcentaje
Si	12	30%
No	28	70%
Total	40	100%

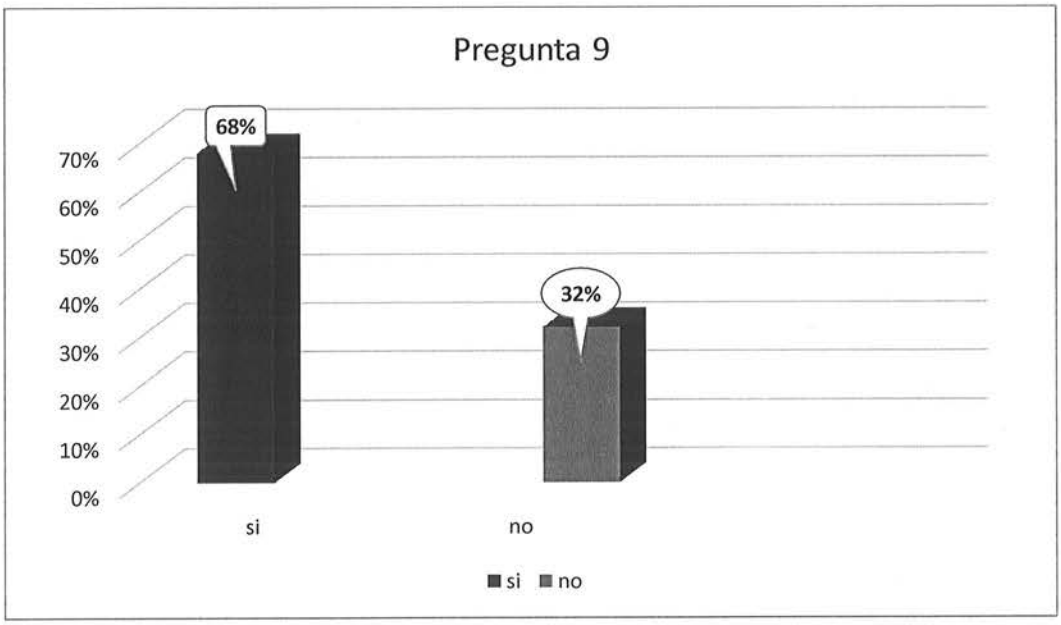


Del total de encuestados, 28 (70%) creen de que no existe una adecuada clasificación de los delitos informáticos que afecten a las empresas bancarias, mientras que 12 (30%) considera que sí.

Pregunta 9

¿Piensa Ud. que las empresas bancarias son presa fácil de los delincuentes informáticos?

Item	Frecuencia	Porcentaje
Si	27	68%
No	13	32%
Total	40	100%

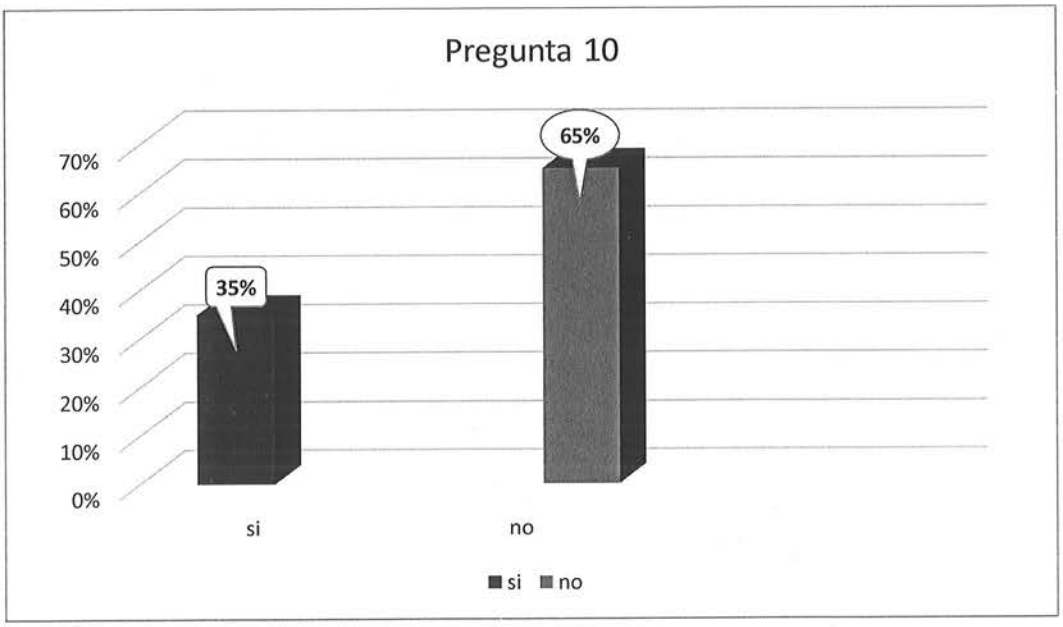


Del total de encuestados, 27 (68%) creen de que las empresas bancarias son presa fácil de los delincuentes informáticos, mientras que 13 (32%) considera que no es así.

Pregunta 10

¿Cree Ud. que el software de seguridad bancaria, son efectivos ante la delincuencia informática?

Item	Frecuencia	Porcentaje
Si	14	35%
No	26	65%
Total	40	100%

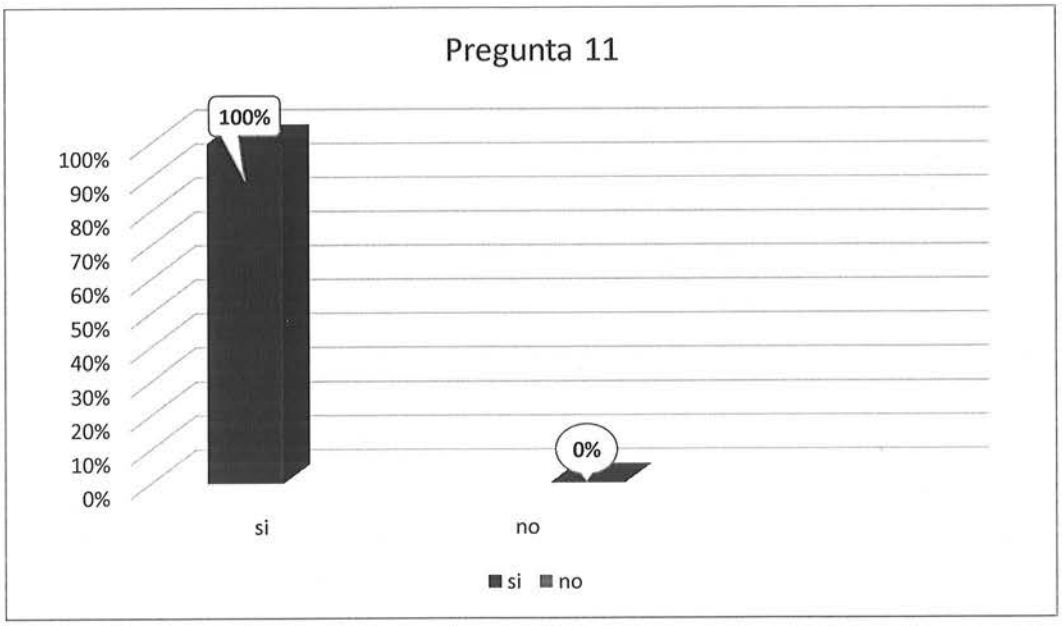


Del total de encuestados, 26 (65%) creen de que el software de seguridad bancaria, no son efectivos ante la delincuencia informática, mientras que 14 (35%) considera que si es así.

Pregunta 11

¿Cree Ud. que los bancos deben de responder a sus clientes, por las pérdidas generadas consecuencia de los delincuentes informáticos?

Item	Frecuencia	Porcentaje
Si	40	100%
No	0	0%
Total	40	100%

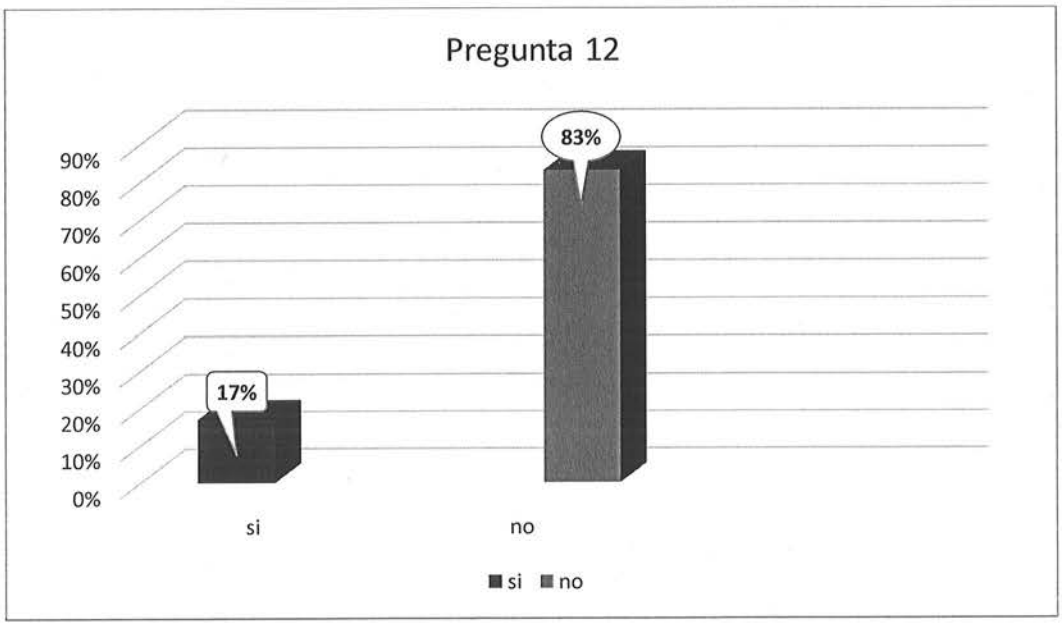


Del total de encuestados, 40 (100%) creen de que los bancos deben de responder a sus clientes, por las pérdidas generadas consecuencia de los delincuentes informáticos.

Pregunta 12

¿Cree Ud. que se requiere una normativa específica sobre delitos informáticos?

Item	Frecuencia	Porcentaje
Si	7	17%
No	33	83%
Total	40	100%



Del total de encuestados, 33 (83%) no creen de que se requiere una normativa específica sobre delitos informáticos, mientras que 7 (17%) considera que si se requiere.

5.3. Discusión de Resultados

Luego de haber revisado los resultados, graficados los mismos, y habiendo realizado el análisis correspondiente hemos podido denotar que un número alto de encuestados, considera que los delitos informáticos, generan un impacto económico y social a las empresas bancarias, económico respecto que le puede generar pérdidas económicas, es aquí donde se ha podido denotar procesos penales respecto del tema, en el aspecto social, todos refieren de la credibilidad de la empresa bancaria frente a la sociedad, y lo está piensa sobre la empresa bancaria, luego de verse perjudicados con su dinero o transacciones.

Consecuencia de lo anterior, es posible afirmar que los delitos informáticos, generarían impactos en la estabilidad jurídica de la empresa, ello según lo manifestado por el 88% de los encuestados; según afirman que los delitos informáticos, inmiscuirían a las empresas en diferentes procesos judiciales, tanto civiles como penales, lo cual lógicamente generaría una inestabilidad jurídica.

Existen posiciones de que la finalidad del derecho penal es preventiva, a fin de prever posibles afectaciones, sin embargo, ante la pregunta de si la tipificación de los delitos informáticos, coadyuvan a una defensa efectiva del bien jurídico protegido, existe un debate y discusión, pues el 57% (23) consideran que si dan protección efectiva, sin embargo un 43% (17) consideran que no es así, pues el determinar un delito informático, es complicado, y la solo tipificación no protege el bien jurídico, sino que igual se siguen cometiendo actos ilícitos, relacionados al tema. Es así que se planteó

la pregunta de que si los persecutores del delitos, cumplen una labor efectiva al momento de perseguir los delitos informáticos, para lo cual el 60% (24) consideran que es así, debemos entender que la mitad de los encuestados están en función al Ministerio Público, el 40% (16) consideran que no cumplen con una labor efectiva, estos consideran, que es por la falta de especialización de los fiscales, en estos temas, y que en el constante cambio de la tecnología y las herramientas con las que cuenta el Ministerio Público, para perseguir estos delitos.

Uno de los puntos de mayor relevancia, es si se considera a las empresas bancarias como presa fácil, para la comisión de delitos informáticos, el 68% (27) consideran que es así, manifestando que en todo el mundo grandes empresas del sistema financiero, se ven afectas a los delitos informáticos, y por ello sus sistema de seguridad están todo el tiempo vigilados por los mejores ingenieros de sistemas; lo cual escapa a las empresas bancarias del Perú.

La responsabilidad de las empresas bancarias, es justificada, al ser ellos quienes presten servicios, y ante afectaciones, son ellos quienes deberían de incurrir en responsabilidad, y reparar el daño surtido; ello ha sido establecido por el 100% (40) encuestados, en ello no hay debate alguno.

Por último, se realizó una interrogante, respecto si sería necesario encontrar una normativa, específica sobre delitos informáticos, así como la hay en los delitos aduaneros, el 83% (33) de los encuestados, consideran que no es necesaria una normativa específica, toda vez que el Código Penal, es la normativa que debería de contener todos los delitos, tener normativas

diferentes, conllevaría a tener un sistema multiregulatoria, que conllevaría a no manejar de manera adecuada el sistema penal.

CONCLUSIONES

En ese sentido, y en base a la investigación realizada, sobre los delitos informáticos, y sus impactos en las empresas bancarias, hemos podido denotar, las siguientes conclusiones:

1) Conforme a lo recabado en tanto al marco teórico, como en las encuestas, hemos podido identificar que los delitos informáticos, surten un impacto económico y social en las empresas bancarias, asimismo surte un impacto en su estabilidad jurídica. Primero, surte un impacto económico, respecto de las pérdidas que estas generan a la empresa, así como las pérdidas que se generan a los clientes de estas empresas, consecuencia de ello, es el impacto social que se tiene, pues lo clientes asumen una desconfianza en las empresas bancarias, lo cual a largo plazo podría generar pérdidas a las empresas bancarias. Las inestabilidad jurídica que podría generarse, se basa en los procesos civiles y penales que se podrían generar, ello ante el agravio de los clientes, quienes desconfiados podrían iniciar algún tipo de proceso a las empresas bancarias; lo cual en suma podría generar grandes pérdidas para las empresas, sobre todo en sus activos; si bien es cierto, las empresas pueden contar con seguros, estas no necesariamente serán suficientes para reparar los daños cometidos.

2) Se ha podido denotar sobre todo de las encuestas, que no existe un adecuado sistema normativo sobre delitos informáticos, es decir la existente no es suficiente para tutelas los derechos de las empresas bancarias, sin embargo hemos podido denotar que no se requiere una

normativa específica, es decir una ley especial, ello según criterio de los encuestados, toda vez que ello, conllevaría a la creación de un sistema multiregulatoria, que en lugar de dar estabilidad, surtiría cierta indiferencia al momento de iniciar los procesos judiciales.

3) Consecuencia de la anterior conclusión, es la clasificación inadecuada que se tiene de los delitos informáticos, que afecten a las empresas bancarias, debemos entender que las empresas bancarias son entidades que resguardan el dinero, capital y ahorros de muchas personas; y lo delitos que se cometen contra estas son en suma muy específicos, y denotarlo solo como hurto, o como robo, no identificaría en específico la comisión del delito; por ello es necesario una identificación adecuada en el Código Penal.

4) La modernidad ha conllevado a la creación de diferentes software que brinden seguridad, no solo a las empresas bancarias, sino a todas las empresas que puedan mover fuertes capitales, sin embargo con ello los llamados hackers, a previsto estos software de seguridad y denotando las falencias, han podido violentar estos sistemas de seguridad, y en consecuencia hacer uso ilegal de su conocimiento, a fin de obtener supuestas ganancias, que no solo afectan a las empresas bancarias, sino también a sus usuarios.

RECOMENDACIONES

Conforme las conclusiones, se puede llegar a las siguientes recomendaciones:

1) Un sistema multiregulatorio penal, conlleva a que la sociedad civil tena desconocimiento de la normativa vigente, si bien es cierto, se dice que la sola publicación en el diario el peruano, conlleva a que las personas civiles, conozcan de las normas, y no puedan alegar su pleno desconocimiento, encontrar diferentes leyes que tipifiquen los delitos sería erróneo, pues tenemos el Código Penal, normatividad que debe de contener todos los actos tipificados como delitos, en ese sentido, se recomienda la unificación normativa de delitos.

2) La aplicación de la ley de delitos informáticos, no se ha podido dar de manera valida y efectiva, pese a las observaciones que se le han podido hacer, siendo necesaria modificaciones, teniendo en cuenta las evidencias empíricas, que puedan tener los jueces y fiscales especializados en la materia, quienes han de aplicar las normas.

3) Es necesario, que el estado, por medio de sus instituciones insten a la población a que pueda conocer este tipo de delitos, a fin de que no puedan incurrir en los mismos, todos sabemos que existen

lugares donde venden y ofrecen estos servicios, nos referimos a infringir sistemas de seguridad, y las personas recurren a estos lugares, sin conocer plenamente que podrían cometer un delito; y es deber del estado, informar a la población, no solamente con la publicación en un diario, sino también mediante programas informativos.

VI. REFERENCIAS BIBLIOGRÁFICAS

ABALOS, M., ABBIATI, J., & OTROS. (2002). *Derecho a la Información, Hábeas Data e Internet.* Buenos Aires: Editorial La Rocca.

ARMAGNAGUE, J. (2002). *Derecho a la Información, Habeas Data e Internet.* Buenos Aires: Editorial La Rocca.

BIDART CAMPOS, G. (1988). *Tratado Elemental del Derecho Constitucional Argentino.* Buenos Aires : Editorial Ediar.

BLOSSIER MAZZINI, J. J. (2008). Los Delitos Informáticos y la Banca Electrónica. *Revista ABOGADOS*(8).

Chavez, G. (10 de Junio de 2014). *Expansión*. Recuperado el 15 de Febrero de 2018, de Expansion en Alianza: https://expansion.mx/tecnologia/2014/06/09/bancos-pierden-93-mdd-en-fraude-online

Congreso Constituyente Democrático . (29 de Diciembre de 1993). Constitución Política del Perú . Lima, Lima, Perú .

Convenio de Budapest. (23 de Noviembre de 2001). Convenio sobre la cibercriminalidad . Budapest, Hungría.

Dávila Laguna, W. (15 de Enero de 2017). *Resultado Legal.* Obtenido de http://resultadolegal.com/%EF%BB%BFdelitos-informaticos-peru/

Fernández Villegas, C. B., Vivanco Quinto, R., & Vara Morocco, A. (30 de Junio de 2018). *Facultad de Derecho USMP.* Obtenido de http://www.derecho.usmp.edu.pe/cedetec/articulos/DELITOS_INFORMATICOS.pdf

Grisanti A., H. (1989). *Lecciones de Derecho Penal.* Caracas: Móbil Libros .

IASONI, M. (2002). *Comercio Electrónico, Aspectos Legales: Un Desafío para el Derecho Peruano.* Lima: Editorial Portocarrero.

Ley de Delitos Informaticos. (21 de Octubre de 2013). Ley N° 30096. Lima, Lima, Perú: El Peruano. Recuperado el 15 de Febrero de 2018, de http://www.derecho.usmp.edu.pe/cedetec/normas/Ley_Delitos_Informaticos_Ley_30096.pdf

Ley General de Propiedad Industrial . (26 de Diciembre de 1992). Decreto Ley N° 26017. Lima, Lima, Perú: EL Peruano.

Ley sobre Represión de la Competencia Desleal. (29 de Diciembre de 1992). Decreto Ley N° 26122. Lima, Lima, Perú: El Peruano .

Motessi, C. (14 de Noviembre de 2017). *otrawebdetecno.* Recuperado el 15 de Enero de 2018, de https://otrawebdetecno.com/:

https://otrawebdetecno.com/2017/11/14/convenio-de-budapest-argentina-busca-adherir-al-tratado-sobre-ciberdelincuencia/

Peña Cabrera, R. (1997). *Tratado de Derecho Penal. Estudio Programatico de la Parte General.* Lima: Editorial Grijley.

Redacción Gestión. (25 de Febrero de 2014). *Gestión*. Recuperado el 13 de Marzo de 2018, de Diario Gestión Web: https://gestion.pe/tecnologia/fraudes-internet-duplican-latinoamerica-brasil-afectado-4981?ref=gesr

Warren, S. D., & Brandeis, L. D. (1981). The Right to Privacy in Nineteenth Century America. *Harvard Law Review*, 1982 - 1910.

ANEXOS

MATRIZ DE CONSISTENCIA				
PROBLEMAS DE INVESTIGACIÓN	**OBJETIVOS DE INVESTIGACIÓN**	**HIPOTESIS DE INVESTIGACIÓN**	**VARIABLES O INDICADORES**	**METODOLOGÍA**
PROBLEMA GENERAL ¿Cuál es el impacto de los delitos informáticos en la Empresa Bancaria? **PROBLEMAS ESPECÍFICOS** ▪ ¿En qué medida se encuentran tipificados los delitos informáticos, que afecten directamente a las Empresas Bancarias? ▪ ¿Existe una clasificación adecuada de los delitos informáticos	**OBJETIVO GENERAL** Determinar cuál es el impacto de los delitos informáticos en la Empresa Bancaria. **OBJETIVOS ESPECÍFICOS** ▪ Evaluar en qué medida se encuentran tipificados los delitos informáticos, que afecten directamente a las Empresas Bancarias. ▪ Evaluar si existe una clasificación adecuada de los delitos informáticos que afecten a las empresas Bancarias.	**HIPÓTESIS GENERAL** Existe un impacto en las Empresas Bancarias, producto de los delitos informáticos. **HIPÓTESIS ESPECÍFICAS** ▪ No encontramos una adecuada tipificación de los delitos informáticos, que aguarden íntima relación con las Empresas Bancarias? ▪ No Existe una clasificación adecuada de los delitos informáticos que afecten a las empresas Bancarias.	**Variable Independiente:** Delitos Informáticos **Indicadores** - Acceso a una base de datos - Sabotaje Informático - Agravantes **Variable Dependiente:** Banca Empresarial **Indicadores**	**TIPO DE LA INVESTIGACIÓN** Básico – descriptivo de enfoque cuantitativo. **NIVEL DE LA INVESTIGACIÓN** Descriptivo – Cuantitativo. **MÉTODO DE INVESTIGACIÓN** Método dogmático – analítico. **DISEÑO DE LA INVESTIGACIÓN** Documental **MUESTRAS** La muestra de este trabajo de investigación es no probabilística. **TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS** **Técnicas de recolección de datos:** •Revisión documental

que afecten a las empresas Bancarias? ▪ ¿De qué manera la Empresa Bancaria es blanco de los delincuentes informáticos?	▪ Determinar de qué manera la Empresa Bancaria es blanco de los delincuentes informáticos.	▪ La Empresa Bancaria es blanco de los delincuentes informáticos.	- Derecho Bancario y Monetario. - Los Contratos Empresariales Modernos. - Derecho Penal Común y de la Empresa. - Derecho Constitucional Económico.	•Cuestionario **<u>Instrumentos de recopilación de datos:</u>** • Formato de Encuestas • Ficha bibliográfica

ANEXO N° 2

Ficha de Encuestas

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL

ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE ENCUESTA PARA TESIS DE MAESTRIA

"EL DELITO INFORMATICO Y SU INCIDENCIA EN LA EMPRESA BANCARIA"

Estimado Sr (a), soy el Bachiller **BLOSSIERS MAZZINI, JUAN JOSÉ** y he culminado mis estudios de Magister, abocándome a la ejecución de mi Tesis, motivo por el cual recurro a Ud. para que tenga a bien responder la presente encuesta.
Los datos que Ud. consigne serán tratados con la debida reserva y confidencialidad, no serán entregados a las autoridades o persona alguna. MUCHAS GRACIAS.

OBJETIVO DE LA ENCUESTA: Realizar la Tesis de Maestría.

Encuestador: **Abog. BLOSSIERS MAZZINI, JUAN JOSÉ**

Sírvase contestar las preguntas planteadas de acuerdo a la opción que considere conveniente:

Cuestionario

1. ¿Conoce Ud. que los impactos que puedan tener la comisión de delitos informáticos, respecto de las empresas bancarias?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

2. ¿Considera Ud. que la comisión de delitos informáticos, generan impactos económicos, respecto de las empresas bancarias?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

3. ¿Considera Ud. que la comisión de delitos informáticos, ejerce impactos sociales, respecto de las empresas bancarias?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

4. ¿Considera Ud. que la comisión de delitos informáticos, ejercería un impacto en la estabilidad jurídica de la empresa bancaria?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

5. ¿Considera Ud. que la comisión de delitos informáticos, ejercería un impacto en la estabilidad económica de la empresa bancaria?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

6. ¿Cree Ud. que la tipificación de los delitos informáticos, coadyuvan a a una defensa efectiva de bien jurídico protegido?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

7. ¿Considera Ud. que la tipificación de los delitos informáticos, son utilizados válidamente por el persecutor del delito?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

8. ¿Cree Ud. que existe una adecuada clasificación de los delitos informáticos que afecten a las empresas bancarias?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

9. ¿Piensa Ud. que las empresas bancarias son presa fácil de los delincuentes informáticos?

   a) SI b) NO c) NO SABE / NO OPINA

   Precise:.....

   .....

   .....

10. ¿Cree Ud. que el software de seguridad bancaria, son efectivos ante la delincuencia informática?

    a) SI b) NO c) NO SABE / NO OPINA

    Precise:.....

    .....

    .....

11. ¿Cree Ud. que los bancos deben de responder a sus clientes, por las pérdidas generadas consecuencia de los delincuentes informáticos?

    a) SI b) NO c) NO SABE / NO OPINA

    Precise:.....

    .....

    .....

12. ¿Cree Ud. que se requiere una normativa específica sobre delitos informáticos?

    a) SI b) NO c) NO SABE / NO OPINA

    Precise:.....

    .....

    .....

Nota: Tenga la bondad de marcar con un X la respuesta que considere pertinente.