VICERRECTORADO ACADÉMICO

ESCUELA DE POSGRADO

TESIS

"LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE PREVENCIÓN DE LOS DELITOS INFORMÁTICOS EN EL PERÚ, EN LOS AÑOS 2017 Y 2018"

PRESENTADO POR:

MG. FERNANDO MARTÍN ROBLES SOTOMAYOR.

PARA OPTAR EL GRADO ACADÉMICO DE
DOCTOR EN DERECHO

LIMA - PERÚ

2018

VICERRECTORADO ACADÉMICO

ESCUELA DE POSGRADO

TÍTULO DE LA TESIS

"LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE PREVENCIÓN DE LOS DELITOS INFORMÁTICOS EN EL PERÚ, EN LOS AÑOS 2017 Y 2018"

LÍNEA DE INVESTIGACIÓN

DERECHO CONSTITUCIONAL – DERECHOS FUNDAMENTALES

DERECHO PENAL – DELITOS Y FALTAS

ASESOR

Dr. JOSÉ ANTONIO RODRÍGUEZ ULLOA

DEDICATORIA

A Carmen, mi esposa, por su indesmayable y permanente apoyo y amor.
A Luis, mi padre, quién desde el cielo sigue estando orgulloso de cada logro personal y profesional que alcanzo.
A Marina, mi madre, por su eterno amor y comprensión hacia este hijo aventurero.
A mis hijos Rosa, Richard y Diana, que engrandecen mi vida y me otorgan mayores motivos de superación.

AGRADECIMIENTO

A la Universidad Alas Peruanas y sus distintas autoridades, que me han permitido ser parte integrante de esta gran alma mater.

A mis colegas y amigos Fedatarios Juramentados con Especialización en Informática, que desinteresadamente han aportado sus ilustradas opiniones sobre el tema de esta Tesis y han sido el público en que se ha basado la investigación.

A mis alumnos y exalumnos de pre y postgrado de las Universidades Alas Peruanas, Continental, Científica del Perú y Peruana del Oriente, que con su entusiasmo me obligan a aprender cada día más en las especialidades del Derecho Informático e Informática Jurídica.

RECONOCIMIENTO

Al Dr. José Antonio Rodríguez Ulloa, excelente abogado y docente que tempranamente ha sido llamado a los brazos del Señor, por su desinteresada asesoría, en la elaboración del presente trabajo de Tesis.

A los Dres. Wander Saúl Muñoz Pantigoso, Kennedy Peter Pacheco Montes, Vladymir Villarreal Balbín y Roger Cabrera Paredes que con su experiencia y conocimiento han validado la confiabilidad de mi instrumento de investigación.

A los docentes y jurados de la Universidad Alas Peruanas, por sus enseñanzas y orientaciones para alcanzar el grado académico de Doctor.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

La tesis titulada "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú, en los años 2017 y 2018", es un trabajo de investigación para optar el grado de Doctor en Derecho, que busca determinar la relación causal entre la Protección de Datos Personales y los Delitos Informáticos, aplicándose la investigación en especialistas en la materia, es decir especialistas en Derecho Informático, que son abogados especializados e inscritos en el Ministerio de Justicia, como Fedatarios Juramentados con Especialización en Informática.

El objetivo principal de la investigación es "Determinar si la Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú", para ello el tipo de la investigación es básica - transversal, el método de investigación a aplicar es el deductivo - inductivo - dogmático, siendo su nivel el explicativo y su diseño el no experimental – transversal - causal, la técnica utilizada para reunir la información es la encuesta y el instrumento para el recojo de información es el cuestionario aplicado a una muestra de 57 especialistas en Derecho Informático, que son abogados especializados e inscritos en el Ministerio de Justicia, como Fedatarios Juramentados con Especialización en Informática, de una población total de 135 –a Enero de 2017– profesionales del Derecho con esa especialidad.

Los resultados obtenidos coinciden y se complementan con la información teórica nacional y extranjera obtenida de otros estudios relacionados, lo que ha permitido confirmar la hipótesis general, en el sentido de que la Protección de Datos Personales sí se relaciona en forma directa con la prevención de los Delitos Informáticos en el Perú, así como las hipótesis específicas, en las cuales se establece la relación entre el titular de los datos y su exposición que facilita a los delincuentes informáticos su uso, así como los mecanismos que provee la Ley de Protección de Datos Personales (Ley N° 29733) para coadyuvar en la prevención, de cada uno de los delitos tipificados en la Ley de Delitos Informáticos (Ley N° 30096), generándose una serie de recomendaciones a partir de las conclusiones obtenidas en la presente investigación.

PALABRAS CLAVE

- Protección de Datos Personales.
- Delito Informático.
- Dato Personal
- Dato Sensible
- Dato Informático
- Sistema Informático
- Constitución.
- Ley.
- Derecho.

ABSTRACT

The thesis entitled "The Protection of Personal Data as a Means of Prevention of Computer Crimes in Peru, in the years 2017 and 2018", is a research work to choose the degree of Doctor of Law, which seeks to determine the causal relationship between the Protection of Personal Data and Computer Crimes, applying research in specialists in the field, ie specialists in Computer Law, who are specialized lawyers and registered in the Ministry of Justice, as Sworn Federates with Specialization in Information Technology.

The main objective of the research is "To determine if the Protection of Personal Data is related to the prevention of computer crimes in Peru", for this the type of research is basic - transversal, the research method to be applied is the deductive - inductive - dogmatic, its level being the explanatory and its design the non-experimental - transversal - causal, the technique used to gather the information is the survey and the instrument for the collection of information is the questionnaire applied to a sample of 57 specialists in Computer Law, which are specialized lawyers and registered in the Ministry of Justice, as Sworn Federations with Specialization in Computer Science, from a total population of 135 - January 2017 - Law professionals with that specialty.

The results obtained coincide and are complemented by national and foreign theoretical information obtained from other related studies, which has allowed confirming the general hypothesis, in the sense that the Protection of Personal Data is related to the prevention of Computer Crimes in Peru, as well as the specific hypotheses, in which the relationship between the data subject and his exposure is established, which facilitates the use of data by computer criminals, as well as the mechanisms provided by the Personal Data Protection Law (Law No. 29733) to assist in the prevention of each of the crimes defined in the Computer Crimes Act (Law No. 30096), generating a series of recommendations based on the conclusions obtained in the present investigation.

KEYWORDS

- Personal data protection.
- Cybercrime.
- Personal Data
- Sensible data
- Computer Data
- Computer system
- Constitution.
- Law.

RESUMEN EN UN TERCER IDIOMA (PORTUGUÉS)

RESUMO

A tese intitulada "Protecção de Dados Pessoais como uma prevenção do cibercrime no Peru, nos anos de 2017 e 2018", é uma pesquisa para o grau de Doutor em Direito, que busca determinar a relação causal entre a Proteção de Dados Pessoais e Crimes de Informática, aplicando pesquisas em especialistas na área, ou seja, especialistas em Direito da Informática, que são advogados especializados e registrados no Ministério da Justiça, como Federados Juramentados com Especialização em Tecnologia da Informação.

O objetivo principal da pesquisa é "Determinar se a Proteção de Dados Pessoais está relacionada à prevenção de crimes de computador no Peru", para isto o tipo de pesquisa é básica - transversal, o método de pesquisa a ser aplicado é o deductive - indutivo - dogmática, e o seu nível de motivos e design experimental não - transversal - causal, a técnica utilizada para reunir informação é o levantamento e o instrumento para a recolha de informação é o questionário aplicado a uma amostra de 57 especialistas em Direito da Informática, que são advogados especializados e registrados no Ministério da Justiça, como Federações Juramentadas com Especialização em Ciência da Computação, de uma população total de 135 a janeiro de 2017 - profissionais do Direito com essa especialidade.

Os resultados obtidos coincidem e são complementados por informações teóricas nacionais e estrangeiras obtidas de outros estudos relacionados, o que permitiu confirmar a hipótese geral, no sentido de que a Proteção de Dados Pessoais está relacionada à prevenção de Crimes de Computador em Peru, bem como as hipóteses específicas, nas quais a relação entre o titular dos dados e sua exposição é estabelecida, o que facilita o uso por criminosos de computador, bem como os mecanismos previstos pela Lei de Proteção de Dados Pessoais (Lei No. 29733) para ajudar na prevenção de cada um dos crimes incluídos na Lei de Crimes por Computador (Lei No. 30096), gerando uma série de recomendações com base nas conclusões obtidas no presente inquérito.

PALAVRAS CHAVE

• Proteção de dados pessoais.
• Crime Informático.
• Dados Pessoais
• Dados sensíveis
• Dados do Computador
• Sistema de computador
• Constituição.
• Lei.
• Direito.

INTRODUCCIÓN

La presente Tesis, es el fruto de un trabajo de investigación que está ligado al análisis de dos normas que han entrado en vigencia en el Perú en el año 2013, como son la Ley Nº 29733 "Ley de Protección de Datos Personales" y la Ley Nº 30096 "Ley de Delitos Informáticos" y sus modificatorias; las cuales ofrecen un nuevo marco protector para un derecho fundamental de las personas, recogido en el Inc. 6º del Art. 2º de la Constitución Política, y aunque no fuese su objetivo principal, de manera directa va a favorecer la prevención de delitos que se caracterizan por utilizar para su comisión, las nuevas tecnologías de la información y la comunicación.

El Perú ha ingresado a vivir en la denominada "Sociedad de la Información", y como tal incorpora nuevas formas de relacionarse, nuevas formas de comunicarse, nuevas formas de trabajar, de estudiar, de socializar, de informarse, que al ser un campo nuevo para muchas de las personas, ofrecen grandes beneficios pero también grandes peligros cuando no se sabe tomar las medidas de prevención en ese nuevo mundo virtual.

Un aspecto que desconocemos en gran parte en nuestro país, es el proteger nuestros datos personales por Internet, para que no sean utilizados por personas de mal vivir, que los aprovechan para cometer diferentes delitos informáticos.

En ese sentido, el derecho como disciplina ordenadora de la sociedad, que la regula para lograr que los seres humanos que la integran puedan vivir en paz, se ha visto en la necesidad de emitir nuevas normas, cuyos resultados se tendrán que ir midiendo con el paso del tiempo.

Por ese motivo recurrimos para la presente investigación a expertos en Derecho Informático y Nuevas Tecnologías, como son los Fedatarios Juramentados con Especialización en Informática, a fin de poder determinar desde su apreciación, cuáles son los efectos que tiene la Protección de Datos Personales, como medio para coadyuvar en la prevención de los Delitos Informáticos.

Nuestra motivación para el presente trabajo se encuentra íntimamente ligada a nuestra especialidad y campo laboral como abogado – docente, puesto que al dedicarme a la enseñanza de cursos afines a la especialidad del "Derecho Informático", en diferentes Universidades en pre y posgrado, así como en la Academia de la Magistratura, al tratar en calidad de alumnos a jueces, fiscales, abogados y estudiantes de derecho, me ha permitido observar la enorme inquietud y expectativa que han recogido estas dos normas, que marcan un importante avance legislativo en esta especialidad, el cual es en gran parte novedoso en el Perú.

Finalmente aspiramos a que las conclusiones del presente trabajo, sirvan como punto de partida para otras investigaciones que se desarrollen en la materia, en este nuevo campo del Derecho en el Perú.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA.

Nuestra sociedad en la actualidad está inmersa en un mundo que ha cambiado mucho durante las últimas dos a tres décadas, debido principalmente al avance de las tecnologías de la información y la comunicación, manifestadas a través del desarrollo de la informática, las telecomunicaciones y el Internet. El vivir en un mundo que se encuentra constantemente comunicado e informado, implica que adecuemos nuestra forma de vivir a esta nueva sociedad llamada "Sociedad de la Información", con los nuevos peligros que ella encierra a través de una serie de infracciones por estos medios y que se plasman en las diferentes figuras que se encuentran tipificadas como "Delitos Informáticos", lo que conlleva a la necesidad de tomar nuevas precauciones para no ser víctimas de los ciberdelincuentes, también llamados cibercriminales o delincuentes informáticos, precauciones entre las cuales se encuentran inmersas las relativas a la protección de nuestros datos personales.

El fenómeno informático permite la posibilidad de realizar actos lícitos e ilícitos, ya que está a disposición de todas las personas, ahora conectadas desde cualquier lugar citadino gracias al crecimiento y expansión de los celulares inteligentes, por ello el derecho es el medio correcto que a través de su normativa pone un límite a ciertas acciones que podrían

atentar contra la intimidad u otros derechos de las personas, a fin de conducir y controlar esta nueva situación dentro de los diferentes medios sociales en el Perú.

Hoy en día encontramos interesante y novedoso el uso de celulares, tablets, laptops, computadoras o cualquier otro medio que permite conectarnos a Internet, y que ha abierto desde principios de siglo un amplio mundo de comunicación virtual que en la presente década se ha vuelto predominantemente móvil, permitiéndonos acceder a medios de comunicación social, ya sea a través de redes sociales como Facebook, Twitter, Instagram, LinkedIn u otras, chats en donde el antiguo Messenger se ha renovado e integrado al Facebook y donde el WhatsApp ha adquirido enorme importancia, herramientas que han incorporado las videoconferencias convirtiéndose al igual que Skype en una gran gama de posibilidades a las que se han ido adecuando los antiguos blogs, páginas web y correos electrónicos, que para mantenerse vigentes han integrado también múltiples posibilidades sociales, en fin, todo un mundo virtual que nos permite interrelacionarnos e interactuar en un mundo paralelo a nuestro mundo físico, que hoy en día captan nuestra atención y se han vuelto parte integrante de nuestras vidas, en la que, sin embargo, muchas veces actuamos irresponsablemente dejando o registrando nuestros datos personales en perfiles públicos a los que pueden acceder todas las personas, con el fin de hacer nuevas amistades, recibir información, acceso a ofertas, premios, trámites con el Estado, compras on line o como simple registro para poder acceder a páginas del mundo del Internet o simplemente por compartir información personal con nuestras amistades y contactos. Estos son solo ejemplos de cómo utilizamos, en la actualidad, las Tecnologías de la Información y la Comunicación para realizar diversas actividades de nuestra vida diaria.

Luego de hablar de los medios informáticos, es importante describir la cibercriminalidad, que es la forma para denominar a los diversos delitos que se pueden cometer utilizando Internet u otras redes virtuales; ya que, gracias a los medios electrónicos, los actores del delito pueden obtener información personal de diferentes personas, que les van a servir para sacar provecho propio o a favor de tercero de manera ilícita.

Para definir al delito informático, el maestro mexicano Julio Téllez (2009), señala que los delitos informáticos son “actitudes ilícitas en que se tienen a las computadoras como

instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo." (Mezzasalma/Pérez, 2001, Par. 7)

Es importante resaltar que, en la sociedad global, todos los ciudadanos de una u otra forma encuentran su accionar cotidiano vinculado a la informática y el Internet. La injerencia de estas nuevas tecnologías ha rebasado distintas esferas, de trabajo, estudio y relaciones sociales que obligan al profesional del siglo XXI, a conocer y dominar estos avances tecnológicos.

Lo señalado anteriormente, está empíricamente comprobado, puesto que en la vida en ciudad se hace imprescindible el uso de Internet como un medio de comunicación, como un medio de trabajo, como un medio de estudio, así como un medio facilitador de información para los usuarios que se ven obligados a utilizar estas nuevas tecnologías.

Asimismo, tomando en consideración el uso continuo de páginas web, redes sociales, chats y el constante intercambio de información en la que están inmersos nuestros datos personales, no es novedad que exista una extensa red de tráfico de datos, mediante la búsqueda individual o la comercialización ilícita de bancos de datos personales, por ello la Ley de Protección de Datos Personales (Ley N° 29733 del 02 de julio de 2011) tiene la finalidad de regular su uso, evitando así la explotación indebida por parte de terceros, de cualquier dato personal, sin gozar del consentimiento previo y expreso del titular del mismo.

El titular de los datos personales, al utilizar los medios electrónicos, puede brindar información sensible sin tener en cuenta que podría ser utilizada en un futuro, por personas que afectarán su patrimonio u otros bienes jurídicos tutelados por los delitos informáticos.

Es preciso señalar que la Ley de Protección de Datos Personales, ha creado un registro de bancos de datos personales y regula determinadas condiciones en cuanto a la forma de llevar a cabo el tratamiento de esos datos.

Con la plena entrada en vigencia de la Ley de Protección de Datos Personales, el 08 de Mayo del 2013, se dio inicio al registro de bancos de datos personales y a aplicar sus distintas normas; por lo que, cada vez que se suscriba un contrato con una empresa de telecomunicaciones o con un banco, la entidad debe informar expresamente cual será la utilización que dará a los datos personales del usuario, cada vez que se tenga una venta por internet o se pacte algún servicio, se requerirá el consentimiento del titular para registrar sus datos personales, cada vez que ingresemos a un nuevo juego virtual, conoceremos para qué serán utilizados nuestros datos personales registrados en el mismo. Asimismo, si más adelante el titular de los datos desea acceder (derecho de acceso) a ellos, la empresa, institución o entidad que los posea se encontrará obligada a facilitar dicha información. Del mismo modo, si los datos reportan algún error, la empresa se encuentra obligada a rectificarlo (derecho de rectificación).

La Ley de Protección de Datos Personales tiene como eje fundamental el devolverle al usuario la posibilidad de que controle sus datos personales y que pueda decidir qué hacer o no hacer con los mismos; lo que le permitirá, asimismo, utilizar tales datos dentro del mercado con un respaldo legal que no existía anteriormente. Por otro lado, si estos datos no son utilizados adecuadamente, también se puede revocar esa decisión.

Todo ese control de nuestros datos personales en los medios virtuales, va a permitirnos tomar adecuadas medidas de prevención, para que no seamos objeto de delitos informáticos.

Cabe mencionar que existe poca información estadística sobre los delitos informáticos en el Perú, tanto por la ocurrencia de cada uno de sus tipos, como por el impacto económico e índice de pérdidas que ocasionan, y que las existentes no tienen carácter oficial, refiriéndose principalmente a fraudes informáticos (hurto por medios informáticos, estafa, etc.), realizados en concurso con los delitos de acceso ilícito a los sistemas o datos informáticos.

Asimismo dos campos importantes dentro de los delitos informáticos que han causado mayor seguimiento en el Perú y trabajo por parte de la policía informática (DIVINDAT), son los relativos contra la libertad sexual por un lado, y contra el patrimonio por otro, respecto al primero ya en el Código Penal se encuentran tipificados la pornografía infantil, la trata de menores, el turismo sexual infantil, etc.; pero la Ley Nº 30096 y su modificatoria, han tipificado el delito de grooming incorporándolo así, en los delitos contra la indemnidad y libertad sexual que son sancionados en el país. Respecto al segundo, cada vez se presentan mayores sustracciones por Internet de dinero que tenemos en tarjetas de débito o crédito, por lo que la nueva Ley de Delitos Informáticos ha centralizado todas las conductas ilícitas contra el patrimonio utilizando las nuevas tecnologías, como delito de Fraude Informático, que integra a los preexistentes delitos de estafa, apropiación ilícita y hurto agravado previstos en el Código Penal, pero que no tipificaban de manera precisa el delito cuando se cometía a través del mundo virtual.

De lo expuesto, podemos colegir que las redes y sistemas de computadoras, ofrecen grandes ventajas, pero a la vez nuevas oportunidades de infringir la Ley, ya que crea de esa forma la posibilidad de cometer delitos tradicionales en formas no tradicionales, esto quiere decir utilizando los medios electrónicos de manera intencional con la finalidad de manejar información perteneciente a terceras personas, sin su consentimiento.

El desarrollo de la informática ha ocasionado la aparición de nuevos delincuentes llamados ciberdelincuentes, quienes hacen uso de sus conocimientos de informática, para obtener ciertos beneficios económicos u otros, de forma ilícita en perjuicio de las personas que vivimos en esta nueva Sociedad de la Información.

Antes de la entrada en vigencia de la Ley de Protección de Datos Personales y su Reglamento, se corría un gran riesgo, puesto que los datos, como por ejemplo la dirección, el teléfono, opción sexual, pensamiento político, credo religioso, datos médicos, no estaban regulados, lo cual ocasionaba que cualquier persona desarrolle un banco de datos personales, sin que necesariamente tenga que estar protegida con medidas de seguridad o tener acceso libre a ellos. Esto demuestra que con esta ley se busca proteger al usuario o titular de los datos personales; al respecto cabe agregar que, los países referentes para el Perú, en la dación de esta Ley, fueron España y Argentina, en donde se considera de gran

importancia la protección de los datos personales, no sólo por el hecho de ser un derecho fundamental de las personas humanas, sino también por su efecto positivo en la prevención de los delitos informáticos, lo que ha dado lugar a una serie de campañas en su difusión y conocimiento.

Actualmente, al aplicarse las normas sobre protección y tratamiento de los datos personales, nos lleva a pensar que las mismas van a coadyuvar en la prevención de los delitos informáticos previstos en la Ley Nº 30096 y su modificatoria, como los referidos delitos de Fraude Informático o de Grooming por ejemplo, al efectuarse un mal uso de los avances de la tecnología, la cual en sí misma no es una fuente negativa, sino por el contrario es muy útil y trae grandes y múltiples beneficios a los usuarios, pero cuando esta es utilizada correctamente y sin invadir los espacios privados de las personas.

Un ejemplo de cómo una persona toma conocimiento que sus datos se encuentran en manos de terceros, es cuando te llaman de una compañía oncológica, de seguros, bancaria o telefónica, para ofrecer nuevos servicios, lo que nos genera la pregunta cómo obtienen nuestro número telefónico y lo usan sin nuestro consentimiento.

En virtud al párrafo anterior, esto es posible ya que al acceder a un sistema financiero o a cualquier servicio, uno por contrato puede estar entregando sus datos. Sin embargo, en la actualidad todo contrato o condiciones de uso deben incluir cláusulas de privacidad de datos y precisar el objeto o uso que se dará a los datos personales que su titular está facilitando a una empresa, a fin de que ésta pueda gestionarlos adecuadamente y conforme a los parámetros previstos en la relación contractual.

Respecto al control, es conveniente mencionar que resulta necesario plantear mecanismos de control como un medio para la prevención de la ciberdelincuencia, por ello es que nos planteamos como problema de investigación, si una forma de prevenir la comisión de los delitos informáticos, es asegurar la debida protección de los datos personales de una persona, y en qué medida colabora en su prevención, lo que implica por ende, que se procure un mayor conocimiento y difusión de la nueva normativa sobre protección de datos personales, para lograr de esa manera, que nuestros datos personales se vean afectados, por un uso indebido que se les pueda dar con fines delictivos.

Resumiendo, nuestro problema general está dirigido a identificar la magnitud de influencia que tiene la Ley de Protección de Datos Personales del Perú, como medio de prevención de los Delitos informáticos en el Perú. Obviamente, cada una de esas dos leyes contienen una serie de normas cuyo tratamiento y estudio en detalle, haría sumamente extensa y dificultosa su investigación; por lo que, a fin de delimitarlo, para nuestra primera variable que es la Protección de Datos Personales, nos hemos centrado en estudiarlo desde dos dimensiones. Cada una de esas dimensiones nos ofrece una perspectiva diferente del problema general; en primer lugar, vamos a investigar las conductas del Titular de los Datos Personales, quién por falta de conocimiento respecto a la importancia de proteger sus datos personales, o por negligencia en su manejo, o por exceso de confianza en su uso, los expone innecesariamente, permitiendo que sus datos sean obtenidos por ciberdelincuentes, quienes ven facilitada su labor criminal, haciendo uso indebido de los mismos, para cometer delitos informáticos tipificados en el Perú; en segundo lugar, investigaremos los mecanismos que ofrece la Ley de Protección de Datos Personales, que sirvan como medio para proteger los datos de las personas, colaborando de esa manera, en la prevención de los delitos informáticos en el Perú que se facilitan con su uso.

En lo relativo a nuestra segunda variable, que son los delitos informáticos, su estudio lo abordaremos a partir de cada uno de los delitos informáticos que tiene tipificada la Ley de Delitos Informáticos peruana, examinándolos a partir de la propia clasificación que ofrece la Ley y que los diferencia en delitos informáticos contra los datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidad y secreto de las comunicaciones, contra el patrimonio y contra la fe pública, buscando identificar los delitos informáticos cuya comisión sí se ve facilitada por el acceso indebido a los datos personales de la víctima.

1.2 DELIMITACIÓN DE LA INVESTIGACIÓN.

La presente investigación, la vamos a delimitar desde cuatro perspectivas diferentes; en primer lugar en el espacio, es decir el ámbito geográfico al que se circunscribió la investigación; en segundo lugar, en cuanto al ámbito social, referido a las personas y/o sociedades que se podrán beneficiar con el presente trabajo; en tercer lugar, tenemos un

ámbito temporal, es decir el lapso de tiempo en que se desarrolló la investigación, y; el ámbito conceptual, que son los parámetros conceptuales que hemos utilizado en el desarrollo del presente trabajo de investigación.

1.2.1 DELIMITACIÓN ESPACIAL

El estudio se efectuará en la ciudad de Lima Metropolitana, toda vez que en dicha ciudad radican los abogados Fedatarios Juramentados con Especialización en Informática sobre cuyas capacitadas opiniones, se ha realizado el estudio de campo de la presente investigación.

1.2.2 DELIMITACIÓN SOCIAL

Nuestra unidad de análisis se encuentra en los especialistas en Derecho Informático, que cuenta con el título de Fedatario Juramentado con Especialización en Informática.

El Fedatario Juramentado con Especialización en Informática, es un funcionario de la fe pública creado en el Perú por el Decreto Legislativo N° 681, en cuyo Reglamento, aprobado por Decreto Supremo N° 009-92-JUS, se establece que para obtener ese título, se requiere ser abogado titulado, acreditar idoneidad técnica, a través de la aprobación de un curso de especialización aprobado por el Ministerio de Justicia y a cargo de un Colegio de Abogados o de Notarios, con una duración de dos semestres académicos, juramentándose el cargo ante la Corte Superior de la Jurisdicción y registrándose en el Ministerio de Justicia.

La delimitación social de la investigación, se da en razón de que la misma se ha realizado sobre Fedatarios Juramentados con Especialización en Informática, dado que su opinión especializada, genera un alto índice de confiabilidad sobre los resultados, a partir de sus opiniones respecto a un tema del cual aún no se tienen datos estadísticos confiables en el Perú, por ser relativamente nuevos en nuestro país.

1.2.3 DELIMITACIÓN TEMPORAL

Enero 2017 – Julio 2018.

1.2.4 DELIMITACIÓN CONCEPTUAL

Delimitamos nuestros conceptos, al entender a la Protección de Datos Personales como aquel derecho fundamental de la persona que tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de las computadoras y el Internet.

Por otro lado, entendemos por delito informático, a aquella conducta típica, antijurídica y culpable, en que se tiene a las computadoras e Internet como instrumento o fin.

1.3 PROBLEMAS DE INVESTIGACIÓN

1.3.1 PROBLEMA PRINCIPAL

¿Cómo la Protección de Datos Personales, se relaciona con la prevención de los Delitos Informáticos en el Perú?

1.3.2 PROBLEMAS ESPECÍFICOS

Son dos los problemas específicos que se han planteado, extraídos de dos aspectos primordiales del contenido del problema principal, de tal manera que al darse respuesta a esos dos problemas específicos, va a contribuir también en la respuesta al problema principal. Los problemas específicos son los siguientes:

a) ¿Cómo el titular de los datos personales relaciona su uso indebido para la comisión de delitos informáticos?

b) ¿Cómo la Ley de Protección de Datos Personales relaciona la prevención de los delitos informáticos en el Perú?

1.4 OBJETIVOS DE LA INVESTIGACIÓN

1.4.1 OBJETIVO GENERAL

Determinar si la Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú.

1.4.2 OBJETIVOS ESPECÍFICOS

Son dos los objetivos específicos que se han seleccionado, que corresponden a dos aspectos primordiales del contenido del objetivo principal, de tal manera que al alcanzarse esos dos objetivos específicos, contribuyen también a lograr el objetivo principal, los cuales detallamos a continuación:

a) Determinar si el titular de los datos personales relaciona su uso indebido para la comisión de delitos informáticos.

b) Establecer si la Ley de Protección de Datos Personales relaciona la prevención de los delitos informáticos en el Perú.

1.5 JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN.

1.5.1 JUSTIFICACIÓN.

La justificación del tema que hemos elegido para la presente investigación, vamos a analizarla desde cuatro perspectivas, que son la teórica, la práctica, la metodológica y la legal.

1.5.1.1 JUSTIFICACIÓN TEÓRICA.

La correlación causal que existe entre la protección de datos personales y los delitos informáticos, es un tema que no ha sido investigado en el Perú, ni se han encontrado investigaciones al respecto en los países de habla hispana, motivo por el cual, es necesario realizar un estudio detallado de la relación causal que existe entre ambas instituciones jurídicas, que permitan plasmar un conocimiento teórico de cada una, aportando a su conocimiento científico, a fin de poder determinar la forma como una afecta o influye en la otra.

Por lo señalado en el párrafo anterior, se justifica teóricamente la presente investigación, por ser un aporte al conocimiento el establecer en qué medida la Protección de Datos Personales, sirve como un medio de prevención de los Delitos Informáticos.

1.5.1.2 JUSTIFICACIÓN PRÁCTICA.

La presente investigación se inició en el año 2014, de modo exploratorio, cuando recién se comenzaba a aplicar en el Perú, la Ley de Protección de Datos Personales (Ley 29733) y la Ley de Delitos Informáticos (Ley Nº 30096), que entraron en vigencia en su totalidad a partir del 08 de mayo y 23 de octubre del año 2013, respectivamente; en los años que han pasado, no se ha efectuado una adecuada difusión de estas dos normas, ni tampoco existe una información estadística sistematizada, que nos permita conocerlas individualmente o en su correlación, es por ello, que la significación práctica y social de la presente investigación, se ve enmarcada en dos perspectivas, por un lado la de brindar a los funcionarios públicos encargados de su aplicación, de un sustento teórico para aplicarlo a los casos prácticos que tienen que afrontar en su trabajo diario, y por otro lado la de brindar a la sociedad peruana de un aporte que permita incentivar el conocimiento de la protección de datos personales, así como motive a la autoridad nacional de protección de datos personales, a realizar campañas de difusión sobre la normativa en la materia, desde una perspectiva que realce su importancia como medio de prevención de los delitos informáticos.

1.5.1.3 JUSTIFICACIÓN METODOLÓGICA.

Como señala Bernal (2010), la justificación metodológica del estudio se da cuando el proyecto que se va a realizar propone un nuevo método o una nueva estrategia para generar conocimiento válido y confiable; en ese sentido, debemos precisar que en el Perú son mínimas las investigaciones que existen sobre la Protección de Datos Personales y los Delitos Informáticos, en consecuencia, la presente investigación se justifica metodológicamente en la medida que es un punto de partida para estudiar estas dos instituciones jurídicas, lo cual es una estrategia para promover el conocimiento científico de las mismas, a partir de estudios que sean confiables para construir una doctrina nacional a partir del estudio válido de la Ley de Protección de Datos Personales (Ley 29733) y la Ley de Delitos Informáticos (Ley Nº 30096) en el Perú, estudio que se aplicó desde el mes de Enero de 2017 hasta el mes de Julio de 2018.

1.5.1.4 JUSTIFICACIÓN LEGAL.

Desde el punto de vista legal, la presente investigación se justifica por ser dos instituciones jurídicas de vigente actualidad en el país, cuyo estudio se suele enmarcar únicamente entre los especialistas del derecho informático, motivo por el cual son aún poco conocidas entre los abogados peruanos, así como han sido escasos los eventos de capacitación que han propuesto las diferentes instituciones públicas y privadas para la difusión de la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos.

Si bien por su campo práctico, los abogados penalistas son los que han desarrollado un mayor conocimiento en la aplicación de la Ley de Delitos Informáticos, estos no se dirigen al ámbito de la prevención del delito, en la cual los especialistas del derecho, tenemos la responsabilidad de colaborar con su difusión.

Respecto a la Ley de Protección de Datos Personales, debemos recordar que existe una autoridad nacional dependiente del Ministerio de Justicia y Derechos Humanos; que está realizando una importante labor en la aplicación de esta normativa entre las instituciones públicas y privadas, pero que no ha promocionado su mejor conocimiento en los eventos de derecho administrativo, que permita a abogados especializarse en un campo que aún es nuevo en el Perú.

Es por lo señalado que, al igual que en los aspectos teórico, práctico y metodológico, la justificación legal sustenta debidamente la realización de la presente investigación sobre la correlación causal que existe entre la protección de datos personales, como medio de prevención para los delitos informáticos.

1.5.2 IMPORTANCIA.

El tema de la ciberdelincuencia es cada vez más alarmante en el Perú, sin embargo, con la promulgación de la Ley de Protección de Datos Personales (Ley N° 29733), que ofrece una serie de mecanismos para prevenir que nuestros datos personales no sean obtenidos de manera ilícita, se ofrece una alternativa en los miembros de la sociedad peruana, para evitar ser agraviados por los delincuentes informáticos.

Es por ello, que con su aplicación se espera que ayude a prevenir los delitos informáticos reduciendo su comisión, lo cual mediremos a partir de la percepción de especialistas en la materia, al no existir estadísticas que nos permitan determinar de manera efectiva su reducción. Los delincuentes informáticos aprovechan la ausencia de medidas de control para obtener los datos personales de sus víctimas, utilizándolos para su accionar delictivo, esto es posible debido a que la información brindada por un usuario a Bancos de Datos Personales, se ha visto transgredida fácilmente por agentes del delito, ya sea por falta de cuidado de los titulares de los datos o por la ausencia de mecanismos de seguridad amparados en una normativa expresa, que impida o reduzca la obtención ilegal de información de personas, con el objeto de usarlas para actos delictivos.

En consecuencia, con la influencia de esta Ley aplicada en su integridad, se puede coadyuvar en la reducción de la ciberdelincuencia en el Perú, lo cual, a su vez ayudará a que los usuarios que forman parte de la sociedad de la información, vean asegurados sus datos personales.

La mayoría de las personas, hoy en día, dependemos de un computador e Internet para nuestra labor diaria, ya que este permite obtener información fácilmente, motivo por el cual origina confianza en nosotros; sin embargo, debemos tener en cuenta que podemos ser víctimas de personas que podrían apoderarse de los datos que compartimos de diversas formas a través de Internet, es decir, datos personales que individualizan a las personas y por tanto permiten su identificación.

Ahora en la sociedad de la información podemos preguntarnos cuál es la finalidad de que exista una Ley que proteja los Datos Personales, y encontramos la respuesta, en que estos datos pueden ser utilizados sin nuestra autorización o consentimiento por agentes del delito informático, que podrían causarnos algún daño personal y/o patrimonial ya sea por medio de los delitos de acceso ilícito a datos y sistemas informáticos, contra la indemnidad y libertad sexuales, contra la intimidad y el secreto de las comunicaciones, fraude informático, suplantación de identidad informática, o abuso de mecanismos y dispositivos informáticos, tipificados en la Ley de Delitos Informáticos y su modificatoria (Ley N° 30171).

1.6 FACTIBILIDAD DE LA INVESTIGACIÓN.

La investigación es factible, toda vez que se cuenta con los recursos humanos, financieros y materiales para el desarrollo de la investigación. Especial mención consideramos conveniente hacer, a fin de precisar que el investigador, es decir el tesista, es también Fedatario Juramentado con Especialización en Informática y por lo tanto mantiene relación profesional con las personas en las cuales se practicará la investigación, lo que facilita la aplicación virtual de la investigación.

1.7 LIMITACIONES DEL ESTUDIO

Las limitaciones de la investigación, las podemos tratar desde una doble perspectiva, una en cuanto a la extensión de la investigación y otra respecto a la limitada información estadística que existe aún sobre el tema en el Perú.

Las limitaciones de la investigación respecto a su extensión, las podemos enfocar desde el punto de vista espacial, a pesar de que el accionar de los ciberdelincuentes se da en todo el Perú, temas de accesibilidad a Internet, dan lugar a que la recurrencia de delitos informáticos en el Perú, esté mayormente concentrada en Lima Metropolitana.

Otra limitación es que el análisis normativo de las Leyes de Protección de Datos Personales y de Delitos Informáticos, necesariamente tendrá un importante enfoque teórico cuya reciprocidad práctica se verá sustentada en la opinión de especialistas en la materia, más que en información estadística por ser esta aún inexistente.

CAPÍTULO II: MARCO FILOSÓFICO

2.1 FUNDAMENTACIÓN ONTOLÓGICA

2.1.1 ORÍGENES DE LA SOCIEDAD DE LA INFORMACIÓN.

No nos vamos a referir a los orígenes del término, más es importante precisar que la vida del ser humano desde finales del siglo XX y de manera principal en el presente siglo, se ha visto fuertemente influenciada por un fenómeno mundial generado a partir del desarrollo de las tecnologías de la información y la comunicación, una revolución científica y tecnológica que ha generado una transformación en la vida del hombre, no sólo en sus ámbitos educativos y profesionales, sino también, en lo económico, en lo político, en lo cultural, en lo social, esta transformación ha llegado hasta los ámbitos más íntimos del ser humano, pues también ha cambiado sus formas de relacionarse, de socializar, de crear amistades, de enamorarse y por ello la Sociedad de la Información, denominación elegida para este nuevo fenómeno, nos brinda una nueva forma de vida del ser humano en sociedad, en la que todos tenemos que aprender a desenvolvernos.

En las décadas del 60 o 70, cuando el hombre llegó por primera vez a la luna y se iniciaron los viajes espaciales, se pensaba que el año 2000 nos traería una nueva forma de vida.

Inspirados por las novelas, series de ciencia ficción e incluso dibujos animados, la imaginación nos llevaba a creer que en el siglo XXI nos alimentaríamos con comida en píldoras, los automóviles se desplazarían por el aire como naves voladoras familiares, robots humanizados nos servirían en todas nuestras necesidades manuales, fungiendo de mayordomos, cocineras, obreros, etc. En fin, imaginábamos una vida totalmente distinta; sin embargo, terminó el siglo XX y seguimos comiendo jugosos trozos de carne con arroz, huevos, menestras, verduras, y nada en pastillitas que las sustituyan como alimento, los automóviles siguen rodando por la tierra sobre sus llantas, y aunque tenemos maquinaria que nos facilita mucho las labores manuales, no se presentan aún como robots inteligentes o humanizados, lo que lleva a preguntarnos ¿Qué es lo que ha cambiado en nuestra vida?, y la respuesta sólo nos dirige a dos invenciones, que ya existían hace medio siglo, pero cuyo rápido desarrollo en los últimos veinticinco años, ha transformado la forma de vivir de todas las sociedades, nos referimos pues, a la informática y el Internet.

La veloz evolución de las computadoras personales desde su aparición, que hoy en día nos permiten tener microcomputadoras en aparatos tan pequeños como nuestros celulares de bolsillo, cuyo uso se ha masificado, o del Internet que facilita que con esos aparatos nos podamos comunicar y tener información casi al instante, de cualquier lugar del mundo, son lo que ha cambiado nuestras vidas, y que nos permite decir hoy en día, que estamos en una Sociedad de la Información, aquella que Alvin Toffler coloca como el tercer acontecimiento de mayor relevancia en la historia del desarrollo de la humanidad:

> "… la historia de la humanidad se puede dividir en tres etapas a las que denomina "olas". La primera "ola" corresponde a la utilización de la agricultura, cuando las primitivas sociedades dejan de ser nómadas y se crea un orden social teniendo como principal actividad la agricultura. En la segunda ola se produce el cambio de la sociedad agrícola a la sociedad industrial, conocida como la primera revolución industrial que puede ubicarse entre fines del siglo XIX y principios del XX, y la tercera "ola", que corresponde al tiempo actual, caracterizada por el desarrollo y empleo de las tecnologías de la información y comunicaciones(TIC)". (Nieto, 2007, p. 1)

2.1.2 LOS SIGNOS DEL CAMBIO

El siglo XXI, nos trae un mundo con una serie de megatendencias, es decir tendencias cuya magnitud tiene alcance mundial:

- Revolución científica y tecnológica.

- Planetarización de las decisiones.
- Primacía de los servicios.
- Globalización económica y financiera.
- Era del conocimiento.
- Libertad, derechos humanos y democracia.
- Aprendizaje permanente.
- Pobreza y conflictos civilizatorios.

Estos signos del cambio que nos hacen pasar a la primacía de los servicios sobre la producción, a que el capital del tener de paso al capital del saber, que las tecnologías de la producción se vean sustituidas por las tecnologías informatizadas, y otros más nos introducen al siglo XXI, en el cual no se ha logrado erradicar el hambre, la corrupción, las deficiencias en servicios de salud y educación, ante ello, en setiembre del 2000, en la Sede de las Naciones Unidas se aprobó la "Declaración del Milenio", en la que se establecen ocho grandes Objetivos de Desarrollo del Milenio, los cuales apuntan precisamente a estos problemas, pero añaden en sus últimos dos objetivos, la sostenibilidad del medio ambiente y el Fomentar una Alianza Mundial para el Desarrollo, lo cual nos demuestra la gran importancia que se le brinda a esos dos temas: la protección del medio ambiente y la accesibilidad a los beneficios de las nuevas tecnologías, especialmente las de información y comunicaciones (Meta 8.D).

En efecto, en el Informe A/64/665 que realizó en Febrero del 2010, casi 10 años después de efectuada esa Declaración, el entonces Secretario General de las Naciones Unidas manifiesta que:

> "Los adelantos tecnológicos ofrecen una oportunidad para acelerar el proceso de reducción de la pobreza siguiendo un camino que no pudieron transitar los países que se desarrollaron anteriormente. La reducción de la brecha tecnológica puede acelerar el progreso saltando etapas en la adopción de soluciones de desarrollo innovadoras y de bajo costo. Esa tecnología facilita las comunicaciones y el intercambio de información". (p. 33)

Esto nos lleva a preguntarnos, la Información a la cual podemos acceder con tanta facilidad mediante las nuevas tecnologías, ¿qué nos va a permitir?, pues conocimiento, y el conocimiento en esta sociedad se convierte en riqueza, ya no lo es la tenencia de bienes como era en la sociedad industrial, es así que las tecnologías aplicadas como medio de

desarrollo sostenible, y en especial las tecnologías de la información y la comunicación (TIC), son un medio efectivo para proporcionarnos riqueza, si las sabemos utilizar adecuadamente, si somos diestros en su manejo, en nuestro desempeño personal y profesional. Es posible que demore mucho en cambiar el mundo, pero trabajando para la reducción de la brecha digital, es decir la distancia que separa a los países en desarrollo de aquellos denominados desarrollados en el uso que tienen del Internet y las nuevas TICs, se podrá aminorar la pobreza y lograr una sociedad en donde prime la democracia, la libertad y el profundo respeto a los derechos humanos que, desde la óptica del derecho, posiblemente constituya aquella megatendencia de mayor importancia.

2.1.3 UNA NUEVA SOCIEDAD Y LA BRECHA DIGITAL

La diversidad de autores coincide en que fue por los años setenta, que el concepto de sociedad industrial comenzó a evolucionar hacia un modelo distinto, caracterizado por el procesamiento y manejo de la información gracias a las nuevas TICs, el cual se ha denominado sociedad de la información.

Esta nueva sociedad, tiene como eje característico principal, el acceso a la información, la cual debidamente procesada produce conocimiento y debidamente utilizada proporciona riqueza, en tal sentido, el factor diferencial que introduce la Sociedad de la Información, se refiere a que cada persona u organización no solo dispone de sus propios conocimientos, sino que también tiene una capacidad para acceder a la información, que es generada por los demás y es casi ilimitada; por ello, esa característica alude al potencial para convertirse en un generador de información para otros.

Esta nueva sociedad recibe diversas definiciones, pero hemos buscado una que tenga legitimidad u oficialidad, como la siguiente:

> El concepto de "sociedad de la información" hace referencia a un paradigma que está produciendo profundos cambios en nuestro mundo al comienzo de este nuevo milenio. Esta transformación está impulsada principalmente por los nuevos medios disponibles para crear y divulgar información mediante tecnologías digitales. Los flujos de información, las comunicaciones y los mecanismos de coordinación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva. (CEPAL, 2003)

En la actualidad creemos que es indiscutible, que la facilidad para informarnos, los diversos medios para comunicarnos, todas las nuevas tecnologías que nos permiten estar más cerca y más informados por medios virtuales, ha creado definitivamente una nueva sociedad. Una sociedad que exige que todos los que la componen, se adapten y trabajen de acuerdo a los parámetros sociales que tiene establecidos, es decir, sepan utilizar esas tecnologías en su vida diaria.

A esta nueva cultura alude Marqués, quién es citado en el blog de Ghirardotti, para decirnos lo siguiente:

> Esta nueva "cultura", que conlleva nuevos conocimientos, nuevas maneras de ver el mundo, nuevas técnicas, pautas de comportamiento y el uso de nuevos instrumentos y lenguajes; va remodelando todos los rincones de nuestra sociedad e incide en todos los ámbitos en los que desarrollamos nuestra vida, exigiendo de todos nosotros grandes esfuerzos de adaptación. (2007)

Así pues, hoy en día todos sabemos hablar por celular, utilizar una tarjeta bancaria, mandar un email, chatear (incluido el "wasapear"), crear un documento digital en un procesador de textos, y muchas otras habilidades que se van incrementando a medida que las nuevas generaciones, los nativos digitales, crecen en medio de esas tecnologías. Pero somos conscientes de cómo nos insertamos en esa sociedad casi inadvertidamente, a la pregunta de ¿podemos vivir sin computadoras?, que he planteado a mis alumnos universitarios, la respuesta general es no, no es posible, y entonces cabe preguntarnos, y como viven esas personas en los pueblos alto andinos sin energía eléctrica, y obviamente sin computadoras e internet, como viven las personas de los barrios marginales, que se encuentran en extrema pobreza, que no tienen acceso a estas nuevas tecnologías, definitivamente estas situaciones podrían encajar en lo que se llama brecha digital, en su concepción amplia, es decir toda diferencia entre las personas por su acceso o uso de las nuevas tecnologías de la información y la comunicación.

Sin embargo, el concepto de brecha digital ha sido enfocado más desde una perspectiva internacional, la cual no alude a esas diferencias internas por acceso a las tecnologías, dadas por diferencias regionales o socioeconómicas, sino que alude a aquellas sociedades que usan las TIC cotidianamente, en beneficio de su calidad de vida y aquellas que no tienen acceso a esas tecnologías, o teniéndolas no las aprovechan adecuadamente por

desconocimiento. En el año 2006, esta brecha era notoria, toda vez que en los países desarrollados tecnológicamente el 58.6% de los habitantes tenían acceso a Internet, mientras los que estaban en vías de desarrollo, apenas alcanzaban al 10.2%. La diferencia o brecha digital, no ha dejado de existir, pues el año 2013 por ejemplo, 39.2% de las personas usaba Internet en el Perú, mientras que en España eran el 71.6%, y en países como Holanda, Dinamarca, Noruega y Suecia se supera el 94%, estando al otro extremo de la estadística países como Honduras, Nicaragua, India y Haití que están por debajo del 18%, no llegando ni al 10% varios países africanos.

2.1.4 NUEVOS VALORES EN LA SOCIEDAD DE LA INFORMACIÓN

Esta nueva Sociedad, también está generando nuevos valores en el ser humano, valores plasmados en diferentes expresiones de la vida, como en el ámbito jurídico, en el cual han adquirido una mayor importancia derechos como la libertad de información, la intimidad y la protección de datos personales y el acceso a la información, dando lugar a que por su importancia merezcan una protección especial desde el Derecho Penal, en el cual el bien jurídico "Información" se erige como el más característico en la Sociedad de la Información y ha dado nacimiento a los denominados "Delitos Informáticos".

Estos nuevos valores, que pueden contribuir a un desarrollo tecnológico equilibrado en las diferentes naciones, dieron lugar a que desde el ámbito político, tanto internacional como nacional, se le brinde especial atención, ya que es evidente que una nueva sociedad, tiene que reestructurar y mejorar sus tipos de organización gubernamental, brindando nuevos y mejores servicios a los ciudadanos, aprovechando las nuevas tecnologías de la información y la comunicación para ello, así como los demás factores sociopolíticos.

2.1.5 LA CUMBRE MUNDIAL Y POLÍTICAS REGIONALES.

Un gran evento mundial impulsado por la Organización de las Naciones Unidas y la Unión Internacional de las Telecomunicaciones, se produjo hace unos años y fue denominado Cumbre Mundial sobre la Sociedad de la Información, que no se detiene en haber sido una serie de reuniones y conferencias al respecto, sino que constituye un trabajo mundial, permanente evaluado, para la construcción de esta Sociedad, ello se grafica en la definición de Sociedad de la Información que aparece en su Portal web:

> La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo. El objetivo de la Cumbre Mundial sobre la Sociedad de la Información es garantizar que estos beneficios sean accesibles para todos y fomentar ciertas ventajas específicas en algunos campos, como estrategias-e, negocio-e, gobernanza-e, salud-e, educación, alfabetización, diversidad cultural, igualdad de género, desarrollo sostenible y protección del medio ambiente. En la Cumbre de Ginebra de diciembre de 2003, los líderes mundiales declararon: "nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos". (CMSI, 2005)

Con la Resolución de las Naciones Unidas 56/183 se dio inicio al trabajo para desarrollar la Cumbre Mundial sobre la Sociedad de la Información, en ella se aprueba que se realice dicha cumbre en dos Sesiones, la primera se realizó del 10 al 12 de diciembre de 2003, siendo la sede elegida para su realización Ginebra (Suiza) país desarrollado tecnológicamente, y; la segunda fase se llevó a cabo del 16 al 18 de noviembre de 2005, en Túnez, un país con poco desarrollo tecnológico, como un símbolo del objeto central de la Cumbre, que se manifiesta en esta Resolución que comienza diciendo:

> *"La Asamblea General,*
> *Reconociendo* la urgente necesidad de aprovechar las posibilidades que ofrecen los conocimientos y la tecnología para promover los objetivos fijados en la Declaración del Milenio, y de encontrar medios eficaces e innovadores de poner estas posibilidades al servicio de un desarrollo para todos". (2002)

Debemos entender, que la Cumbre Mundial sobre la Sociedad de la Información no solamente ha reunido a una gran cantidad de naciones de todo el mundo, sino que también reunió a organizaciones de la sociedad civil y personalidades distinguidas que le dieron mayor realce.

En la primera fase de la Cumbre, se aprobó la Declaración de Principios y el Plan de Acción, mientras que en la segunda fase, se adoptó el Compromiso de Túnez y la Agenda de Túnez para la Sociedad de la Información.

Dentro de la labor de seguimiento de esos documentos y en particular de la Agenda de Túnez, las Naciones Unidas, mediante la Resolución Nº 60/252 de Marzo del 2006, decidió proclamar el 17 de mayo como el Día Mundial de la Sociedad de la Información, como un día que permitiera conocer mejor las posibilidades que pueden brindar el Internet y otras tecnologías de la información y las comunicaciones a las sociedades y economías, así como las diferentes formas de reducir la brecha digital.

La Cumbre Mundial planteó una serie de objetivos a largo plazo, que vienen siendo evaluados anualmente; sin embargo, se entendía que debían existir objetivos a corto plazo, que fueran trabajados en esferas más pequeñas, dando lugar a los encuentros regionales.

En América Latina y el Caribe, el año 2005 se realizó la Primera Conferencia Ministerial sobre la Sociedad de la Información, conocida como eLAC 2007, dado que sus objetivos se plantearon a dos años, es decir al corto plazo. A partir de allí cada dos o tres años se han seguido dando las Conferencias Ministeriales sobre la Sociedad de la Información, habiendo sido la tercera en la que el Perú se volvió protagonista, ya que se realizó del 21 al 23 de Noviembre del 2010 en la ciudad de Lima. Este eLAC 2015, permitió evaluar la implementación del programa de la Sociedad de la Información en América Latina y el Caribe y establecer medidas políticas que se dieron al mediano plazo, ya que serían verificadas hacia el año 2015.

Entre el 05 y 07 de Agosto del 2015, se desarrolló en México la Quinta Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Caribe (eLAC 2018), el cual presenta cinco áreas de acción: 1) Acceso e infraestructura, 2) Economía digital, innovación y competitividad, 3) Gobierno electrónico y ciudadanía, 4) Desarrollo sostenible e inclusión, y, 5) Gobernanza para la sociedad de la información.

En la actualidad estamos viviendo dentro de la Agenda Digital para América Latina y el Caribe (eLAC 2020), que conjuntamente con la Declaración de Cartagena de Indias, son los dos documentos normativos formulados en el sexto eLAC, desarrollado del 18 al 20 de abril del 2018, en la ciudad de Cartagena de Indias – Colombia, el cual actualiza las áreas de acción, señalando las siete siguientes: 1) Infraestructura digital, 2)

Transformación digital y economía digital, 3) Mercado digital regional, 4) Gobierno digital, 5) Cultura, inclusión y habilidades digitales, 6) Tecnologías emergentes para el desarrollo sostenible, y, 7) Gobernanza para la sociedad de la información.

Como apreciamos, los organismos y acuerdos internacionales propenden a que se logre un crecimiento tecnológico con equidad, generando y/o fortaleciendo nuevos valores, a favor de un desarrollo humano y social más integral.

2.1.6 PLAN DE DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN EN EL PERÚ.

El Perú no ha estado ajeno a todo este movimiento internacional en torno a la Sociedad de la Información, ya en la Cumbre Mundial sobre la Sociedad de la Información entre los 175 países que estuvieron representados, se encontró el Estado Peruano, participando en su primera fase con una delegación de 11 personas y en la segunda fase con 3 representantes.

No es casual entonces, que en el año en que se inició dicha Cumbre, en el Perú tomando conciencia sobre el tema, se haya creado la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información – CODESI, mediante la Resolución Ministerial N° 181-2003-PCM del 04 de Junio de 2003.

Esta Comisión, tuvo como objeto elaborar un Plan de Desarrollo de la Sociedad de la Información en el Perú, asimismo formular las acciones necesarias a ejecutar, para su desarrollo y los proyectos de normas y los dispositivos que coadyuven al adecuado desarrollo, implementación y promoción de la Sociedad de la Información en el Perú; el mismo fue culminado el año 2005, siendo conocido como "La Agenda Digital Peruana" disponiéndose su publicación mediante la Resolución Ministerial N° 148-2005-PCM, es decir meses antes de que se llevará a cabo la Segunda Sesión de la Cumbre Mundial de la Sociedad de la Información, ello seguramente como un compromiso nacional respecto al Plan de Acción diseñado en la Primera Sesión en Ginebra.

Pero fue mediante el Decreto Supremo Nº 031-2006-PCM, se aprobó dicho Plan, el cual consta de 06 Capítulos, además de su Presentación, Glosario y Anexos, encontrándose en su Quinto Capítulo los 05 grandes objetivos estratégicos de la Agenda Digital Peruana:

1. Disponer de infraestructura de telecomunicaciones adecuada para el desarrollo de la Sociedad de la Información.
2. Promover el desarrollo de capacidades que permitan el acceso a la Sociedad de la Información.
3. Desarrollar el sector social del Perú garantizando el acceso a servicios sociales de calidad, promoviendo nuevas formas de trabajo digno, incentivando la investigación científica e innovación tecnológica, así como asegurando la inclusión social y el ejercicio pleno de la ciudadanía.
4. Realizar acciones de apoyo a los sectores de producción y de servicios en el desarrollo y aplicaciones de las TIC.
5. Acercar la administración del Estado y sus procesos a la ciudadanía y a las empresas en general, proveyendo servicios de calidad, accesibles, seguros y oportunos, a través del uso intensivo de las TIC. (2006)

Posteriormente se dio en el Perú un trabajo de evaluación y seguimiento, CODESI mantuvo su sigla pero cambió de denominación, pasando a llamarse "Comisión Multisectorial para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de la Información en el Perú", adquiriendo el año 2008 un carácter permanente, siendo destacable la creación de grupos de trabajo para asesoramiento de la Comisión, en 6 áreas diferentes cuyos grupos de trabajo fueron coordinados de la siguiente manera:

Tabla 1

GRUPO DE TRABAJO	COORDINADORES
Grupo N° 1: Infraestructura y acceso.	Designado por el Vice Ministerio de Comunicaciones del MTC
Grupo N° 2: Educación y mejoramiento de capacidades humanas.	Designado por el Ministerio de Educación
Grupo N° 3: Salud y desarrollo social.	Designado por el Ministerio de la Mujer y Desarrollo Social
Grupo N° 4: Producción y servicios.	Designado por el Ministerio de la Producción.
Grupo N° 5: Gobierno electrónico.	Designado por la Oficina Nacional de Gobierno Electrónico e Informática
Grupo N° 6: Instrumentos de política y estrategias.	Designado por la Oficina Nacional de Gobierno Electrónico e Informática

El escenario social en el Perú, desde que se aprobó el Primer Plan de Desarrollo de la Sociedad de la Información - Agenda Digital Peruana, ha sufrido importantes cambios

con el rápido avance tecnológico, siendo notorio en los últimos años el incremento de la banda ancha mejorando la accesibilidad a Internet, permitiendo que el usuario la utilice en forma diaria a través de computadoras, Laptops, Tablets y principalmente celulares.

Esos cambios tecnológicos ya se habían plasmado en la Agenda Digital Regional del año 2010, como consecuencia del tercer eLAC que se llevó a cabo en la ciudad de Lima, es por ello que, mediante Decreto Supremo Nº 066-2011-PCM del 26 de Julio de 2011, se aprobó el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0", documento elaborado por la Comisión Multisectorial de Seguimiento y Evaluación para el Desarrollo de la Sociedad de la Información (CODESI).

Estos cambios presentan una nueva situación que, de aprovecharse adecuadamente, asegurarán el logro de los objetivos de la Agenda Digital Peruana 2.0, debiendo destacarse en primer lugar el liderazgo político que ha conducido a que nuestros últimos Presidentes de la República, mencionen en sus discursos anuales temas alusivos a la Sociedad de la Información, la cual ya es considerada una política de Estado.

En segundo lugar, debemos mencionar que este tema se está considerando mediante una intervención articulada e insertada en la planificación estratégica y operativa de los tres niveles de gobierno, implementados a partir de planes de acción sectoriales e institucionales donde se identifican, insertan y comprometen un conjunto de programas, proyectos y acciones para el desarrollo de la Sociedad de la Información.

En tercer término aunado a las políticas de Estado y las intervenciones sectoriales e institucionales, deben proveerse los recursos económicos y de otra índole, que aporten la sostenibilidad a las propuestas de las referidas políticas; todo ello articulado institucionalmente en un inicio por la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), y a partir del año 2017 por la Secretaría de Gobierno Digital en el Perú, pero que con el paso del tiempo, nos debe conducir al cuarto aspecto, que es la Institucionalización del tema de la Sociedad de la Información, con una entidad directriz que podría tener incluso rango ministerial.

Finalmente, es necesario que se dé un compromiso de las organizaciones públicas, instituciones privadas, sociedad civil y los medios académicos en su conjunto, que deben apoyar y participar activamente en el desarrollo de la Sociedad de la Información y del

Conocimiento en el Perú, así como velar por la correcta implementación de los enfoques que desarrolla la Agenda Digital Peruana 2.0.

Han sido múltiples los esfuerzos para avanzar en el desarrollo de nuestra Agenda Digital, la misma que al unísono con la Agenda Regional de América Latina y el Caribe, ha generado importantes avances en infraestructura, transparencia, inclusión digital, participación ciudadana digital, servicios electrónicos, tecnología e innovación y seguridad de la información, por mencionar los siete ejes sobre los cuales se ha trabajado el gobierno digital.

La Agenda Digital Peruana 2.0., se estructura en 08 Objetivos, contando cada uno con sus respectivas estrategias para alcanzarlos, por ello se crearon ocho grupos de trabajo, que dieron lugar a una serie de trabajos y proyectos de planificación, entre los que han destacado la aprobación y difusión del DNI electrónico, la aplicación del Plan Nacional de Gobierno Electrónico 2013 – 2017, y la Estrategia Nacional de Gobierno Digital 2017 – 2021. Apreciamos a continuación los ocho grupos de trabajo creados para el desarrollo de la sociedad de la información en el Perú:

Tabla 2

Grupo de Trabajo	Responsable	Participantes
Infraestructura TIC	MTC	MINSA, CONCYTEC, MINEDU, RENIEC
Competencias y capacidades TIC	MINEDU	CONCYTEC, MTPE, MEF, MTC, RREE
Sectores y las TIC	MINSA	MIDIS, MTPE, MININTER, RENIEC, MINEDU, MTC, CONCYTEC
I+D+I TIC	CONCYTEC	MINCETUR, MTPE, RENIEC, MINSA
Productividad y las TIC	PRODUCE	MTPE, MEF, RENIEC, PRODUCE
Industria TIC	MINCETUR	MTPE, MEF, MTC, CONCYTEC, RREE, PRODUCE
Gobierno Digital	PCM	MININTER, MTPE, MINSA, MEF, RENIEC, CONCYTEC, MINEDU
Institucionalidad de las TIC	MEF	MTC, RENIEC, MTPE, MIDIS, CONCYTEC, RREE

Además de lo antes mencionado, el Decreto Supremo que aprueba la Agenda Digital Peruana 2.0, dispone que los titulares de las entidades de la Administración Pública que conforman el Sistema Nacional de Informática (Decreto Legislativo Nº 604 del 30 de Abril de 1990) son los responsables de disponer en la entidad a su cargo, la adopción de

las acciones necesarias para el cumplimiento de los objetivos de la Agenda Digital Peruana 2.0 y la ejecución de sus estrategias.

Estas políticas nacionales sobre la Sociedad de la Información, no solamente revalorizan su importancia y deben generar nuevas actitudes en la sociedad, incluido el Gobierno, además de que influyen directamente en la protección de datos personales y los delitos informáticos, nuestros temas a investigar, cuyos alcances epistemológicos esperamos permitan enriquecer el conocimiento sobre la materia.

2.1.7 DE LA WEB 2.0 A LA WEB 4.0

En nuestros días, cuando requerimos encontrar una definición, jurídica o no, ya no recurrimos al diccionario común o especializado, lo que hacemos es ingresar a Google, el buscador más popular o megabuscador, y poner la palabra que deseamos definir, pero como nos surgen demasiadas posibilidades, entonces recurrimos a Wikipedia la enciclopedia más grande del mundo, así como Youtube es el repositorio de videos más grandes o Flickr el mayor contenedor de fotos, pero todos caracterizados por lo que se ha llamado web 2.0 (Web Social), es decir los medios de internet que no solamente nos proporcionan información, sino que también nos permiten adicionarla, lo que constituyó un gran cambio en Internet, cuya información a partir de allí comenzó a aumentar de manera rápida y descontrolada.

Pasando por la web 3.0 (Web Semántica), que buscó organizarnos mejor esa información que había aumentado de manera indiscriminada, llegamos en la presente década a la web 4.0 (Web Móvil), lo que ha constituido un nuevo gran cambio, ya que ha permitido en poco tiempo la masificación en el uso de Internet, accediendo a la red de redes por equipos móviles inteligentes, celulares que en diversos modelos, marcas y precios abundan hoy en nuestro medio, generando que en nuestro país exista prácticamente un celular por cada persona en la actualidad, que el año 2015 hayamos superado el 50% de usuarios diarios en la población nacional y que el 2018 posiblemente estemos bordeando el 80%. No obstante, que en la actualidad ya se está hablando de la web 5.0 (Web Sensorial) y el uso de las TICs a través de diversos y modernos equipos tecnológicos se vuelva algo usual más aún con la difusión del DNI electrónico, la Sociedad de la Información sigue siendo

un concepto con diversas definiciones, pero que es una realidad que alcanza a todos los países del orbe, y particularmente en el Perú, se está extendiendo desde las ciudades hacia el ámbito rural, con sus virtudes y defectos, entre los que destacan el reconocimiento de derechos fundamentales como la protección de datos personales y la existencia de la delincuencia informática, temas que nos preocupan y son parte de este estudio.

CAPÍTULO III: MARCO TEÓRICO CONCEPTUAL

3.1 ANTECEDENTES DE LA INVESTIGACIÓN.

3.1.1 ANTECEDENTES INTERNACIONALES

Encontramos las siguientes tesis de posgrado desarrolladas en los países de España y México, relacionadas con nuestro tema de investigación, las cuales hemos ordenado de la menos antigua a la más antigua, conforme se aprecia a continuación:

- Pascual Huerta (2017), en su Tesis de Doctor: "La Génesis del Derecho Fundamental a la Protección de Datos Personales", presentada en la Universidad Complutense de Madrid, España, nos dice que, "…se establecerán ciertos requisitos que deberán cumplirse para concluir que en un determinado contexto social hay "protección de datos". Estos requisitos son tres: en primer lugar, la existencia de normas jurídicas relativas al tratamiento de datos personales; en segundo lugar, que el contenido de esas normas sea el establecimiento de restricciones al tratamiento, que deben incluir un cierto derecho de disposición sobre los propios datos personales; finalmente, que la finalidad de las normas sea proteger a las personas, en el sentido más amplio posible, pero permitiendo o facilitando el derecho a su autonomía o

autodeterminación. Sólo cuando se den los tres a la vez existirá un auténtico esquema normativo de protección de datos".

- Gacitúa Espósito (2014) en su Tesis de Doctorado "El Derecho Fundamental a la Protección de Datos Personales en el Ámbito de la Prevención y Represión Penal Europea", presentada en la Universidad Autónoma de Barcelona, España, señala como una de sus conclusiones que "Respecto de los límites y excepciones al derecho a la protección de datos en el ámbito específico de la prevención y la represión penal, señalamos que este derecho, como cualquier otro, puede ser objeto de injerencias, ya sea producto de su interrelación con otros derechos, ya sea por la necesidad de satisfacer otros bienes y valores jurídicos relevantes en una sociedad democrática. No obstante, para que dichas limitaciones y excepciones sean toleradas, se deben cumplir ciertos estándares propios de un estado democrático de derecho, con la finalidad de precaver posibles afectaciones arbitrarias a los derechos fundamentales".

- García Guilabert (2014) en su Tesis de Doctorado "Victimización de Menores por Actos de Ciberacoso y Actividades Cotidianas en el Ciberespacio", presentada en la Escuela Internacional de Doctorado de la Universidad de Murcia, España, señala lo siguiente: "La conducta de grooming es, en realidad, un largo proceso, que comienza con la elección por parte del depredador sexual de un lugar que sea atractivo para el menor o adolescente (Choo, 2009), como chats, redes sociales, etc. Esto, llevado al espacio físico, podría ser equiparado a los lugares que frecuentan los menores como escuelas, parques, centros comerciales, etc. (Davidson et al., 2011); sin embargo, donde se inicia realmente la conducta, es cuando el depredador sexual selecciona a una víctima. Habitualmente, los agresores buscan víctimas más débiles, especialmente aquéllas con vulnerabilidades relacionadas con la incomprensión familiar o social (McAlinden, 2006). Una vez seleccionado el menor objeto de ataque, se acerca a él, fingiendo ser atractivo para el mismo, haciéndole creer que comparten hobbies o que entiende su situación. En otras palabras, le presta un interés particular para que se sienta especial y comienza a ganarse su confianza (Choo, 2009), pudiendo de esta forma obtener información del menor y consiguiendo, por ejemplo, que éste se conecte a la webcam y pose medio desnudo, o le mande fotografías comprometidas. Esta información permite al agresor continuar con el

acoso mediante la manipulación del menor, o la amenaza de difundir lo obtenido en Internet o a sus contactos personales (Pereda, Abad y Guilera, 2012)".

- Guzmán García (2013) en su Tesis de Doctorado "El Derecho Fundamental a la Protección de Datos Personales en México: Análisis desde la Influencia del Ordenamiento Jurídico Español", presentada en la Universidad Complutense de Madrid, España, señala lo siguiente: "El reconocimiento del derecho a la protección de datos personales es relativamente moderno y viene de la mano del desarrollo tecnológico. En la década de los 80´s los avances tecnológicos comienzan a permitir que la recogida, almacenamiento y utilización de datos personales (su tratamiento) se lleve a cabo de una forma antes inimaginable. El aumento del número de ordenadores personales, así como su mejora técnica y la conexión entre ellos propicia que se puedan almacenar un mayor número de datos personales, que se produzca con más facilidad la movilidad de los mismos, y por lo tanto, que las posibilidades de su conocimiento por terceros, también sean mayores".

- Saltor, Carlos (2013) en su Tesis de Doctorado "La Protección de Datos Personales: Estudio Comparativo Europa - América con especial análisis de la Situación Argentina", presentada en la Universidad Complutense de Madrid, España, señala lo siguiente: "… otorga al titular de los datos, los siguientes derechos sobre sus datos personales: a) el derecho a la información sobre sus datos personales; b) el derecho al acceso a los datos personales; c) el derecho a conocer el contenido de la información; d) el derecho de rectificación de sus datos personales; e) el derecho de actualización de sus datos personales; y f) el derecho a la supresión de sus datos personales; g) derecho a impugnar las valoraciones personales fundamentadas en el resultado de un tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado; h) derecho a la gratuidad del ejercicio a la rectificación, actualización y supresión de datos personales".

3.1.2 ANTECEDENTES NACIONALES

Encontramos las siguientes tesis de posgrado relacionadas con nuestro tema de investigación, realizadas en el Perú, las cuales hemos ordenado por orden de antigüedad, comenzando por la más reciente, como se aprecia a continuación.

- Núñez Ponce (2016), en su Tesis de Doctor "Derecho de Identidad Digital en Internet", presentada en la Universidad Nacional Mayor de San Marcos, señala lo siguiente: "Una de las principales prioridades con la dación de la Nueva Ley Peruana de Datos Personales, debe ser extender y consolidar en la sociedad una auténtica cultura de la protección de datos personales en el contexto de la sociedad de la información y un uso intensivo de internet y las tecnologías de comunicaciones digitales e informática".

- Morales Delgado (2016) en su Tesis "La Inseguridad al Utilizar los Servicios de Redes Sociales y la Problemática Judicial para Regular los Delitos Informáticos en el Perú", presentada en la Universidad Señor de Sipán, Pimentel – Perú, efectúa un estudio conceptual de los delitos informáticos en el Perú, y cómo está legislación no soluciona los problemas de la inseguridad ante el accionar de ciberdelincuentes en el uso de las redes sociales. Al respecto precisa que los delitos informáticos "…se encuentra íntimamente asociada al desarrollo tecnológico informático", habiéndose reportado los primeros casos de ciberdelincuencia en el año 1958.

- Eslava Morales (2016) en su Tesis "El Principio Constitucional de la Resocialización de los Penados en la Era del Internet: Entre el Tratamiento de Datos Personales y el Derecho al Olvido, a propósito de la Sentencia C-131/12 del Tribunal de Luxemburgo", presentada en la Universidad Nacional de Trujillo – Perú, señala que "Ante el masificado tratamiento de datos personales en el Internet, el derecho al olvido es un mecanismo razonable y eficaz para la cautela del principio constitucional a la resocialización del ciudadano que ha cumplido una pena, sin considerar excepciones por reincidencia, cualidad del sujeto o importancia del delito imputado".

- Mejía Verástegui (2010) en su Tesis de Magister "La Globalización en el Desarrollo de una Cultura de Protección de los Derechos Humanos y su Influencia en el Perú" presentada en la Universidad Nacional Mayor de San Marcos, Lima – Perú, señala lo siguiente: "La globalización es un proceso económico, tecnológico, social y cultural a gran escala, que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo unificando

sus mercados, sociedades y culturas, a través de una serie de transformaciones sociales, económicas y políticas que le dan un carácter global. La globalización es a menudo identificada como un proceso dinámico producido principalmente por las sociedades que viven bajo el capitalismo democrático o la democracia liberal y que han abierto sus puertas a la revolución informática, plegando a un nivel considerable de liberalización y democratización en su cultura política, en su ordenamiento jurídico y económico, y en sus relaciones internacionales".

- La Rosa Vásquez (2002) en su tesis: "Los Desafíos Jurídicos frente a las Nuevas Tecnologías de la Información y Comunicación: El Caso de la Firma Digital" presentada en la Pontificia Universidad Católica del Perú-Lima, Perú, dice lo siguiente: "Las nuevas tecnologías de la información y de la comunicación constituyen un desafío para el Derecho porque, éste debe adaptarse a los cambios que se dan en la realidad, ante las nuevas herramientas que se utiliza para intercambiar información"

3.2 BASES TEÓRICAS O CIENTÍFICAS

3.2.1 DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

En nuestro país, es recién en el año 2011 con la dación de la Ley N° 29733 "Ley de Protección de Datos Personales", que se reconoce con esta denominación a este derecho de la persona humana. Si bien, ya teníamos los antecedentes constitucionales, tal como lo había precisado el Tribunal Constitucional, en diferentes Sentencias a las que se refiere al derecho a la autodeterminación informativa (Ver Sentencia del Exp. N° 1797-2002-HD/TC del 29 de Enero de 2003), este derecho sólo se podía defender de manera posterior a su violación o amenaza de violación a través de un proceso de Hábeas Data. La Ley tiene como aspecto destacado, que genera una organización y mecanismos administrativos, bajo la dirección de la Autoridad Nacional de Protección de Datos Personales (Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales), que van a permitir la protección del derecho de manera previa, es decir, el desarrollo legislativo del derecho constitucional, ha permitido ampliar y mejorar su ámbito de protección.

3.2.1.1. ORÍGENES.

Si bien, mantenemos el criterio de que el derecho a la protección de datos personales, conocido también en doctrina como autodeterminación informativa, existe desde que existe el ser humano, al ser inherente a su propia naturaleza, su reconocimiento normativo se origina de manera confusa conjuntamente con otros derechos, como a la privacidad, a la intimidad y al honor. Si bien existe cierta información que desde el derecho romano ha existido una clara protección jurídica al honor, como un aspecto de la personalidad con una doble dimensión espiritual y moral, es recién a finales del siglo XIX, que se da un reconocimiento a la intimidad tal como la concebimos en la actualidad. (Pascual, 2017, p. 60).

Es a fines del siglo XIX, con ocasión de la "Segunda Revolución Industrial", que encontramos los inicios de las tecnologías de la información, cuando con el uso de la electricidad, se crea el primer telégrafo eléctrico, y con él una serie de implicancias jurídicas relativas a los datos íntimos de las personas.

Es en esa época también, en que, ante los inicios de la decadencia del liberalismo en Europa, el Estado comienza a adquirir un rol interventor en la vida de la sociedad, que comienza a generar registros de las personas con datos detallados de las mismas. Ese deseo estatal de registrar los datos de las personas no se va a detener, y con un naciente afán democrático, se crean los primeros ficheros o bancos de datos personales con fines electorales, otros para el reclutamiento de soldados y otros con objetivos de recaudación de tributos.

De manera paralela, en Estados Unidos desde su Constitución producto de la revolución norteamericana, se comienzan a practicar los censos de la población, los cuales se afianzan en la segunda mitad del siglo XIX, generando bancos de datos de las personas.

Como podemos apreciar, el origen del Derecho a la Protección de Datos Personales, se encuentra relacionado con el tratamiento de los datos de las personas, a través de la creación de ficheros (como son conocidos en España los Bancos de Datos Personales),

con diferentes fines de carácter estatal, los cuales dan lugar a los primeros compromisos de confidencialidad de los datos de las personas.

A pesar de su antigüedad, en el Perú, el reconocimiento del Derecho a la Protección de Datos Personales es relativamente reciente, las Sentencias del Tribunal Constitucional que tratan el derecho bajo la denominación de Autodeterminación Informativa, son del presente siglo, la Ley después de proyectos fallidos, inspirada en la legislación española y la legislación argentina, se aprueba el año 2011, entrando en vigencia en su integridad el año 2013, por lo cual, los orígenes del reconocimiento de este derecho en el Perú, es bastante reciente.

3.2.1.2. ANTECEDENTES.

El crecimiento en el uso de las tecnologías de la información y las telecomunicaciones, tanto en el ámbito estatal como privado, ha permitido que en muchas ocasiones los datos personales sean utilizados para fines distintos a los que originalmente fueron recabados, y que sean transmitidos con objetos distintos a los que el dueño (titular) de los datos aceptó confiarlos. Ello afecta la esfera de privacidad de la persona y, en ocasiones, lesiona otros derechos y libertades.

En este sentido nos parece acertado lo señalado por el Dr. Erick Iriarte, cuando hace referencia a tres etapas de la evolución tecnológica, una primera en que el Estado monopoliza la información, una segunda en que la información se democratiza y va de la mano con la difusión de las computadoras personales y una tercera en donde el tráfico de la información es masivo gracias a Internet, (Iriarte, 2013. p. 101) y que es en donde se comienza a poner en grave riesgo nuestro derecho a la autodeterminación informativa, gracias a la facilidad con que nuestros datos son transferidos de un banco de datos a otro, o transmitidos a otros países en cuestión de segundos o fracciones de segundo.

Con el fin de equilibrar las fuerzas entre un individuo y aquellas organizaciones públicas o privadas que recaban datos personales, surgió en Europa el concepto de la protección de los datos personales, a través del cual, el titular de dichos datos tiene el derecho y la libertad de elegir qué desea comunicar, cuándo y a quién, manteniendo el control sobre su información personal.

El Consejo de Europa es considerado el promotor de la tendencia legislativa en materia de protección de datos, con ocasión del Convenio Nº 108 del Consejo de Europa aprobado en 1981, sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. (Saltor, 2013, p. 158)

En el desarrollo constitucional, la protección de datos personales es uno de los más nuevos derechos que se reconocen a la persona humana, como sucede en el artículo 8° de la Carta de los Derechos Fundamentales de la Unión Europea, que fue aprobado el 7 de diciembre de 2000.

Tan sólo seis años después, el Comité de Ministros del Consejo de Europa resolvió declarar el 28 de enero como el "Día de la Protección de los Datos Personales", con motivo del 25° aniversario de la firma del Convenio N° 108 del Consejo de Europa.

3.2.1.3. DATOS PERSONALES Y DATOS SENSIBLES

Los datos personales son cualquier información relacionada con la persona, así como cualquier otro dato que pueda servir para identificar a la persona. Este tipo de datos te permiten interactuar con otras personas, con una o más organizaciones, así como ser sujeto de derechos.

En tal sentido, los datos personales no se refieren solo a los datos íntimos como muchas veces se les ha confundido, sino también a cualquier tipo de dato que identifique o permita la identificación de una persona, y esté en conocimiento o tratamiento de terceros. Por ello, son datos personales el nombre, DNI o documento de identidad, una fotografía o grabación de voz, la IP, un pin de teléfono, un avatar, la dirección de email, el curriculum vitae, la orientación sexual, la condición de consumidor de un producto o de cliente de una empresa, la situación crediticia, un diagnóstico o el historial médico, los hábitos de consumo, la cuenta de banco, la afiliación a un club o red social, etc.

Con el fin de organizarlos, podemos clasificar a los datos personales de la manera siguiente:

- Datos de identificación.- Podemos incluir a los nombres, apellidos, domicilio, firma, documentos de identidad, fecha de nacimiento, edad, nacionalidad, estado civil, sexo, imagen, dirección de IP, teléfono, WhatsApp y otros chats, redes sociales (Facebook, Twitter, Instagram, LinkedIn, etc.), emails o correos electrónicos (Gmail, Hotmail, Outlook, Yahoo, Live, Corporativos, etc.), entre los principales.

- Datos laborales.- Incluimos al currículum vitae, puesto de trabajo, empleador, domicilio laboral, correo electrónico institucional, teléfono del trabajo, legajo personal, boletas de pago, sanciones, licencias, seguridad social, historial en la empresa, sociedades comerciales, organizaciones profesionales, etc.

- Datos patrimoniales.- Agrupamos principalmente a los datos bancarios y tributarios, como información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos anuales, información de consumos, situación de solvencia, tarjetas de crédito y débito, etc.

- Datos de salud.- Son las relacionadas con nuestro estado de salud, historias médicas físicas o electrónicas, enfermedades que ha padecido, vacunaciones, enfermedades crónicas, antecedentes psicológicos y psiquiátricos, internamiento en centros de salud (hospitales o clínicas), operaciones quirúrgicas, etc.

- Datos académicos.- Son los relacionados con nuestra educación, entre los que podemos citar a la trayectoria educativa primaria y secundaria, estudios superiores técnicos o profesionales, calificaciones, matriculas habilitantes, certificados de estudios, condición de alumno, títulos obtenidos, grados académicos alcanzados, trabajos de investigación, publicaciones, etc.

- Datos ideológicos.- No sólo incluimos las opciones políticas, sino todos aquellos vinculados con nuestro estilo de vida, como pueden ser creencias religiosas, afiliación política, agrupación sindical, organizaciones de la sociedad civil, asociaciones culturales, clubes con fines recreativos o deportivos, hermandades y logias, etc.

- Datos sobre la vida y hábitos sexuales.- En este conjunto se encuentran los referidos al origen étnico, características raciales, árbol genealógico, orientación sexual, análisis de perfiles, etc.

- Datos físicos de la persona.- Muy usados por la policía para identificación de delincuentes, muchas veces son llamados biométricos, y pueden ser tipo de sangre, ADN, huellas dactilares, tipo de cara, estatura, peso, contextura corporal, discapacidades, color de piel, iris y cabellos, tipo de nariz y orejas, señales particulares como cicatrices, etc.

Podemos diferenciar a los datos, como aquellos que nos identifican, es decir, la información que hace referencia a una persona física específica, y que permite sin lugar a dudas, saber a qué persona se refiere sin necesidad de ningún tipo de averiguación posterior. El ejemplo más claro de ello lo constituye el Documento Nacional de Identidad (DNI), ya que la información que contiene, identifica de manera precisa a una persona física determinada.

Por otro lado, tenemos los datos que nos hacen identificables, es decir la información que hace referencia a una persona física sin decirnos de quién se trata, pero que nos aporta información suficiente para poder llegar a averiguar su identidad. Verbigracia el ADN.

Dentro de la amplitud de los datos personales, también se diferencia a un grupo de ellos llamados datos sensibles, por estar más ligados con la esfera íntima de la persona. Entre ellos tenemos al origen racial o étnico, el estado de salud, la información biométrica, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas, las preferencias sexuales. Estos datos requieren mayor protección y la ley establece un tratamiento especial para ellos.

La ley peruana les da un tratamiento diferenciado, especialmente en lo que se refiere a la forma de otorgar el consentimiento para su uso, ya que la disposición general establece que el consentimiento debe ser previo, expreso, informado e inequívoco, agregándose

para los datos sensibles que el titular de los datos debe otorgar su consentimiento por escrito.

Karin Castro nos dice que un rasgo esencial y a la vez determinante para calificar a un dato personal como sensible, es que alude a cuestiones cuya divulgación o comunicación a terceros puede dar lugar a prácticas discriminatorias (Castro, 2008, p. 264).

3.2.1.4. PRINCIPIOS

Los principios que rigen la protección de datos personales son principios generales del derecho, que por ende, van a permitir interpretar e integrar las normas sobre la materia; asimismo, el tratamiento de datos personales y su registro en ficheros o bancos de datos, debe efectuarse respetando dichos principios, que nuestra legislación precisa que se trata de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Seguridad, Disposición de Recurso y Nivel de Protección Adecuado.

3.2.1.4.1. Principio de Legalidad

El principio de legalidad reconocido en diferentes ramas del derecho, remonta sus orígenes al siglo XVIII, como parte de una reacción contra la arbitrariedad, el abuso del poder y la inseguridad jurídica, generando que se constituye en elemento importante de las ideas de Hans Kelsen en el siglo XIX, ya que en la medida que surgen las normas positivas, es decir la legislación escrita, el principio de legalidad adquiere su real trascendencia dentro del ámbito jurídico.

Se entiende por principio de legalidad a la prevalencia de la ley sobre cualquier actividad o función del poder público, esto quiere decir que todo aquello que emane del Estado debe estar regido por la ley, y nunca por la voluntad de los individuos; sin embargo, el Art. 4° de la Ley N° 29733 "Ley de Protección de Datos Personales", se refiere a él de una forma un tanto escueta, puesto que dice *"El tratamiento de los datos personales se hace conforme a lo establecido en la ley"*. Agregando que se encuentran prohibida la recopilación de datos por medios fraudulentos, desleales o ilícitos. De esa manera, amplía la concepción estricta del principio de legalidad referido a la licitud y la ilicitud, ya que la norma también lo asocia con la "lealtad" y por lo tanto alude indirectamente al principio

de la buena fe, y al hacer mención al término “fraudulento”, lo está relacionando además con el principio de “honestidad”.

3.2.1.4.2. Principio de Consentimiento

El principio del consentimiento es uno de los principios más característicos en la protección de datos personales, ya que el titular del banco de datos personales al administrar los datos del titular, requiere de manera obligatoria contar con su consentimiento, el cual como ya hemos mencionado, debe ser previo, informado, expreso e inequívoco.

Al respecto, es importante resaltar que el consentimiento debe ser previo a la obtención de los datos personales, y para su otorgamiento previo se debe estar informado del objeto o fines para los que serán usados, ya que tal como nos dice Blossiers, cuando una empresa vía Internet va a recolectar datos personales, debe informar sobre la existencia de un archivo automatizado, la finalidad de ese archivo, los destinatarios de sus informaciones, el carácter obligatorio o facultativo de sus respuestas y las consecuencias de la obtención de datos o su negativa de proporcionarlos. (2003, p. 387)

El consentimiento ha sido más analizado desde la óptica contractual, ligándolo a la manifestación de voluntad, elemento fundamental del acto jurídico, siendo susceptible en consecuencia, de los vicios de la voluntad enunciados en el Código Civil, que son el error, el dolo, la violencia y la intimidación.

En esta área el consentimiento también es una manifestación de la voluntad, más no con fines contractuales, sino con un fin distinto, que es el de autorizar el tratamiento de los datos personales contenidos en un fichero o banco de datos.

En este aspecto, el Art. 5° de la Ley N° 29733 “Ley de Protección de Datos Personales” es aún más escueta al decir únicamente respecto al principio de consentimiento que: *“Para el tratamiento de los datos personales debe mediar el consentimiento de su titular”*; sin embargo, el Reglamento de dicha Ley, se encarga de ampliar un poco su acepción, al señalar que el consentimiento debe ser libre, previo, expreso, informado e inequívoco, de lo cual nos percatamos, que se ha añadido el término “libre”, ligándolo

directamente con los vicios de la manifestación de la voluntad, ya que de existir uno de ellos, el consentimiento será nulo al afectar la libertad del individuo que manifestó su autorización para el uso de sus datos personales.

El Reglamento de la Ley de Protección de Datos Personales, en su Art. 7°, se ha preocupado aún más en identificar con precisión la expresión del consentimiento, al decir *"... No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara"*.

El consentimiento referido al tratamiento de datos sensibles, también ha sido precisado en el Art. 14° del Reglamento, al decir que "… el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular".

Al respecto, la autoridad nacional de protección de datos personales, a través de su Director, ha precisado que resulta obvio, que no es válido el consentimiento para tratamiento de datos sensibles obtenidos de forma verbal, ya sea presencialmente o a través de una llamada telefónica al no ser formas escritas de la manifestación de la voluntad, la cual ha superado las modalidades del "lápiz y papel", habiéndose hecho extensivo su desarrollo también en el entorno digital. (Quiroga, 2013).

El principio de consentimiento se erige seguramente como uno de los fundamentales dentro de nuestra normatividad sobre Protección de Datos Personales, por ello lo consideramos como un aspecto destacable de nuestra Ley N° 29733; en doctrina, el consentimiento se suele considerar no sólo como un principio sino también como un derecho que se deriva del derecho fundamental a la protección de datos personales, en tal sentido, consideramos que tiene esa doble perspectiva de principio y derecho, que le brinda una especial importancia.

3.2.1.4.3. Principio de Finalidad

En general, cuando hablamos de finalidad nos referimos de manera abstracta, a aquello que simboliza a la causa o la razón, el objetivo para el cual se realiza determinada acción, se tiene determinado comportamiento, etc. La finalidad es la justificación que se establece antes de comenzar algo y a la cual se quiere llegar cuando uno está en el proceso de realizarlo.

En materia de datos personales, la finalidad es el objeto para el cuál van a ser utilizados los datos, lo que debe ser informado al titular de los datos antes de que brinde su consentimiento. En efecto, el Art. 6° de la Ley N° 29733 "Ley de Protección de Datos Personales", nos dice que: "Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación…".

La autoridad nacional en la materia, precisa que el principio de finalidad quiere decir que lo que se puede hacer con los datos, es aquello que responda a la finalidad autorizada por el titular de los datos y no se extiende a otra u otras finalidades, que no le hayan sido informadas o establecidas de manera inequívoca como tal, al momento de su recopilación. (Quiroga, 2013)

Por su parte, el Reglamento de la Ley de Protección de Datos Personales, específica respecto a la finalidad, que debe ser expresada con claridad, sin lugar a confusión, es decir, la información que se debe proveer al titular de los datos personales, sobre los objetos para los que serán utilizados sus datos personales, no deben dar margen alguno a error sobre el tratamiento a que serán destinados.

Tratándose de datos sensibles, la creación de bancos de datos personales que los contengan, solo se justifica si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.

3.2.1.4.4. Principio de Proporcionalidad

El principio de proporcionalidad es uno de los que más alcances tiene en las distintas ramas del derecho, en tal sentido, este principio exige una relación ponderada de los medios empleados con el fin perseguido, para evitar el sacrificio innecesario o excesivo de los derechos fundamentales.

El Tribunal Constitucional peruano se ha referido múltiples veces a este principio, como en la Sentencia del expediente N° 045-2004-AI del 29 de octubre de 2005, cuando dice que *"el principio de proporcionalidad que normalmente es empleado para examinar las intervenciones legislativas en los derechos constitucionales, ahora, es proyectado para examinar el supuesto concreto de una eventual contravención del derecho-principio de igualdad".* También ha extendido este principio al test de proporcionalidad, que permite analizar y determinar en un caso concreto, si ha existido proporcionalidad o no; el indicado test incluye evaluar la idoneidad, la necesidad y la ponderación del asunto o proporcionalidad en sentido estricto, que son los tres subprincipios que conforman o integran el principio de proporcionalidad.

El test de idoneidad consiste en la relación de causalidad, de medio a fin, entre el medio adoptado y el fin propuesto. El test de necesidad tiene como finalidad principal verificar la existencia o no de medios alternativos al elegido y, de haberlos, si son menos gravosos que este último. El test de proporcionalidad en sentido estricto, es denominado también test de la ponderación que persigue la optimización de las posibilidades jurídicas, a diferencia de la idoneidad y necesidad que tienen como propósito la optimización de las posibilidades fácticas.

El principio de proporcionalidad implica, un equilibrio entre el fin a alcanzar y los medios para lograrlo. Por ello, aplicándolo en relación a la protección de datos personales, implica una equivalencia entre los fines para los cuales fueron introducidos en un Banco de Datos Personales y el tratamiento que se les dé. Nuestra norma en materia de protección de datos personales, al referirse sobre el principio de proporcionalidad, alude a un trato adecuado, relevante y no excesivo respecto a la finalidad para la que ha sido

creado el Banco de Datos Personales. (Art. 7° de la Ley de Protección de Datos Personales).

El Dr. José Alvaro Quiroga León, cuando se desempeñaba como Director General de Protección de Datos Personales, precisa que de acuerdo al principio de proporcionalidad cuando se trata de datos personales, debe tratarse sólo la información que resulte imprescindible para alcanzar la finalidad autorizada, o sea, el tratamiento de los datos se restringe únicamente a los datos que sean relevantes para cumplir con los fines para los que fueron recopilados. (Quiroga, 2013).

3.2.1.4.5. Principio de Calidad

Este principio se refiere a la calidad de los datos recopilados en los bancos de datos personales, tanto en cuanto a cantidad y exactitud de los mismos, la Ley de Protección de Datos Personales, lo precisa bastante bien al decir lo siguiente:

> "Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento" (Ley N° 29733, 2011, Art. 8).

En tal sentido, la calidad no sólo se refiere a la exactitud y precisión con que se ajustan a la realidad, sino también a la calidad de los bancos de datos personales para conservarlos con total seguridad. El Art. 9° del Reglamento de la Ley precisa que, en virtud al principio de calidad, se presume que los datos proporcionados por el titular son exactos.

3.2.1.4.6. Principio de Seguridad

El término seguridad proviene de la palabra securitas del latín. Cotidianamente nos referimos a la seguridad como la reducción del riesgo o también a la confianza en algo o alguien. Con el desarrollo de las tecnologías de la información y la comunicación, el término a adquirido nuevos alcances, puesto que los riesgos que cada día se van incrementando más y más, generados por personas mal intencionadas que intentan tener

acceso a los datos de nuestros ordenadores, ha dado lugar no sólo a principios sino también a toda una industria de seguridad informática.

La seguridad informática comprende al software y al hardware, pero evidentemente, por su diversidad e importancia, los medios tecnológicos para su protección se ven centrados en el software; sin embargo, no hay que olvidar los datos que se transfieren a través de la informática, lo que da lugar a pensar en la seguridad de la información, que es algo más amplio y da mérito para que las organizaciones valoren y le presten especial atención para garantizar su confidencialidad, llegando a convertirse en muchos casos en información privilegiada.

Daniel Ricardo Altmark define la seguridad informática como *ciberseguridad* o seguridad de tecnologías de la información, que es el área de la informática enfocada en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. (2012, p. 254)

En relación a la protección de datos personales, las medidas de seguridad incluyen los cuidados para evitar la adulteración, pérdida o desviación de la información, ya sea que los riesgos provengan de la acción humana, intencional o no, o del medio técnico utilizado. En tal sentido, los responsables de la seguridad de los bancos de datos son el titular y el encargado de su tratamiento, los cuales no deben limitarse a las medidas técnicas, sino que deben incluir también las organizativas y legales, como precisa el Art. 9° de nuestra Ley de Protección de Datos Personales, que permitan garantizar plenamente la seguridad de los datos personales.

En tal sentido, la seguridad en el ámbito del tratamiento de los datos personales, va más allá de las normas, procedimientos, métodos y técnicas destinados a que el software, hardware y redes de computadoras sean seguros y confiables, que es el ámbito del que se ocupa normalmente la seguridad informática, sino que incluye ámbitos administrativos y jurídicos que completen todo el circuito de seguridad para garantizar que el tratamiento de los datos personales, no sea expuesto a riesgos, ni objeto de atentados de ninguna clase.

La Autoridad Nacional de Protección de Datos Personales, dentro de sus funciones de elaborar las herramientas para garantizar el adecuado tratamiento de los datos personales, ha aprobado mediante Resolución Directoral N° 019-2013-JUS/DGPDP la Directiva de Seguridad de la Información, que es un instrumento facilitador para guiar a las organizaciones, titulares de Bancos de Datos y personas encargadas de su tratamiento, para lograr que actúen conforme a las normas sobre Protección de Datos Personales vigentes en nuestro país y de esa manera, evitar que el principio de seguridad sea una norma que no cuente con el conocimiento ni los instrumentos adecuados para su cumplimiento; la misma que se ha actualizado al reestructurarse la Autoridad Nacional y convertirse en Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

3.2.1.4.7. Principio de Disposición de Recurso

Este principio dentro de todos los que ya hemos tratado, seguramente es el que menor tratamiento doctrinario tiene, aludiendo la Ley N° 29733 "Ley de Protección de Datos Personales", a la posibilidad de disponer con los medios para hacer valer nuestros derechos en materia de protección de datos personales.

La referida Ley, establece expresamente lo siguiente:

> "Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales". (Ley N° 29733, 2011, Art. 10)

De la lectura previa, podemos considerar que este es un principio garantista, pues prevé que los titulares de los datos, tengamos los medios para hacer cumplir nuestros derechos, cuando estos son objeto de un indebido tratamiento.

Por un lado nos habla de las vías administrativas, y estas son las que está implementando la propia Ley de Protección de Datos Personales y su Reglamento, al crear toda una estructura administrativa dentro del Ministerio de Justicia y Derechos Humanos, que permitirá que los titulares del derecho, puedan presentar sus denuncias y/o quejas, a fin de lograr que los derechos generados en torno a sus datos personales, no sean vulnerados.

Asimismo este principio alude a las vías jurisdiccionales, al respecto ya existía el Proceso de Hábeas Data, instaurado por la Constitución Política del Perú de 1993 y desarrollado en el Código Procesal Constitucional, pero al generar una estructura administrativa, le brinda además la posibilidad de poder recurrir a la vía judicial en un Proceso Contencioso Administrativo, cuando no se acoja su derecho o se encuentre en desacuerdo con lo resuelto administrativamente.

3.2.1.4.8. Principio de Nivel de Protección Adecuado

Este es un principio que por su nombre pudiera parecer redundante, ya que, al referirnos a la protección de datos personales, evidentemente estamos aludiendo a que esa protección debe tener niveles adecuados para su objeto. Es por ello, que la direccionalidad que ha recibido este principio, se encuentra en el ámbito de la transferencia internacional de datos, aludiendo de manera especial, al nivel de protección que brinda el país al cual se van a transferir, para determinar si son adecuados y semejantes al del país que los transfieren.

En efecto, nuestra ley vigente, recoge en ese sentido este principio al referirse al tratamiento de los datos personales, desde la perspectiva de su flujo transfronterizo, es decir, cuando son transferidos a organizaciones de otros países.

A este respecto, existen una serie de normas complementarias, tanto en la Ley de Protección de Datos Personales como en el Art. 18° de su Reglamento, que por un lado precisa que el flujo transfronterizo de datos personales se refiere a la transferencia de datos personales fuera del territorio nacional, más por otro establece que ese flujo de datos personales solo se producirá, si el país destinatario mantiene niveles de protección semejantes a los que se provee por nuestra legislación nacional.

Adicionalmente, también abre la posibilidad de que se realice el flujo transfronterizo de datos personales, cuando el país destinatario no cuente con un nivel de protección adecuado, siempre y cuando se garantice que el tratamiento de los datos personales se efectúe con el nivel de protección establecido en nuestro país.

Al respecto, el Reglamento de la Ley de Protección de Datos Personales es bastante específico, al establecer lo siguiente:

> "Los flujos transfronterizos de datos personales serán posibles cuando el receptor o importador de los datos personales asuma las mismas obligaciones que corresponden al titular del banco de datos personales o responsable del tratamiento que como emisor o exportador transfirió los datos personales". (Reglamento de Ley N° 29733, 2013, Art. 24)

3.2.1.5. BANCOS DE DATOS PERSONALES Y SU REGISTRO

Como veremos más adelante, la Dirección de Registro Nacional de Protección de Datos Personales es una unidad orgánica que depende de la Dirección General de Protección de Datos Personales, responsable del registro en el que las entidades públicas y privadas inscribirán sus bancos de datos personales.

Esa Dirección es la responsable de realizar la inscripción en el Registro Nacional de Protección de Datos Personales, siendo responsable también, de evitar la divulgación de la información contenida en los bancos de datos personales materia de inscripción, asegurando así la existencia de los bancos de datos personales y la información que se contiene en ellos.

El Registro Nacional de Protección de Datos Personales, es la unidad de almacenamiento destinada a contener principalmente la información sobre los bancos de datos personales de titularidad pública o privada y tiene por finalidad dar publicidad de la inscripción de dichos bancos.

Sobre los Bancos de Datos Personales, estos son un conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso, cuya administración puede estar a cargo de una institución privada o de una entidad pública.

La creación, modificación o cancelación de bancos de datos personales de administración pública y de administración privada se sujetan a lo establecido por la Ley y lo precisado

por su Reglamento, que en sus artículos 81 y siguientes, precisa el procedimiento de inscripción de los Bancos de Datos Personales en el Registro Nacional.

3.2.1.6. DERECHOS DEL TITULAR DE DATOS PERSONALES

Internacionalmente se conoce a los subderechos del Derecho Fundamental a la Protección de Datos Personales, con la sigla "ARCO", que alude a los derechos de Acceso, Rectificación, Cancelación y Oposición, respecto al tratamiento de sus datos contenidos en un Banco de Datos Personales.

El derecho de acceso, confiere al titular de datos personales la posibilidad de obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados y las razones que motivaron su recopilación.

El derecho de rectificación del titular de datos personales, incluye también su derecho a la actualización o inclusión de sus datos personales materia de tratamiento, cuando estén en todo o parte inexactos, se encuentren incompletos, o cuando se advierta omisión, error o falsedad.

El derecho de cancelación, implica el suprimirlos del Banco de Datos Personales, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopiladas o cuando hubiera vencido el plazo establecido para su tratamiento.

El derecho de oposición, permite al titular de los datos personales, el oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

La Ley de Protección de Datos Personales peruana, reconoce no solamente esos cuatro derechos, sino que alude también al derecho a un tratamiento objetivo, por medio del cual, el titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa.

Agrega también el derecho a la tutela, el mismo que alude a la posibilidad del titular de los datos personales, de recurrir a la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data, como medios de protección de su derecho fundamental a la protección de datos personales.

También añade el derecho a ser indemnizado, que le confiere al titular de datos personales que se ha visto afectado por el incumplimiento de la Ley N° 29733 "Ley de Protección de Datos Personales", por el accionar del titular del Banco de Datos Personales o por el encargado de su tratamiento o por actividades de terceros, a obtener la indemnización correspondiente, otorgada por la Dirección General de Protección de Datos Personales a través de procedimiento administrativo ante la misma.

Por último, nuestra norma considera también el derecho a ser informado, que debe ser previo a prestar el consentimiento, por una parte, pero también puede ser posterior respecto a cualquier variación o modificación en el Banco de Datos Personales, incluido el traslado a otro responsable del mismo. El derecho del titular de datos personales a ser informado, incluye el recibir en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, la información sobre la finalidad para la que sus datos personales serán tratados, quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y encargado del tratamiento de sus datos personales; lo que puede hacerse a través de la publicación de las condiciones de privacidad, cuando los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas.

3.2.1.7. INFRACCIONES Y SANCIONES

La Ley de Protección de Datos Personales, bajo los principios de proporcionalidad y legalidad, prevé tres tipos de infracciones, las leves consistentes en realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia; recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos; no modificar o rectificar los datos

personales objeto de tratamiento cuando se tenga conocimiento de su carácter inexacto o incompleto; no suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios, pertinentes o adecuados para la finalidad para la cual fueron recopilados o cuando hubiese vencido el plazo para su tratamiento; no inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo treinta y cuatro de la Ley; o el dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento; las que son sancionables entre media y cinco unidades impositivas tributarias (UIT).

Las infracciones graves, cuya sanción va entre cinco y diez UITs, consisten en no atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales; dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular; realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia; recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos; utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación; obstruir el ejercicio de la función fiscalizadora de la Autoridad; incumplir la obligación de confidencialidad; o no inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo treinta y cuatro de la Ley, a pesar de haber sido requerido para ello por la Autoridad en el marco de un procedimiento sancionador.

Las infracciones muy graves pueden ser sancionadas entre cincuenta y cien UITs, previendo como tales el dar tratamiento a los datos personales contraviniendo las obligaciones contenidas en la Ley y su Reglamento, cuando con ello se impida o se atente contra el ejercicio de otros derechos fundamentales; recopilar datos personales mediante medios fraudulentos, desleales o ilícitos; suministrar documentos o información falsa a la Autoridad Nacional; no cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador; o no cumplir con las medidas correctivas establecidas por la Autoridad como resultado de un procedimiento trilateral de tutela.

3.2.1.8. AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ

La Autoridad Nacional de Protección de Datos Personales (ANPDP) se encarga de supervisar, administrar y actualizar los datos personales, así como resolver las reclamaciones formuladas por los titulares de datos personales en tutela de sus derechos de acceso, rectificación, cancelación y oposición. Asimismo, emite opinión técnica vinculante respecto de los proyectos de normas que regulen los datos personales y emite las directivas para la adecuada aplicación de la Ley de Protección de Datos Personales y su Reglamento.

La Autoridad Nacional también recibía el nombre de Dirección General de Protección de Datos Personales, denominación con la que forma parte de la estructura organizativa del Ministerio de Justicia, se encuentra dividida en cuatro Direcciones (Dirección de Registro Nacional de Bancos de Datos Personales, la Dirección de Normatividad y Asistencia Legal, la Dirección de Supervisión y Control y la Dirección de Sanciones), a través de las cuales desempeña funciones fiscalizadoras y sancionadoras, para evitar que haya un uso indebido o ilegal de los datos personales en el Perú, por lo tanto se encarga de supervisar e imponer multas cuando se transgrede o vulnera dicha normatividad.

La función general de la Autoridad Nacional de Protección de Datos Personales, es cumplir y hacer cumplir la normatividad vigente en materia de protección de datos personales, en ese sentido, tiene funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras, las mismas que son detalladas en el Art. 33 de nuestra Ley de Protección de Datos Personales vigente.

Entre sus funciones administrativas están el representar al país en la materia, generar mecanismos de cooperación internacional y administrar el Registro Nacional de Protección de Datos Personales, manteniéndolo actualizado.

Entre sus funciones orientadoras destaca el promover campañas de difusión y promoción sobre la protección de datos personales, así como fortalecer una cultura de protección de los datos de los niños y de los adolescentes.

Entre las funciones normativas se encuentra el emitir opinión técnica sobre los proyectos de normas en la materia y emitir las directivas necesarias para la mejor aplicación de lo previsto en la Ley N° 29733 "Ley de Protección de Datos Personales" y su Reglamento, especialmente en materia de seguridad de los bancos de datos personales.

Las funciones resolutivas se centran en conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento.

Sus funciones fiscalizadoras se basan en supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales, así como iniciar fiscalizaciones de oficio o por denuncia de parte.

Por último, sus funciones sancionadoras básicamente son el imponer multas por la comisión de infracciones previstas en la Ley de Protección de Datos Personales, en general por incumplimiento a la misma o su Reglamento.

En la actualidad la Autoridad Nacional de Protección de Datos Personales, dentro de la estructura orgánica del Ministerio de Justicia, se denomina Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

3.2.1.9. CARACTERÍSTICAS PRINCIPALES DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DE PERÚ.

Esta Ley regula la forma y condiciones en que deben utilizarse los datos personales por parte de los encargados de las bases de datos a quienes el titular de los mismos pone a disposición de aquellos encargados. Tiene por objeto garantizar la protección de la información personal del titular para que este pueda ejercer el derecho a decidir, de manera libre e informada, sobre el uso que las entidades privadas o públicas darán a los datos.

La Ley tiene como finalidad el garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2° numeral 6 de la Constitución Política del Perú

a través de su adecuado tratamiento, en un marco de los demás derechos fundamentales que en ella se reconocen.

Según la Ley N° 29733 "Ley de Protección de Datos Personales", a través del tratamiento de datos personales, se podrá realizar cualquier operación o procedimiento técnico automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por trasferencia o por difusión o cualquier otra forma que facilite el acceso, conexión o interconexión de los datos personales.

Entre sus características principales podemos mencionar el haber creado una Autoridad Nacional en la materia, el reconocimiento de una serie de sub derechos, que abren la posibilidad del titular de datos, de hacer garantizar el respeto a los mismos ante cualquier violación por la que se vea afectado, la creación del Registro Nacional de Bancos de Datos Personales, la enunciación de principios como el de consentimiento y la especificación de infracciones clasificándolas en leves, graves y muy graves, con sanciones imponibles que van desde media hasta cien unidades impositivas tributarias.

3.2.1.10. IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES EN LA INVESTIGACIÓN.

Luego de que hemos revisado el marco teórico y normativo en el Perú sobre protección de datos personales, es necesario entender todo ello para enfatizar algunos aspectos puntuales que nos sirvan para la discusión final de nuestra investigación.

En tal sentido los principios y derechos del titular de los datos personales es un aspecto de gran importancia, en la medida que la población conoce la importancia de proteger sus propios datos, tomará mejores medidas para la aplicación de los principios y ejercicio de derechos que ya mencionamos, por una parte debemos destacar el consentimiento, toda vez que es fundamental para que el propio titular ejerza un control sobre el uso de sus datos; a través del consentimiento, podemos mencionar los derechos internacionalmente reconocidos con la sigla "ARCO", que alude a la posibilidad de Acceso, Rectificación, Cancelación y Oposición en el uso de los datos personales, como diferentes

manifestaciones del consentimiento, ya que todos se encuentran enmarcados en la facultad del titular de determinar los aspectos de su información personal y familiar que pueden ser de público conocimiento y cuál debe estar restringida a determinadas personas.

Por otra parte, la labor preventiva que ofrece la legislación sobre protección de datos personales, consideramos que se encuentra dentro de la actividad de prevención y control que realiza la autoridad nacional, a través de diferentes mecanismos entre los que destaca el Registro Nacional de Bancos de Datos Personales, que permite conocer y supervisar que nuestros datos no sean utilizados indiscriminadamente y menos para fines delictivos.

3.2.1.11. DERECHO COMPARADO SOBRE PROTECCIÓN DE DATOS PERSONALES.

La legislación internacional en materia de protección de datos personales, tiene sus primeros antecedentes en Europa, ya que Suecia en 1973, Alemania en 1977, Francia, Dinamarca y Noruega en 1978, las emitieron hasta que la célebre Sentencia del Tribunal Constitucional Federal (Bundesverfassungsgericht) de la República Federal de Alemania, en el año 1983, que identifica el derecho a la autodeterminación informativa, considerando a la intimidad como uno de sus atributos, establece que la idea de autodeterminación se refiere a decidir cuáles son los límites respecto a las situaciones de su propia vida, que sirvió como referente para que otros países posteriormente, reconozcan la protección de datos personales como un atributo de cada ser humano. (García, 2007)

En esos países, existen aspectos regulatorios semejantes al que tenemos en la actualidad al Perú, como por ejemplo nos señala Carrasco, que la Ley Federal Alemana, admite que el tratamiento de datos personales es lícito únicamente cuando la propia ley lo autorice o cuando el interesado lo hubiese consentido por escrito; asimismo en Italia, los datos sensibles sólo pueden ser objeto de tratamiento, cuando el titular lo consienta por escrito. (2008, p. 113-114).

Asimismo, a fin de evitar indebidos tratamientos de datos personales, a nivel europeo se tiene el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal del Consejo de Europa (Convenio 108 de

Estrasburgo del 28 de enero de 1981) y respecto al cual, muchos han reorientado su normatividad, dándole tres de ellos rango constitucional, otros jerarquía de ley y algunos un rango infralegal. (Blossiers, 2003, p. 150-151).

Para el presente trabajo, queremos referirnos con mayor detalle, a algunos antecedentes legislativos de Latinoamérica y de España, que nos permitan entender mejor el derecho a la protección de datos personales desde una perspectiva internacional.

3.2.1.10.1 Argentina.

Consideramos relevante tratar en primer término a este país, que junto con España son las legislaciones en las cuales se inspiró nuestra vigente ley peruana. La Ley 25.326 del año 2000, es la vigente en Argentina, y en ella se regula aspectos que consideramos fundamentales en la labor de prevención de los delitos informáticos, como son los mecanismos y resultados que ofrece el consentimiento (Art. 5°), lo cual obviamente, pone en gran parte bajo la responsabilidad del titular de los datos su protección, porque él será el que deberá consentir su uso o no y limitará las actividades para las que podrán ser usados. Esto que puede sonar un tanto irrelevante, es de especial importancia en la prevención de delitos informáticos en nuestro país, pero para esto, la población en general, en especial los menores de edad, deben conocer la importancia de proteger sus datos personales para no brindar el consentimiento para su uso indiscriminadamente.

Al igual que la legislación peruana, la argentina diferencia a los datos personales de los datos sensibles, que requieren especial protección por estar más ligados a la esfera íntima de la persona, como son los relativos a salud, vida sexual, afiliación sindical, creencias u opiniones y origen racial y étnico.

En Argentina, que es el país pionero en la materia en América Latina, se creó un órgano de control dependiente del Ministerio de Justicia y Derechos Humanos, al igual que en el Perú, denominado Dirección Nacional de Protección de Datos Personales, que hoy es la Agencia de Acceso a la Información Pública y Protección de Datos Personales (https://www.argentina.gob.ar/aaip/datospersonales), la cual asiste y asesora a las

personas acerca de los alcances y defensa de los derechos en materia de protección de datos personales; asimismo, mantiene el registro permanente de los bancos de datos, entre otras funciones precisadas en el Art. 29° de la Ley 25.326. La referida Ley, tiene como en nuestro país sustento constitucional, toda vez que los principios de protección de datos personales se encuentran presentes en la Constitución Nacional de la República Argentina, así como en la Ley de Habeas Data y en las Constituciones Provinciales de ese país.

Es importante destacar la labor de prevención del delito que existe en Argentina, en base a la difusión y conocimiento del derecho a la protección de datos personales, por intermedio de videos animados, que son de fácil comprensión para menores de edad y adultos, con consejos prácticos para proteger su información, campañas promovidas no solo por la autoridad en la materia, sino también por la Oficina Nacional de Tecnología de Información, la Secretaría de Gabinete y Gestión Pública, la Subsecretaría de Tecnologías de Gestión, u otras más concretas como la realizada por la Defensoría del Pueblo en Buenos Aires, denominada “Conéctate seguro”.

3.2.1.10.2 Colombia

El año 2012, se aprobó la Ley 1581, cuyo objeto es desarrollar el Art. 15 de la Constitución colombiana, que recoge el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos; el cual señala que el Tratamiento de los datos sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular, creando para su control y dirección, a una autoridad de protección de datos, que funciona como una Delegatura de la Superintendencia de Industria y Comercio (http://www.sic.gov.co/), el cual tiene a su cargo el Registro Nacional de Bases de Datos, que es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país colombiano.

Es importante mencionar, que en la aprobación de esta Ley, se han tenido una serie de consideraciones que son parte de la participación ciudadana e institucional en su dación. En tal sentido se señala que, en el derecho comparado existen dos modelos de protección de datos ampliamente reconocidos: un modelo centralizado y un modelo sectorial. El

primer modelo, implementado en los países europeos y, con algunas modificaciones, en la propia Unión Europea, parte de una categoría general de datos personales y de la idea de que cualquier tratamiento de ellos es considerado per se potencialmente problemático, razón por la cual debe sujetarse a unos principios y garantías mínimas comunes, susceptibles de ser complementadas con regulaciones especiales -según el tipo de dato y los intereses involucrados, pero que de ninguna manera suponen una derogación de los estándares de protección generales. En contraste, el modelo sectorial no parte de una categoría común de datos personales y por ello no se considera que todos estos datos deban estar sometidos a la misma regulación mínima. Este modelo sectorial se inspira en la idea de la autorregulación de los mercados, razón por la cual el Estado solamente participa en la protección de ciertos datos en ámbitos en los que se presenta un alto riesgo de lesión de la intimidad, como la esfera financiera, la salud y los derechos de los niños.

En tal sentido, se aprecia que la protección de datos personales de los menores de edad, es un rasgo común a toda legislación pues se encuentra incluido en los diferentes modelos legislativos sobre protección de datos personales.

3.2.1.10.3 Chile

En este país, la protección de datos de carácter personal se encuentra regulada por la Ley sobre protección de la vida privada, Ley 19.628, cuya última versión es del año 2012, la que diferencia los datos personales de los datos sensibles igual que en el Perú, siendo estos últimos los datos personales que se refieren a las características físicas o morales de las personas, relativos a su vida privada o intimidad, por lo cual, se requiere el consentimiento para estos datos, incluyendo también a los datos de salud .

Sin embargo, en el país del sur, no se prevé una autoridad nacional, prefiriéndose un sistema de control sectorial como ya hemos mencionado, cabe precisar, que en el año 2018, se encuentra en debate la modificación de la Constitución chilena, para incorporar la protección de datos personales como un derecho constitucional, encontrándose también en curso en el año 2018, la modificación de la Ley 19.628, a fin de crear una Agencia de Protección de Datos Personales siguiendo el modelo español.

3.2.1.10.4 Ecuador

El Art. 66 de la Constitución de Ecuador, a través del proyecto de Ley de Protección de Datos, busca desarrollar el contenido y el ámbito de defensa de los derechos a la protección de datos, privacidad e intimidad; en consecuencia, como podemos apreciar, Ecuador es un país que está buscando implementar una legislación sobre protección de datos personales al igual que sus países vecinos, en donde aún existe mucha controversia sobre aspectos que deberían considerarse en el mismo.

No obstante, lo antes señalado, en Ecuador sí existe una Dirección Nacional de Registro de Datos Públicos, pero que se ve limitada en la medida que su acceso a los datos registrados en las empresas privadas no es completo, ni tiene atribuciones de supervisión o control sobre los mismos; motivo por el cual, en el año 2018 viene desarrollando un nuevo proyecto de Ley de Protección de Datos Personales, que absuelva las expectativas de los diferentes sectores que no se vieron satisfechos por los anteriores.

3.2.1.10.5 España

A fin de terminar está revisión de la legislación comparada sobre protección de datos personales, es necesario referirnos a nuestro otro referente que ha inspirado nuestra Ley de Protección de Datos Personales vigentes, que es el europeo país de España.

La Ley Orgánica 15/1999 es la Ley de Protección de Datos de Carácter Personal, que se encuentra vigente en España, que denomina a los datos de carácter personal, como cualquier información concerniente a personas físicas identificadas o identificables. Asimismo, lo que en nuestro país se conoce como Banco de Datos Personales, en España se denomina “Fichero”, que viene a ser todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Esa Ley al igual que la nuestra, crea una Autoridad Nacional, con la diferencia de que para ellos es un organismo autónomo que no depende de ningún sector ministerial, lo que para algunos, le brinda mayores mecanismos de acción. La Agencia de Protección de

Datos, es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones; entre las cuales destaca la de controlar el cumplimiento de la legislación en la materia y en especial la referida a los derechos de los titulares de los datos, entre los que destaca el principio del consentimiento, previsto en su art. 6°, el cual establece que para el tratamiento de los datos de carácter personal, se requiere el consentimiento inequívoco del afectado; el que debe ser expreso y por escrito cuando se trata de datos sensibles, que dicha legislación los denomina como datos especialmente protegidos.

Por lo señalado, podemos apreciar gran similitud con la legislación peruana, lo cual también sucede en lo relativo a la creación de un Registro Nacional de Ficheros o Bancos de Datos Personales, lo que va a permitir tener un mayor y mejor control sobre el registro y tratamiento de los datos, protegiéndolos de esa manera ante el uso indebido por terceros.

Hay que agregar que en España al igual que en nuestro país, la protección de datos personales también se encuentra en su Constitución de 1978, cuyo artículo 18.4 establece que la ley pondrá los límites para el uso de la información, que permita garantizar el honor y la intimidad personal y familiar de los ciudadanos. Pero además en Europa existe la Directiva 95/46/CE del Parlamento Europeo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos; motivo por el cual, a diferencia de américa, el ámbito de protección internacional de los datos personales se encuentra mejor consolidado.

Cabe destacar que la Agencia Española de Protección de Datos - AEPD, explota mucho más los medios web que las otras autoridades nacionales, para realizar labores de difusión de la normativa sobre la materia, con consejos muy concretos, que permiten desarrollar una mejor labor preventiva, como la forma para eliminar fotos o videos de Internet, ya sea se encuentren en redes sociales, como Facebook, Instagram o Twitter, o en buscadores incluido el megabuscador Google. Otro ejemplo destacable es cómo ejercer el derecho a la supresión o cancelación en buscadores de Internet, proporcionando 5 aspectos fundamentales sobre el derecho al olvido, respecto al cual ya existe la Sentencia del Tribunal de Justicia de la Unión Europea del 13 de mayo de 2014.

Al hablar del Internet y las redes sociales, nos dice que en buena parte de los casos los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que los usuarios aportamos, por lo que debemos ser conscientes de los riesgos que esto puede suponer para nuestra seguridad y privacidad. (AEPD, 2018)

No obstante lo antes señalado, hay que adicionar una esfera de prevención que es de destacar, dada la amplia información para menores de edad en la materia, a través del slogan "tú decides en Internet", que resalta la importancia de que el propio titular sea el que proteja sus datos personales, brindando información variada con videos y otros medios didácticos, e incluso con una guía para centros educativos, a fin de que den a conocer la importancia de saber utilizar ese recurso informático tan maravilloso y versátil que es Internet.

3.2.2 DELITOS INFORMÁTICOS

3.2.2.1 DEFINICIÓN.

También llamado delito electrónico, es aquella conducta típica, antijurídica y culpable en la que la computadora, sus técnicas y funciones desempeñan un papel transcendente, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente, cual es el logro de algún perjuicio de tipo patrimonial a su víctima. Por tanto, es el de cualquier medio informático para obtener un beneficio indebido en perjuicio del sujeto pasivo (Salinas, 2008).

Julio Téllez Valdez, el padre del derecho informático en Latinoamérica, define el delito informático, como "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin". (2009)

Esta definición que alude al delito informático en sentido genérico, sigue siendo utilizada en diversidad de artículos; sin embargo, a fin de tener una mayor precisión conceptual, se prefiere utilizar en la actualidad la de "delitos de alta tecnología", que incluye también a los delitos por medio de celulares.

Sin embargo, por su campo de ejecución dentro de la doctrina penal, se tiende a diferenciar a los llamados delitos computacionales de los propiamente delitos informáticos como lo reconocen diversos autores (Pérez Luño, Téllez, Dávara, Gutiérrez Francés, González Rus, Tiedemann). Adicionalmente a ello, debemos tener en cuenta que en nuestro Código Penal mediante Ley Nº 27309 del 16 de Julio de 2000, se incorporó un nuevo capítulo denominado "Delitos Informáticos", lo que implica en sentido estricto, que en nuestra legislación sólo se denomina así al Intrusismo Informático (Art. 207-A) y al Sabotaje Informático (Art. 207-B); sin embargo, a lo largo de la lectura del Código Penal, podemos encontrar diversas tipificaciones delictivas que incorporan o pueden incluir para su comisión, el haber sido realizados por medios electrónicos o informáticos.

La diferenciación conceptual se centra en el bien jurídico protegido, ya que si en los delitos informáticos en sí, lo que se protege es la información y la computadora, en los delitos computacionales el bien jurídico protegido puede ser cualquier otro.

El bien jurídico protegido mediante los delitos informáticos, es la información, la cual está compuesta por todos los datos a los que podemos acceder vía Internet, y que es la materia prima para el conocimiento, que constituye la riqueza en una sociedad de la información, de ello podemos deducir que al afectarse la información estamos afectando un bien patrimonial; es conveniente adicionar que, la información incluye también los soportes lógicos, constituidos por los programas informáticos o software, que van a permitir la distribución de la información.

En cuanto a la información, podemos encontrar, tres tipos de conductas delictivas que pueden atentar contra la misma: las conductas lesivas a la confidencialidad de la información, las conductas lesivas a la integridad de la información y las conductas lesivas a la disponibilidad de la información.

Para ello es preciso entender que debemos apreciar la información como un proceso que incluirá actividades de almacenamiento, de tratamiento y de transmisión.

No obstante, lo antes señalado, con la dación de la Ley N° 30096, denominada "Delitos Informáticos", no se toma en consideración esa distinción conceptual y se aglutina en una sola norma tanto a los propiamente llamados delitos informáticos con los delitos computacionales, dejando existentes inclusive algunos otros delitos tipificados en el

Código Penal y que se realizan por medios electrónicos. Esto genera una confusión sobre el bien jurídico que se protege en cada uno, puesto que en los delitos informáticos el bien jurídico protegido preeminentemente es la información, y serán secundarios otros bienes jurídicos que se protegen como el patrimonio o la fe pública. Ello resulta ilógico en delitos como el Fraude Informático, siendo el Fraude un típico delito contra el patrimonio, pero al haberle dado esta singular tipificación, se protegería en primer lugar la información y en segundo lugar el patrimonio. De manera semejante sucedería con otros delitos señalados en la nueva ley.

Esta imprecisión conceptual, y otras deficiencias en las conductas típicas descritas en la Ley N° 30096 "Ley de Delitos Informáticos", generó un gran debate público en diferentes medios de comunicación escritos, radiales, televisivos y por Internet sobre la conveniencia o no de dicha Ley. Los medios oficialistas comandados por representantes del Ministerio de Justicia alababan la modernidad de dicha ley e incorporación de nuevas figuras penales como el "grooming", señalando que nos acercaba a las disposiciones de la Convención del Cibercrimen de Budapest; mientras que los especialistas opositores, enfatizaban que una tipificación imprecisa permitiría abusos y desmanes en la aplicación de la ley, que por último, generaría problemas y facilitaría la defensa para los ciberdelincuentes que llegasen a un proceso penal.

En efecto, tan grande fue la fuerza de la voz de los especialistas opositores, que en Marzo del año 2014 se promulgó la Ley N° 30171, que modificó la tipificación de todos los delitos informáticos previstos en la Ley N° 30096, con excepción de uno y derogó el Art. 6°, que fue el delito más criticado por los medios de comunicación dado que el mismo atentaría directamente contra las actividades de la prensa para investigar posibles hechos delictivos.

Finalmente, si bien no se han recogido todas las conductas delictivas previstas en la Convención sobre el Cibercrimen de Budapest, estas nuevas leyes, constituyen un acercamiento a la misma, dejándose de lado el proyecto existente en el Ministerio de Relaciones Exteriores, de ratificar dicha Convención. Cabe mencionar que la misma se aprobó inicialmente por representantes de la Unión Europea el 23 de noviembre de 2001 en Budapest, siendo un instrumento importante para la persecución de los ciberdelincuentes, dado que estos con mucha facilidad cometían los delitos desde

distintos países a los que se producían los efectos del delito, por lo que una legislación uniforme facilita la intervención de las policías especializadas para su persecución. Tanto fue su éxito, que con el paso de los años dicha Convención ha sido ratificada por países de distintos lugares del mundo.

3.2.2.2 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Podemos encontrar diversas opiniones respecto a las características de los delitos informáticos, motivo por el cual, preferimos recoger la de uno de los maestros de mayor prestigio en Latinoamérica, que es el mexicano Julio Téllez Valdez, quién nos señala como las principales características de los delitos informáticos a las siguientes:

1) Conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

2) Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto trabaja.

3) Son acciones de oportunidad en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

4) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

5) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse.

6) Son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de regulación por parte del derecho.

7) Son sumamente sofisticados y relativamente frecuentes en el ámbito militar.

8) Presentan grandes dificultades para su comprobación, esto, por su mismo carácter técnico.

9) En su mayoría son imprudenciales y no necesariamente intencionales.

10) Ofrecen facilidades para su comisión a los menores de edad.

11) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

12) Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley.

3.2.2.3 TIPOS DE DELITOS INFORMÁTICOS EN EL PERÚ.

La Ley N° 30096 "Ley de Delitos Informáticos", modificada mediante la Ley N° 30171, considera únicamente delitos dolosos, es decir no se admite la existencia de delitos informáticos que se puedan cometer accidentalmente o por negligencia, denominados culposos, sino que en ellos tiene que imperar la intencionalidad, mencionando al margen de las modificatorias al Código Penal, los delitos siguientes:

- Delito de Acceso Ilícito (Intrusismo Informático).
- Delito de Atentado contra la Integridad de Datos Informáticos (Sabotaje Informático).
- Delito de Atentado contra la Integridad de Sistemas Informáticos (Sabotaje Informático)
- Delito de Proposiciones a menores con fines sexuales por medios Informáticos (Grooming)
- Delito de Interceptación de Datos Informáticos
- Delito de Fraude Informático. (Delito Informático contra el Patrimonio)
- Delito de Suplantación de Identidad mediante las TIC (Delito Informático contra la Fe Pública).
- Delito de Abuso de Mecanismos y Dispositivos Informáticos.

3.2.2.4 DELITO DE ACCESO ILÍCITO.

Este delito en doctrina es considerado como el de intrusismo informático, en consecuencia, su antecedente legislativo lo encontramos en el derogado artículo 207-A del Código Penal; sin embargo, el Art. 2° de la Ley de Delitos Informáticos modificada, le ha dado una nueva visión, al tipificarlo de la manera siguiente:

> "El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa". (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.4.1 Concepto y Esquematización.

Este delito lo que reprime es la conducta de acceder a un sistema informático, vulnerando la seguridad creada para que esto no suceda, así como también reprime la conducta que exceda las facultades concedidas en ese sentido. Se trata de un delito de mera actividad, porque basta con el cumplimiento del tipo penal para su realización, sin importar el daño o resultado posterior.

Dentro del léxico informático delictivo, el hacking suele ser el término que corresponde con "acceso ilícito", el cual mediante la vulneración de puertas lógicas o passwords, permiten acceder en forma no autorizada a datos o sistemas informáticos ajenos.

Estas conductas de acceso no autorizado, englobadas bajo el término hacking o más concretamente hacking blanco, se caracterizan porque están impulsadas por la insaciable curiosidad de los hackers en encontrar en los sistemas informáticos la existencia de agujeros (o puertas falsas) y fallos o a qué se deben, pero una vez conseguido este propósito dentro de la máquina, no borran ni destruyen nada. Conviene indicar que en ocasiones se suele utilizar el término hacking para aludir de forma comprensiva a cualquier ataque a un sistema informático, incluidas conductas de cracking o de ciberpunking, las cuales son impulsadas por una finalidad dañina de diversa índole y que tienen una diferente trascendencia en el ámbito penal. (Rueda, 2009)

Otras conductas como el cracking, el phreaker o el ciberpunking, también son accesos ilícitos a sistemas informáticos, pero que por sus consecuencias presentan mayor gravedad y configuran al mismo tiempo delitos informáticos de mayor gravedad.

En la tabla siguiente, podemos apreciar la esquematización del delito de Acceso Ilícito.

Tabla 3		
N°	**TEMA**	**DESCRIPCION**
01	BIEN JURIDICO	La Información
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	Titular del Sistema Informático
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) Accede sin autorización a todo o parte de un sistema informático C) Vulnerando medidas de seguridad establecidas para impedirlo.
05	PENA PRINCIPAL	No menor de 1 ni mayor de 4 años
06	PENA ACCESORIA	De 30 a 90 días multa

3.2.2.4.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con este delito, es la "información", entendida de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), la cual se encuentra contenida en bases y/o bancos de datos o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico y es la importancia actual del "valor económico" de la información en una sociedad en donde se usan de manera cotidiana las tecnologías de la información y la comunicación, lo que ha hecho que se incorpore como bien jurídico tutelado.

Podemos considerar diferentes bienes jurídicos secundarios, como la Intimidad, que es el respeto que se debe tener hacia lo que una determinada persona guarda para sí y que no es ni debe ser de conocimiento público. El patrimonio, la propiedad, la indemnidad sexual y la libertad sexual pueden verse en casos también afectadas por el acceso ilícito, pero esto implicaría el concurso de delitos con otras figuras tipificadas en la misma ley o que

se encuentran reguladas en el Código Penal vigente, el cual contiene también una serie de delitos que se cometen por medios informáticos.

3.2.2.4.3 Sujetos Activo y Pasivo.

El sujeto activo es aquel que realiza todo o parte de una conducta regulada en el tipo penal del Delito de Acceso Ilícito. Estas personas que resultan ser autores de "Delitos Informáticos", tienen por común denominador poseer ciertas características que no presentan los delincuentes comunes, esto es, tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aunque en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Esta condición del sujeto activo se ajusta al término inglés de hacker.

Por su parte, el sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término, tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso del delito de Acceso Ilícito, las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados en red.

3.2.2.4.4 Figuras Agravadas.

El Art. 2° de la Ley de Delitos Informáticos no los menciona, sin embargo, debe tenerse en consideración las que se encuentran establecidas en el Art. 11° de la misma Ley y que elevan la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, es decir 5 años y 4 meses en este caso, cuando concurre alguna de las circunstancias que detallamos a continuación:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
- El agente comete el delito con el fin de obtener un beneficio económico.
- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.5 DELITO DE ATENTADO CONTRA LA INTEGRIDAD DE DATOS INFORMÁTICOS

El Art. 3° de la Ley de Delitos Informáticos, lo tipifica de la manera siguiente:

> "El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa". (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.5.1 Concepto y Esquematización.

Este delito reprime no sólo el acceso ilegítimo a los datos informáticos, sino también la acción dañosa contra los mismos, lo que lo diferencia claramente del delito de Acceso Ilícito.

Dentro de su tipificación contiene una serie de verbos rectores:

- Dañar (causar detrimento, perjuicio, menoscabo).
- Introducir (entrar en un lugar).
- Borrar (desvanecer, quitar, hacer que desaparezca algo).
- Deteriorar (empeorar, degenerar).
- Alterar (estropear, dañar, descomponer).
- suprimir (hacer cesar, hacer desaparecer).
- Hacer inaccesibles (bloquear, inutilizar o estropear el acceso).

Cualquiera de esas acciones aplicadas a los datos informáticos, configuran este delito, podemos apreciar por tal, que se trata de un delito de mera actividad, porque solamente se requiere el cumplimiento del tipo penal, la sola realización de la conducta ilícita sin importar el resultado posterior.

Conductas de ciberpunking, que propiamente son conductas de daños informáticos o de vandalismo electrónico, a través de virus gusano que se van multiplicando alcanzando cada vez más archivos o con programas de destrucción progresiva, mediante los cuales se ven concretadas en asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones que generan modificación o destrucción de datos. (Rueda, 2009)

Este artículo es compatible parcialmente con el Art. 4º del Convenio contra la Cibercriminalidad de Budapest, aprobado por la unión europea el año 2001, que sanciona el atentado contra la integridad y la disponibilidad del dato informático, haciendo alusión al *acto deliberado que dañe, borre, deteriore, altere o suprima datos informáticos.*

En ese sentido, el Perú está siguiendo el estándar mínimo recomendado en ese Convenio, con las adiciones que ya han sido materia del comentario, estas adiciones, si bien no siguen la línea teleológica del estándar, no comprometen su interpretación ni las acciones de cooperación internacional que se deriven de su invocación y aplicación en la lucha transfronteriza contra el cibercrimen. En la tabla siguiente, podemos apreciar la esquematización del delito de Atentado Contra la Integridad de Datos Informáticos.

Tabla 4

N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Información
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	Persona Jurídica o Natural que posee los Datos Informáticos
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) 1. Dañar Datos informáticos 2. Introducir Datos informáticos 3. Borrar Datos informáticos 4. Deteriorar Datos informáticos 5. Alterar Datos informáticos 6. Suprimir Datos informáticos 7. Hacer Inaccesibles Datos informáticos.
05	PENA PRINCIPAL	No menor de 3 ni mayor de 6 años
06	PENA ACCESORIA	De 80 a 120 días multa

3.2.2.5.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con este delito, es la "información" contenida en los datos informáticos, entendida de manera específica en este caso, como la información que se encuentra en bases y/o bancos de datos; para lo cual debemos recordar que la misma Ley de Delitos Informáticos define a los datos informáticos como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

Al igual que en el acceso ilícito, podemos considerar distintos bienes jurídicos secundarios protegidos, como la intimidad, cuando se da en concurso con el delito de Interceptación de Datos Informáticos, el patrimonio cuando se da en concurso con el delito de Fraude Informático, la indemnidad y la libertad sexual cuando se da en concurso con el delito de Grooming.

3.2.2.5.3 Sujetos Activo y Pasivo.

El sujeto activo es aquel que realiza la conducta regulada en el tipo penal del Delito de Atentado contra la Integridad de Datos Informáticos. Como ya hemos señalado, las personas que actúan como sujeto activo de este delito, tienen por común denominador el tener conocimientos y habilidades para acceder y manipular los datos y los programas que permiten el funcionamiento de los sistemas informáticos.

Por su parte, el sujeto pasivo es la persona natural o jurídica, pública o privada que posee los datos informáticos, sobre los que recae la actividad típica del sujeto activo.

3.2.2.5.4 Figuras Agravadas.

El Art. 3° tampoco las menciona, por lo que se continúan aplicando las establecidas en el Art. 11° de la misma Ley y que elevan la pena hasta en un tercio por encima del máximo legal fijado, es decir en este caso, hasta 8 años de pena privativa de la libertad, cuando concurre alguna de las circunstancias siguientes:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El agente comete el delito con el fin de obtener un beneficio económico.

- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.6 DELITO DE ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS

El Art. 4° de la Ley de Delitos Informáticos, lo tipifica de la manera siguiente:

> "El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa". (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.6.1 Concepto y Esquematización.

Este delito lo que reprime es la conducta lesiva contra un sistema informático para inutilizarlo en parte o su totalidad, a fin de que no sea accesible, no funcione o no sea posible que brinde sus servicios, a través de alguna de las acciones siguientes:

Inutilizar.- Hacer inútil, vano o nulo algo.
Impedir.- Estorbar o imposibilitar la ejecución o acceso.
Entorpecer.- Dificultar, obstaculizar.
Imposibilitar.- Quitar la posibilidad de ejecutar o conseguir algo.

Su antecedente legislativo es el delito de Sabotaje Informático, el cual puede producirse por diferentes medios:

- BOMBA LÓGICA.- introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.

- RUTINAS CANCER.- Son distorsiones al funcionamiento del programa, la característica es la auto reproducción.

- GUSANOS.- Se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse.

- VIRUS INFORMATICO Y MALWARE.- Elementos informáticos que destruyen el uso de ciertos antivirus.

Dentro del léxico informático delictivo, el cracking se relaciona con este delito, ya que suelen ser conductas caracterizadas por eliminar o neutralizar los sistemas de protección de un sistema informático que impide su copia no autorizada o la de una aplicación shareware que impide su uso, pasada una determinada fecha, con vulneración del sistema informático y muchas veces asociado a temas patrimoniales o de derechos de autor.

Estas conductas tienen en común dos notas: en primer lugar, para su realización es necesario que, previamente, se haya producido un acceso ilícito a un sistema informático; en segundo lugar, dichas conductas recaen sobre los sistemas informáticos o sobre la información que se contiene en los mencionados sistemas, con la finalidad de su perturbación, destrucción o modificación. (Rueda, 2009).

Los crakers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como “piratas electrónicos.” La característica que les diferencia de los hackers, es que los crackers usan programas ya creados que pueden adquirir, normalmente vía internet, mientras que los hackers crean sus propios programas. (Villavicencio, 2014).

En la tabla siguiente, siguiendo el orden que ya hemos señalado anteriormente, podemos apreciar la esquematización del delito de Atentado contra la Integridad de Sistemas Informáticos.

Tabla 5		
N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Información
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	El titular o poseedor del sistema informático.
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) 1. Inutilizar total o parcialmente un Sistema informático 2. Impedir el acceso a un Sistema informático 3. Entorpecer el funcionamiento o la prestación de servicios de un Sistema informático 4. Imposibilitar el funcionamiento o la prestación de servicios de un Sistema informático
05	PENA PRINCIPAL	No menor de 3 ni mayor de 6 años
06	PENA ACCESORIA	De 80 a 120 días multa

3.2.2.6.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con este delito, es la "información", la cual puede ser almacenada, tratada o transmitida a través del sistema informático. Al respecto, la norma precisa que un sistema informático es todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Al igual que en el delito anterior, podemos considerar diferentes bienes jurídicos secundarios, como la Intimidad, el patrimonio, la propiedad, la fe pública, la indemnidad sexual y la libertad sexual; sin embargo, cabe la misma atingencia de que por lo general implicará la comisión en concurso con otros delitos informáticos considerados en la misma ley.

3.2.2.6.3 Sujetos Activo y Pasivo.

El sujeto activo es aquel que realiza la conducta regulada en el tipo penal del Delito de Atentado contra la Integridad de Sistemas Informáticos. Esta persona que puede ser cualquiera, tiene como aspecto semejante el conocimiento y la habilidad en el manejo de sistemas informáticos.

Por su parte, el sujeto pasivo es el titular del sistema Informático afectado, pudiendo ser también el poseedor o inclusive el usuario del Sistema Informático. En tal sentido, la víctima o sujeto pasivo, pueden ser individuos, instituciones públicas o privadas, o inclusive gobiernos que usan sistemas automatizados de información, conectados o no en red.

3.2.2.6.4 Figuras Agravadas.

El Art. 4° no las menciona, por lo que nuevamente aplicamos los agravantes establecidos en el Art. 11° de la Ley N° 30096, que eleva la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, es decir, en este caso 8 años de pena máxima, cuando concurre alguna de las circunstancias que detallamos a continuación:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El agente comete el delito con el fin de obtener un beneficio económico.

- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.7 DELITO DE PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS (GROOMING)

El Art. 5° de la Ley de Delitos Informáticos, lo tipifica de la manera siguiente:

> "El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal". (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.7.1 Concepto y Esquematización.

El grooming se define como un comportamiento sexual ilícito que comprende una cadena ordenada de conductas, cuyo primer eslabón comienza cuando el agente -cualquier persona mayor de edad- mediante Internet u otra red análoga, procede a contactar con un menor de edad -a veces haciéndose pasar por otro menor-, luego cuidadosamente va desarrollando lazos emocionales con él, va registrando datos personales de este, utilizando esa información lo va seduciendo y/o provocando, para finalmente llegar al último eslabón de la cadena, en el que se manifiesta el verdadero propósito que lo ha motivado: el solicitar u obtener del menor material pornográfico, o proponerle llevar a cabo actividades de connotación sexual con él.

Este delito también llamado ciberacoso infantil, es entendido por Peña Labrine, como el conjunto de "acciones desplegadas por un adulto, para tomar contacto con un niño, a través de cualquier medio tecnológico con el objeto de entablar una relación o crear una conexión emocional con él, ganarse su confianza, disminuir sus inhibiciones y finalmente determinarlo para involucrarse en situaciones de carácter sexual". (Peña, 2014, p. 4)

Definitivamente, esta figura delictiva tiene su motivación en la realidad que se vive día a día, debido a la masificación del uso de las tecnologías de la información y las telecomunicaciones, a través de las cuales muchas personas obtienen o buscan el

aprovechamiento sexual sobre menores de edad, contactándolos a través de populares redes sociales o medios de comunicación virtual.

Decimos esto porque el Código Penal ya contiene figuras que protegen la libertad y la indemnidad sexual de las personas menores de edad, independientemente del medio o herramienta que se haya utilizado para vulnerar dichos derechos, como la pornografía infantil, la prostitución infantil, el turismo sexual infantil y la venta o trata de personas, niños, niñas o adolescentes. Sin embargo, el Grooming si bien muchas veces se encuentra asociada a esas otras figuras delictivas, no encajaba en ninguna de ellas, puesto que en su forma básica no las configura, siendo algo totalmente distinto de que el niño, niña o adolescente, inducido por la curiosidad sexual exacerbada con morbosidad, se exhiba a través de una webcam o mediante fotografías mostrando su desnudez o zonas íntimas de forma totalmente voluntaria, lo cual en el sujeto activo ni siquiera consiste en exhibiciones obscenas, en la medida en que él no se haya exhibido por el mismo medio.

En la tabla siguiente, podemos apreciar la esquematización del delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

Tabla 6

N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Indemnidad o la Libertad Sexual
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	Niño, niña o adolescente
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Contactar por Internet u otro medio análogo a un menor de 14 años B) 1. Solicitarle material pornográfico. 2. Obtener de él material pornográfico. 3. Llevar a cabo actividades sexuales con él.
		A) Contactar por Internet u otro medio análogo a un menor de 14 a 18 años B) 1. Solicitarle material pornográfico. 2. Obtener de él material pornográfico. 3. Llevar a cabo actividades sexuales con él. C) Utilizando el engaño
05	PENA PRINCIPAL	No menor de 4 ni mayor de 8 años
		No menor de 3 ni mayor de 6 años
06	PENA ACCESORIA	Inhabilitación
		Inhabilitación

3.2.2.7.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, es la indemnidad sexual, cuando la víctima es un menor de 14 años, y la libertad sexual cuando el agraviado tiene entre 14 y menos de 18 años de edad.

En cuanto a la indemnidad o intangibilidad sexual que se protege en el primer párrafo, se encuentra establecido en la doctrina y la jurisprudencia que en las agresiones de connotación sexual en agravio de menores de 14 años, no puede afectarse una libertad que no poseen, sino la salud y condiciones físicas, psicológicas necesarias para lograr un normal desarrollo de la personalidad en el ámbito sexual por cuanto aún no han alcanzado la madurez para decidir de manera libre el ejercicio de su sexualidad.

En el delito de Grooming, se atenta la indemnidad sexual del menor de 14 años de edad, afectando el libre desarrollo de su personalidad por intervenciones que se consideran traumáticas; en tal sentido, la indemnidad sexual puede ser entendida como una manifestación de la dignidad de la persona humana, "una esfera que se puede ver gravemente comprometida, como consecuencia de relaciones —o agresiones— sexuales prematuras". (Peña-Cabrera, 2007, p. 182)

Respecto a la libertad sexual que se protege en el segundo párrafo, hay que considerar que la jurisprudencia constitucional en el ámbito penal (Sentencia del Tribunal Constitucional N° 00008-2012-PI/TC, del 24 de Enero de 2013) le concedió el derecho a la libertad sexual al menor de 14 a 18 años, generando posteriormente el cambio legislativo mediante Ley N° 30076, reconociéndose así el derecho al libre desarrollo de la personalidad del menor; la cual comprende como una manifestación positiva, la libre disposición del propio cuerpo, sin más limitaciones que el respeto a la libertad ajena, y como una manifestación negativa, la facultad de repeler agresiones sexuales de terceros, en consecuencia el no ejecutar o tolerar actos sexuales en los que no quiere participar.

Así, conforme a la redacción del tipo penal, esta libertad se ve vulnerada cuando el agente logra del menor el consentimiento a sus propósitos mediante el empleo del engaño

3.2.2.7.3 Sujetos Activo y Pasivo.

El sujeto activo es cualquier persona adulta con la condición especial de contactarlos a través de los medios informáticos y de telecomunicaciones. Es decir, el sujeto activo es aquel que toma contacto con un niño, niña o adolescente, a través de internet u otro medio semejante que le brinden las TICs, con el objeto de entablar una relación o crear una conexión emocional con él, ganarse su confianza, disminuir sus inhibiciones y finalmente determinarlo para involucrarse en situaciones de carácter sexual, que son las etapas constitutivas del delito de Grooming.

El sujeto pasivo en este delito, es un menor de edad con menos de 14 años, cuyo rango mínimo de edad no se encuentra determinado, pero debe tener la edad suficiente para poder utilizar independientemente la computadora y acceder a redes sociales en Internet, por lo cual suelen ser mayores de 8 años y con mayor incidencia cuando entran a la pubertad.

También la víctima puede ser un adolescente que tiene de 14 a menos de 18 años de edad, siempre que se configure el engaño como elemento objetivo adicional para la comisión del delito. Debemos tener en cuenta que en el *iter criminis de este delito*, el agente, aprovechando el anonimato propio de las comunicaciones que se efectúan con propósitos ilícitos, casi siempre, utiliza el engaño para lograr ganarse la confianza del menor, haciéndose pasar por otro menor que sea conocido o no de este, o de pronto circunstancialmente hacerse pasar por el enamorado de la menor de entre 14 y 18 años de edad, generando que el consentimiento otorgado, resulte viciado por el engaño empleado por el agente.

3.2.2.7.4 Figuras Agravadas.

El Art. 5° presenta dos circunstancias o supuestos de conducta ilícita distintos, diferenciados en función a la edad de la víctima, por lo cual no podemos considerar que una es agravante de la otra, en consecuencia, dicho artículo no contempla figuras agravadas; por lo que al igual que en los delitos anteriores, se debe considerar como

figuras agravadas, a las previstas en el Art. 11° de la Ley N° 30096, que eleva la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, o sea 10 años y 8 meses en este caso, cuando concurre alguna de las circunstancias detalladas a continuación:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El agente comete el delito con el fin de obtener un beneficio económico.

- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.8 DELITO DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS

Bajo este título en la Ley 30096 se contemplaba a los artículos 6° y 7°, como es de conocimiento público, en el mes de Octubre de 2013, pese a la difusión mediática contra la misma, en especial contra su artículo 6° que se consideraba limitativo a la libertad de prensa, el Presidente de la República promulgó la Ley de Delitos Informáticos; sin embargo, la oposición contra dicha norma se mantuvo y cuando se modificó la Ley en Marzo de 2014, merced a la Ley N° 30171, se derogó el artículo 6°, quedando bajo este título únicamente el artículo 7°, que tipifica el delito de Interceptación de Datos Informáticos de la manera siguiente:

> "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
>
> La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
>
> La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

> Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.". (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.8.1 Concepto y Esquematización.

Este injusto penal (interceptar datos informáticos) es un delito de peligro abstracto, en consecuencia, solo basta con demostrar la interceptación de datos informáticos para que el delito se produzca.

Al respecto, es pertinente señalar que, los delitos de peligro concreto son aquellos en los que la ley expresamente necesita que el resultado de la acción sea de peligro. El tipo requiere como resultado la proximidad de una concreta lesión. El peligro concreto es el resultado típico. Serán relevantes las circunstancias conocidas o cognoscibles por el autor del hecho en el momento de su comisión, y si era previsible la causación de un resultado lesivo para el bien jurídico de acuerdo con el saber nomológico. Por su parte, los delitos de peligro abstracto son aquellos en los cuales no se requiere expresamente la efectiva situación de peligro, sino que el fundamento de su castigo es que normalmente suponen un peligro. Basta, por lo tanto, la peligrosidad de la conducta. Se castiga una acción típicamente peligrosa. La peligrosidad de la conducta que se exige es ex ante; si ex post se produce el peligro concreto o no, es irrelevante. Esta clase de delitos plantea problemas de compatibilidad constitucional.

Por lo señalado, este delito se clasifica como uno de mera actividad, porque con el solo hecho de interceptar datos informáticos es suficiente para que se consuma el delito.

Como señala Villavicencio, por ejemplo, se encuentra la interceptación de archivos que contengan información relacionada con una investigación reservada por ley, interceptación de comunicaciones que contenga información sensible que puede ser utilizado por algún país en un contexto bélico. (Villavicencio, 2014, p. 17).

El verbo utilizado en este tipo penal es "interceptar" (Interrumpir, obstruir una vía de comunicación), que es un verbo determinador, que implica la detención de la información contenida en el sistema o en sus emisiones electromagnéticas. De esa manera se puede generar una interceptación a través y en contra de medios telemáticos como internet.

En la tabla siguiente, podemos apreciar la esquematización del delito de Interceptación de Datos Informáticos.

Tabla 7		
N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Intimidad y el Secreto de las Comunicaciones
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	Titular y/o Administrador del Dato Informático
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) intercepta datos informáticos (Incluidas las emisiones electromagnéticas que los transportan) en transmisiones no públicas C) 1. Dirigidas a un sistema informático. 2. Originadas en un sistema informático 3. Efectuadas dentro de un sistema informático.
05	PENA PRINCIPAL	No menor de 3 ni mayor de 6 años

3.2.2.8.2 Bien Jurídico Protegido.

Considerando la ubicación sistemática que ha realizado el legislador en la Ley de Delitos Informáticos, el Bien Jurídico principal que se protege con este delito, es la "intimidad"; sin embargo, no es el único bien protegido de manera principal, ya que también debemos considerar al "Secreto de las Comunicaciones".

El Tribunal Constitucional, en la Sentencia del expediente N° 00009-2014-PI/TC del 04 de marzo de 2016, ha precisado que la intimidad es una manifestación del derecho genérico a la vida privada. En un origen la intimidad involucraba sólo un sentido negativo, en tanto excluye o impide que terceros puedan acceder a determinados contenidos que la propia persona desea resguardar; empero, la evolución social influenciada por el uso de las tecnologías de la información, ha dado lugar a que la protección del derecho a la intimidad también adquiera un ámbito positivo, en la cual "el Estado adopte las medidas que sean indispensables para su adecuada tutela, lo cual abarca la posibilidad del titular de la información de poder resguardarla frente al accionar de terceros…".

El derecho al secreto de las comunicaciones, consagra implícitamente la libertad de comunicaciones, y de forma explícita, su reserva e impenetrabilidad. Este derecho se puede vulnerar tanto por la interceptación en sentido estricto (que supone aprehensión física del soporte del mensaje –con conocimiento o no del mismo- o captación, de otra forma, del proceso de comunicación), como por el simple conocimiento antijurídico de lo comunicado. El secreto de las comunicaciones abarca la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado. (Naranjo, 2013, p. 490).

El Tribunal Constitucional en la STC N° 01058-2004-AA/TC, ha precisado que toda persona tiene derecho a que sus comunicaciones y documentos privados sean adecuadamente protegidos, así como a que las mismas y los instrumentos que las contienen, no puedan ser abiertas, incautadas, interceptadas o intervenidas sino mediante mandamiento motivado del juez y con las garantías previstas en la ley. Agrega que, tanto el correo electrónico como el comando o programa de mensajería instantánea que proporciona el empleador a sus trabajadores, son formas de comunicación que, al igual que la correspondencia, se encuentran protegidas por el derecho al secreto y a la inviolabilidad de las comunicaciones.

La información como apreciamos, en este caso, se convierte en un bien jurídico protegido de carácter secundario.

3.2.2.8.3 Sujetos Activo y Pasivo.

La norma señala que es “el que”, es decir, que puede ser cualquier persona, no requiere cualificación especial para incurrir en esta conducta punible, sin embargo la experiencia de la realidad, nos enseña de que para incurrir en este delito o ser el sujeto activo se necesita que la persona que realice la descripción típica tenga unos conocimientos especiales para lograr este fin, por cuanto implica penetrar a un sistema de información con el propósito de captar datos o emisiones electromagnéticas, lo que no podría realizar un individuo sin estos conocimientos,

El sujeto pasivo de este delito, es indeterminado, ya que puede afectar tanto a los particulares como a las entidades públicas y privada; sin embargo, debido al tráfico económico en el que desarrollan sus actividades, las personas jurídicas son los sectores más afectados por este delito, como son los bancos, las instituciones públicas, industria de transformación, etc.

3.2.2.8.4 Figuras Agravadas.

Como ya lo hemos señalado el delito de Interceptación de Datos Informáticos sanciona la conducta que deliberada e ilegítimamente intercepta (interrumpe, obstruye una vía de comunicación), datos informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas. El Art. 7° a diferencia de los anteriores, sí menciona expresamente tres agravantes:

- El primer agravante se aplica cuando la interceptación recaiga sobre información clasificada como secreta, reservada o confidencial, de conformidad con la Ley 27806 – Ley de Transparencia y Acceso a la Información Pública, cuya penalidad oscila entre cinco a ocho años.

- El segundo agravante se aplica cuando la interceptación recaiga sobre información que compromete a la defensa, seguridad o soberanía nacional, cuya penalidad oscila entre ocho a diez años.

- La tercera agravante consiste en la calidad del agente (integrante de una organización criminal), que comete el delito cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores. Es decir, si concurre con la interceptación de datos informáticos que sean información clasificada, la pena podrá elevarse hasta un máximo de 10 años y 8 meses. Por su parte, si concurre con información que pueda afectar la defensa, seguridad o soberanía nacional, la pena podrá ser hasta un máximo de 13 años y 4 meses.

No obstante, los agravantes señalados expresamente en el Art. 7° de la Ley de Delitos Informáticos, se aplican también los agravantes establecidos en el Art. 11°, aunque

algunos sean repetitivos. Al respecto hay que señalar que en los dos casos que se repiten, debe aplicarse lo establecido de manera específica en el Art. 7°, cuyas penalidades son más graves, subsistiendo los agravantes generales del Art. 11° no repetidos, que elevan la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, es decir 8 años en este caso, cuando concurre alguna de las circunstancias siguientes:

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

- El delito compromete fines asistenciales.

3.2.2.9 DELITO DE FRAUDE INFORMÁTICO

El Art. 8° de la Ley de Delitos Informáticos, lo tipifica de la manera siguiente:

> "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 N° 30096 modificada por la Ley N° 30171)

3.2.2.9.1 Concepto y Esquematización.

Antes de ver conceptos respecto al fraude informático, es necesario definir la palabra Fraude. El fraude es una forma de conseguir beneficios utilizando la creatividad, con la inteligencia y viveza del ser humano. (Ossorio, 1974, p. 426). Es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización, como el Estado o una empresa. (http://definicion.de/fraude). El acto conocido como fraude es aquel en el cual una

persona, una institución o una entidad proceden de manera ilegal o incorrecta según los parámetros establecidos con el objetivo de obtener algún beneficio económico o político. Hay distintos tipos de fraude que son clasificados de acuerdo al ámbito o al procedimiento que toman, pero en general todos los fraudes se caracterizan por incurrir en mentiras, uso inapropiado de fondos, alteración de datos, traición, corrupción, etc. Los fraudes pueden ser llevados a cabo por individuos como también por grupos o entidades. (https://www.definicionabc.com/general/fraude.php). El fraude es un concepto de connotación negativa, ya que implica actitudes engañosas, ardides, dolo, o sea intención maliciosa. Cuando se le dice a una persona que es un fraude, es decirle que toda ella es una mentira, pues se desenvuelve en su vida con ocultamiento de sus verdaderas intenciones. La intención del que comete fraude es lograr un beneficio a través del engaño. (http://deconceptos.com/ciencias-juridicas/fraude).

Como podemos apreciar, entonces, el fraude implica el obtener un beneficio, a través del engaño, en perjuicio de tercero; sin embargo, se ha criticado la inadecuada tipificación del delito de Fraude Informático, puesto que no considera de manera expresa el engaño, más si el provecho ilícito en beneficio propio o de otro, en perjuicio de tercero, indicando en su tipificación una serie de verbos rectores para lograrlo:

- Diseñar (proyecto o plan) datos informáticos.
- Introducir (entrar en un lugar) datos informáticos.
- Alterar (estropear, dañar, descomponer) datos informáticos.
- Borrar (desvanecer, quitar, desaparecer algo) datos informáticos.
- Suprimir (hacer cesar, eliminar) datos informáticos
- Clonar (producir clones, copiar, reproducir) datos informáticos.
- Cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

En suma, podemos decir que es una forma de conseguir beneficios de forma no adecuada, pudiendo configurarse en diferentes formas: i) Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es

común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas; ii) Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar; iii). Alterar o borrar archivos; y, iv) Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento informático y puede traer consecuencias muy graves, tanto para las personas que lo realizan, como para las que son víctimas.

Este delito que antes de la vigencia de la Ley N° 30096, se tipificaba como Hurto Agravado, Apropiación Ilícita o Estafa, ha buscado precisar en un solo tipo delictivo, un ilícito accionar que suele estar relacionado con los hackers o crackers o utilizando otras técnicas como el phreaker, el ciberpunking, el phishing o el pharming ya mencionadas anteriormente.

Se ha buscado englobar en un sólo tipo penal, todo accionar delictivo por medios informáticos o telemáticos, que afecte de manera principal al patrimonio, es por ese motivo que, dentro del Delito de Fraude Informático, se observa que se sanciona diversas conductas, las mismas que tienen en común el considerarlo como un delito de resultado, ya que no basta cumplir con el tipo penal para que se consume la acción ilícita. En este sentido, nos parece pertinente lo que señala Felipe Villavicencio, al decir que "se clasifica como un delito de resultado porque no basta cumplir con el tipo penal para que se consume el delito de fraude informático, sino que, además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa". (2014, p. 19).

Hay que destacar que, dentro de los diferentes delitos informáticos, es el que con mayor frecuencia se produce, dado el beneficio económico o patrimonial que genera para los ciberdelincuentes. Organizaciones delictivas nacionales e internacionales se dedican a la obtención de claves de cuentas bancarias, utilizando diversas técnicas de phishing, las cuales muchas veces van asociadas con el pharming, que les permite el redireccionamiento a páginas web falsas de entidades bancarias, las cuales clonan para hacer creer a la víctima que es una web auténtica e introduzca en la misma su usuario y

clave, lo cual les es suficiente para poder utilizar el dinero o línea de crédito de que dispongan. Existe información del Ministerio del Interior (Policía Informática o DIVINDAT), que más del 40% de los delitos informáticos, consisten en Fraude Informático.

En la tabla siguiente, podemos apreciar la sistematización del delito de Fraude Informático, de acuerdo al esquema siguiente:

Tabla 8

N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	El Patrimonio
02	SUJETO ACTIVO	Cualquier persona con conocimientos de informática
03	SUJETO PASIVO	Cualquier persona natural o jurídica, que ve afectado su patrimonio.
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) Procurar para sí o para otro un provecho ilícito C) En perjuicio de tercero mediante el: D) 1. Diseño de Datos Informáticos. 2. Introducción de Datos Informáticos. 3. Alteración de Datos Informáticos. 4. Borrado de Datos Informáticos. 5. Supresión de Datos Informáticos. 6. Clonación de Datos Informáticos. 7. Cualquier interferencia o manipulación en el funcionamiento de un sistema informático
05	PENA PRINCIPAL	No menor de 3 ni mayor de 8 años
06	PENA ACCESORIA	De 60 a 120 días multa

3.2.2.9.2 Bien Jurídico Protegido.

En este delito, como hemos mencionado, el bien jurídico principal que se protege es el patrimonio, considerándose como bien jurídico secundario a la información.

Entendemos el patrimonio como el conjunto de derechos y obligaciones, referido a bienes de cualquier índole, dotado de un valor económico y que han de ser valorables en dinero. (Queralt, 1996, p. 308). Asimismo, hay que señalar que el patrimonio como bien jurídico

protegido tiene un contenido económico, consistente en que el bien debe tener un valor económico, pero también otro contenido jurídico, referido a la relación de la persona con el bien, sobre el cual tener una protección jurídica (ser propietario o poseedor). (AMAG, p. 51)

No obstante, lo antes señalado, por la extensión en la tipificación del delito de Fraude Informático, hay que tener presente que, al establecer la esfera de protección del bien jurídico, no podemos centrarnos únicamente en la información (delitos informáticos) o el patrimonio (fraude informático), sino a un conjunto de bienes que son afectados, ya que estaríamos ante un delito pluriofensivo. (Gutiérrez, 1991)

3.2.2.9.3 Sujetos Activo y Pasivo.

El sujeto activo es cualquier persona con el conocimiento informático necesario para realizar alguna de las acciones que caracterizan o se encuentran tipificadas en el Delito de Fraude Informático.

Por su parte, el sujeto pasivo es la persona titular del patrimonio, que puede ser una persona natural como también jurídica, siendo las más afectadas con este delito instituciones bancarias o crediticias que; sin embargo, muchas veces no lo denuncian para evitar el desprestigio de su institución y generar desconfianza entre sus clientes.

3.2.2.9.4 Figuras Agravadas.

El Art. 8° sí considera un agravante, el cual coincide en parte con uno de los señalados en el Art. 11°; por lo que, siguiendo el criterio señalado en el delito anterior, se aplica en primer lugar el agravante específico del propio Art. 8°, y luego los demás que considere de manera general el Art. 11°. En tal sentido, la pena privativa de libertad se elevará de 05 a 10 años y de 80 a 140 días-multa, cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social; elevándose la pena hasta en un tercio por encima del máximo legal fijado, es decir hasta 10 años y 08 meses, en las circunstancias siguientes:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El delito compromete la defensa, la seguridad y la soberanía nacionales.

3.2.2.10 DELITO DE SUPLANTACIÓN DE IDENTIDAD

El Art. 9° de la Ley de Delitos Informáticos, tipifica el delito de Suplantación de Identidad de la manera siguiente:

> "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años". (Ley N° 30096).

3.2.2.10.1 Concepto y Esquematización.

La suplantación es la simple creación de un perfil en internet o red social y no será castigada penalmente pues, tanto la ley como los tribunales, no consideran que se trate de un delito, pero ello no implica que el perjudicado no pueda exigir la eliminación del perfil al proveedor de servicios.

Es conveniente precisar que, al referirnos al delito de suplantación de identidad, se entiende a aquella acción por la que una persona se hace pasar por otra, para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas. Lo particular en este caso, es que la acción se realiza a través de las Tecnologías de la Información y la Comunicación.

La Ley N° 30171 modificó todos los artículos de la Ley N° 30096 "Ley de Delitos Informáticos" que utilizaban el término "Tecnologías de la Información y de la Comunicación", ya que fue una de las principales críticas que realizaron los especialistas a dicha Ley, por considerarse sumamente impreciso dicho término; sin embargo, curiosamente, no lo hizo con el de Suplantación de Identidad, al respecto, siendo un tanto

detallista, DÍAZ REVORIO, señala que "se considera como tecnologías de la información y la comunicación o nuevas tecnologías, entre otros instrumentos de transmisión y recepción de comunicaciones e informaciones, la telefonía fija, el móvil, la radio y la televisión, el GPS, la informática y los ordenadores, el fax, la videoconferencia, los SMS y otros servicio de mensajería, el correo electrónico, el chat o mensajería instantánea, y ocupando un indiscutible protagonismo, Internet, que incluye hoy buena parte de las prestaciones anteriores". (Palomino, 2014, p. 38)

Esta acción es cada vez más usual en las redes sociales, en las que una persona utilizando fotografías y datos de otra, crea perfiles en su nombre, desde los cuales realiza actividades diversas, como insultos a terceras personas o incluso llegan a apropiarse de datos personales debido a la poca seguridad de la que gozan algunas APP móviles o cuentas de correo.

Según el tipo de suplantación que se realice conlleva una u otra sanción, así, cuando la suplantación de identidad consiste únicamente en la apertura o registro de un perfil sin que en él se den datos personales, la opción que tiene el suplantado es hablar con el portal web, foro o red social para que sean sus administradores quienes eliminen el perfil falso, es decir, el hecho de utilizar sólo el nombre, no configura el delito.

Por el contrario, si se crea un perfil falso y se utiliza información personal de la persona suplantada, como puede ser una fotografía, se está cometiendo un delito de vulneración del derecho a la propia imagen, y en la medida que la víctima considere esa acción lesiva moral o materialmente, la conducta ilícita correspondería con la tipificación del delito. Lo que es indispensable es que se presenten todos los elementos objetivos para la configuración del delito, ya que si no se ha producido el perjuicio, el delito aún no se habrá producido y podrá catalogarse como una infracción administrativa.

Esta figura penal en tal sentido, se clasifica como un delito de resultado, porque no basta con realizar la conducta típica el cual es suplantar la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio, como por ejemplo: crear perfiles falsos en las redes sociales

(correo electrónico, Facebook, Twitter, Instagram, WhatsApp, etc) atribuidos a personas naturales o jurídicas para engañar y perjudicar a terceros. (Villavicencio, 2014, p. 19)

Hay que tener presente que, el delito de suplantación de identidad suele estar asociado con otros delitos, ya que el agente se hace pasar por otra persona por distintos motivos, como cometer un fraude, realizar ciberbullying o grooming, utilizar identidades supuestas para investigar a terceros, adquirir créditos por medios virtuales o realizar transacciones de comercio electrónico, entre otros.

En la tabla siguiente, apreciamos el esquema del delito de Suplantación de Identidad.

Tabla 9

N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Fe Pública
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	La persona natural o jurídica que resulta perjudicada con la suplantación.
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Mediante las Tecnologías de la Información o la Comunicación. B) Suplanta la identidad de una persona natural o jurídica C) Originando un perjuicio material o moral.
05	PENA PRINCIPAL	No menor de 3 ni mayor de 5 años

Se podría pensar que no se ha presentado casuística sobre este delito, pero no es así, un caso que se difundió en nuestro país a través del programa "Cuarto Poder", fue el siguiente: "Una abogada había sido suplantada en el Facebook y correo electrónico, por la pareja de su amiga, fingiendo ser lesbiana, para captar personas y ganarse la confianza a través del falso perfil y poder obtener materiales (fotos íntimas) que luego eran utilizados para extorsionar a sus víctimas que ingenuamente creyeron estar en contacto con la persona suplantada, este acto trajo perjuicios económicos, laborales, familiares y psicológicos a la suplantada". (Reportaje del 02 de octubre de 2013).

3.2.2.10.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con este delito, por el título dentro del cual ha sido incluido, es la "Fe Pública", que es uno de los bienes

jurídicos más controvertidos dentro de la doctrina especializada, toda vez que hay autores como Von Liszt, Gabba, Lombardi y Binding (citados por FIGARI) que señalan que no existe en realidad este bien jurídico, mientras otros tienen diferentes criterios. En este sentido podría señalarse aquí el criterio dualista de Carrara, para quien lo directamente atacado, vulnerado o desconocido por este tipo de delitos es la fe constituida en cada uno de los miembros de la comunidad, por el valor de veracidad que el Estado (el derecho) otorga a determinadas formas instrumentales de su propia actividad; sin embargo, en este caso, no es la veracidad del Estado lo que se está atentando, sino la veracidad de las personas por los medios tecnológicos, lo cual es más cercano a una fe privada que pública. Al respecto Carrara plantea su argumento respecto a la "Fe Pública", remontándose al origen de la sociedad civil que viene a amparar el derecho con la consabida libertad individual de todos los asociados y el ejercicio pasional libre de las actividades humanas, por ello, asevera, que ella constituye una autoridad que está por sobre todos y que mediante el poder civil mantiene la observancia de los vínculos surgidos de las obligaciones y mediante la función penal sostiene el respeto a los derechos de todos. Consiguientemente, esa autoridad procura ser más libre y rápido el desarrollo de las actividades humanas en los contratos, crea mercancías, les asigna precios y determina un elemento de intercambio por ellas que vendría a ser la moneda. "Todos los asociados, al ver el objeto al que la autoridad atribuye un precio determinado, creen sin vacilaciones en ese precio, lo que aceptan como tal, y en cambio de dicha moneda entregan cosas propias, que juzgan de ese mismo precio". Pero la autoridad pública va más allá de ello al crear signos materiales y delegar en ciertos ciudadanos la potestad de asegurar, por medio de tales signos, las condiciones de un objeto venal o la existencia de ciertos hechos y de ciertos contratos (Figari, p. 3). En este caso, entendemos que el legislador ha buscado equiparar la designación del Estado a determinadas personas que sean encargados de otorgar la fe pública, con el interés del Estado de garantizar la veracidad de la identidad de las personas en las comunicaciones a través del Internet o las Tecnologías de la Información y la Comunicación en general.

3.2.2.10.3 Sujetos Activo y Pasivo.

El sujeto activo puede ser cualquier persona que realiza la suplantación de identidad y la utiliza para generar algún perjuicio en tercero.

Por su parte, el sujeto pasivo es la persona a la que se ha afectado su buen nombre por ser suplantada, generando pérdida económica, pérdida de información confidencial, pérdida de credibilidad, etc., en ella misma o terceras personas, pudiendo ser la víctima una persona natural o una persona jurídica como sociedades, instituciones crediticias, entidades públicas u otras.

3.2.2.10.4 Figuras Agravadas.

El Art. 9° no las menciona, por lo que debe tenerse en consideración las que se encuentran establecidas en el Art. 11° de la misma Ley y que elevan la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, es decir 6 años y 8 meses en este caso, cuando concurre alguna de las circunstancias que detallamos a continuación:

- El agente comete el delito en calidad de integrante de una organización criminal.
- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
- El agente comete el delito con el fin de obtener un beneficio económico.
- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.11 DELITO DE ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

El Art. 10° de la Ley de Delitos Informáticos modificado, lo tipifica de la manera siguiente:

> "El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena

privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.”. (Ley N° 30096 modificada por la Ley N° 30171)

3.2.2.11.1 Concepto y Esquematización.

El delito de Abuso de Mecanismos y Dispositivos Informáticos, es una suerte de sanción a los actos preparatorios de un Delito Informático, alegando la puesta en peligro de la seguridad informática. La tipificación que ha escogido el legislador para este delito lo clasifica como un delito de mera actividad, porque la figura exige cumplir con la conducta descrita en el tipo penal para la consumación del delito, sin importarle el resultado, ya que adelanta las barreras de punibilidad al sancionar el solo hecho, cuya acción la ha detallado en numerosos verbos:

A. Fabricar.- Crear mediante componentes tecnológicos un mecanismo o programa informático, es decir, producir objetos en serie, generalmente por medios mecánicos.

B. Diseñar.- Hacer un diseño, es decir, acto de creación, innovación o planificación de un sistema o mecanismo de información.

C. Desarrollar.- Hacer una serie ideas o proyectos.

D. Vender.- Dar un objeto o cosa a alguien a cambio de un pago. Traspasar a alguien por el precio convenido la propiedad de lo que uno posee.

E. Facilitar.- Proporcionar o entregar una cosa a alguien o hacer de intermediario para que lo consiga, haciendo fácil o posible algo.

F. Distribuir.- Repartir, disponer un mecanismo de información siguiendo un criterio. Entregar una mercancía a los vendedores y consumidores.

G. Importar.- Introducción en el país de un producto extranjero.

H. Obtener.- Conseguir un producto u objeto a partir de otros. Alcanzar, conseguir y lograr algo que se merece, solicita o pretende.

Empero, para completar la comisión del delito, cualquiera de esas acciones tiene que estar destinada a utilizar mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, que han sido diseñados para la comisión específica de los delitos enumerados precedentemente, sancionando también al que ofrece o presta servicio que contribuya al propósito del delito informático. En la tabla siguiente, podemos apreciar la esquematización del delito de Abuso de Mecanismos y Dispositivos Informáticos.

Tabla 10		
N°	TEMA	DESCRIPCION
01	BIEN JURIDICO	La Información
02	SUJETO ACTIVO	Cualquier persona
03	SUJETO PASIVO	La persona natural o jurídica agraviada
04	ELEMENTOS OBJETIVOS DE LA CONDUCTA TIPICA	A) Acción deliberada e ilegítima. B) Fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización. C) 1. Uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos informáticos. 2. El que ofrece o presta servicio que contribuya a un delito informático.
05	PENA PRINCIPAL	No menor de 1 ni mayor de 4 años
06	PENA ACCESORIA	De 30 a 90 días multa

3.2.2.11.2 Bien Jurídico Protegido.

El Bien Jurídico que se protege de manera principal con este delito, es la "información", lo que incluye su almacenamiento, tratamiento y transmisión, la cual se encuentra contenida en bases y/o bancos de datos.

3.2.2.11.3 Sujetos Activo y Pasivo.

El sujeto activo es aquel que realiza cualquiera de las conductas reguladas en el Art. 10° de la Ley de Delitos Informáticos, con la intención de coadyuvar la comisión de otro delito informático.

Por su parte, el sujeto pasivo puede ser cualquier persona, que se vea afectada en calidad de víctima por la comisión de este delito.

3.2.2.11.4 Figuras Agravadas.

El Art. 10° no las menciona, sin embargo, debe tenerse en consideración las que se encuentran establecidas en el Art. 11° de la misma Ley y que elevan la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado, es decir 5 años y 4 meses en este caso, cuando concurre alguna de las circunstancias que detallamos a continuación:

- El agente comete el delito en calidad de integrante de una organización criminal.

- El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

- El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

- El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.2.2.12 LA POLICÍA INFORMÁTICA EN EL PERÚ.

La DIVINDAT o División de Investigación de Delitos de Alta Tecnología, es un órgano de ejecución de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú (PNP), que tiene como misión:

> "Investigar, denunciar y combatir el crimen organizado transnacional (Globalizado) y otros hechos trascendentes a nivel nacional en el campo de los Delitos Contra la Libertad, Contra el Patrimonio, Seguridad Pública, Tranquilidad Pública, Contra la Defensa y Seguridad Nacional, Contra la Propiedad Industrial y otros, cometidos mediante el uso de la tecnología de la información y comunicación, aprehendiendo los indicios, evidencias y

> pruebas, identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente". (2012)

Recordemos que la misión de una institución, hace referencia a su finalidad, al objeto para la cual fue creada, al propósito básico hacia el que apuntan sus actividades; mientras que la visión describe las metas de mediano y largo plazo, expresándose de manera concisa y atractiva, la forma como la organización quiere ser percibida o vista por el mundo.

A fin de diferenciar la Misión de la Visión, nos parece pertinente la cita siguiente:

> "La Misión es el motivo o la razón de ser por parte de una organización, una empresa o una institución. Este motivo se enfoca en el presente, es decir, es la actividad que justifica lo que el grupo o el individuo está haciendo en un momento dado. (…)
>
> La Visión (…) se refiere a una imagen que la organización plantea a largo plazo sobre cómo espera que sea su futuro, una expectativa ideal de lo que espera que ocurra". (De Conceptos, 2018)

La visión que tiene planteada la DIVINDAT es la siguiente:

> "Ser reconocida nacional e internacionalmente en la investigación de delitos cometidos mediante el uso de las tecnologías de la información y comunicación, contando con personal altamente capacitado y especializado, acorde con las necesidades que demanda los avances e innovación tecnológica". (2012)

Los Valores que propone la DIVINDAT para el desarrollo o ejecución de su trabajo, son, Iniciativa, Creatividad, Disciplina, Honestidad, Integridad, Responsabilidad y Lealtad.

La DIVINDAT plantea como estrategias para su trabajo, cuatro tipos de acciones, la preventiva, la disuasiva, la de búsqueda y la de investigación.

La acción preventiva, como su mismo nombre lo dice está dirigida a prevenir la comisión de los delitos informáticos y de alta tecnología, mediante campañas educativas y una adecuada información hacia la comunidad, para que no caiga en mano de este tipo de delincuentes; de manera particular, cabe mencionar que cumple está acción mediante información en su portal web, en la cual encontramos una serie de consejos dirigidos a padres, niños, usuarios, vendedores, compradores, o sobre temática diversa como son seguridad virtual, transacciones económicas, correos electrónicos, fraudes telefónicos y peligros en Internet.

La acción disuasiva la ejecuta principalmente mediante el patrullaje virtual o en el ciberespacio, que es un programa dedicado a la ciber navegación policial, permitiendo la actuación oportuna para combatir las actividades delictivas, como son pornografía infantil, fraude cibernético, piratería de software o hurto de fondos, así como las nuevas modalidades y tendencias criminales del mundo virtual, entre las que se pueden encontrar el terrorismo y narcotráfico internacional, utilizando como instrumento de global de comunicación para planear y organizar sus acciones criminales, al Internet.

Las acciones preventiva y disuasiva, están orientadas a evitar que se cometan los delitos, es decir, se ejecutan antes de la comisión de los mismos, mientras que las acciones de búsqueda y de investigación, se ejecutan cuando ya se han cometido los delitos, para ubicar a los responsables y lograr las evidencias que permitan denunciar el delito.

3.2.2.13 PREVENCIÓN DE LOS DELITOS INFORMÁTICOS

A lo largo de la historia del hombre, éste siempre ha necesitado comunicarse y trasmitir información sobre cualquier tema, en el que también se incluían nuestros datos personales, con el desarrollo del Internet, toda esa información se enriquece al estar disponible a millones de personas en todo el mundo, convirtiéndolo en un ambiente atractivo también para el accionar delictivo, dando surgimiento de esa manera a la ciberdelincuencia y contaminando el mundo virtual de la red de redes.

Margarita Llambías, nos precisa que "La contaminación es de la más variada, entre los últimos ataques a la red y que podemos calificar como de los más graves en el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico". Agrega que ante esa situación, políticos de diversos países pretendieron que se reglamente el uso de Internet, de modo que se lleve un registro de los usuarios; sin embargo, dicha propuesta no prosperó, debido a que hubo la enérgica protesta de que ello atentaría contra la libertad y especialmente sobre la privacidad. (2008, p. 206).

Desde otra posición, existen los que ven en el desarrollo de la informática y las TIC, la solución para todos los males que aquejan a la sociedad; empero existen enfrentados, aquellos que piensan que el cerebro electrónico sobresaldrá frente al humano y llevara a

la aniquilación del hombre. Ambas posiciones llevan a mencionar a Juan José Blossiers, que "La excesiva radicalización de ambas posturas, obvia cualquier consideración sobre su verdadera relevancia en el momento actual del debate acerca de la sociedad de la información. Porque cuando se habla de limitar la informática, no se pretende impedir su uso, sino las amenazas que de su uso pudieran derivarse". (2003, p. 101).

Como podemos percatarnos, con el crecimiento informático, se han dado una serie de preocupaciones sobre el futuro de la sociedad y de la humanidad, entre los cuales, uno de los males más evidentes, es el incremento de la delincuencia informática, lo que ha dado lugar a que se vea la necesidad de combatirla, sin afectar derechos fundamentales como el de Protección de Datos Personales; más no se ha tenido en consideración que, el mismo derecho fundamental, puede servir como un medio de prevención contra la comisión de los delitos informáticos, utilizando estrategias diversas que complementarían y permitiría llegar a más ciudadanos, con actividades diversas de carácter preventivo, como las que efectúa la DIVINDAT.

Es necesario percatarnos que las actividades preventivas deben estar dirigidas a temas culturales y de seguridad, existen casos diversos en que el acceso a datos personales ha sido motivo u origen de una conducta delictiva, como por ejemplo, el caso del periodista Pipi Estrada el 27 de noviembre de 2012, cuando se conoció la noticia de que su agenda telefónica había sido publicada en internet con algunos de los teléfonos de celebrities de España, lo cual lleva a reflexionar sobre el riesgo en que se incurre al descargar un simple archivo o conectar tu bluetooth o wifi, sin tomar ciertas medidas de seguridad, pudiendo originarse la exposición total de un teléfono móvil y todo su contenido (agenda, emails, fotos) a cualquier tercero. El acceso y uso de la agenda electrónica de una tercera persona, supone una vulneración al derecho a la intimidad, además de constituir una infracción administrativa en la mayoría de las legislaciones sobre protección de datos personales; además, también pueden incurrir en conductas ilícitas, las personas que reenviaron a través del WhastApp la información personal obtenida de la referida agenda. (Letslaw, 2017).

En el tema de la prevención de los delitos informáticos, múltiples páginas web recomiendan como un medio el no proporcionar los datos personales. El Centro de

Integración Ciudadana, entre las 11 recomendaciones que brinda para protegerse de los delitos informáticos, en la sexta y sétima señala que "NUNCA PROPORCIONES NÚMEROS O DATOS DE IDENTIFICACIÓN. Tu nombre, tu dirección y medios de contacto son información necesaria para realizar cualquier compra en Internet, sin embargo para evitar ser víctima de robo de identidad o delitos similares nunca proporciones tu Número de Seguro Social, RFC, CURP etc." y "UTILIZA SIEMPRE UNA CONEXIÓN SEGURA. Si vas a realizar una transacción o requieres compartir vía Internet los datos de tu tarjeta de crédito o débito hazlo siempre desde una red propia ya que las redes wifi públicas, ya sean libres o protegidas, puedes ser interceptadas por los ciberdelincuentes". (CID, s/f, parr. 1)

En Argentina, existe un portal web que liga a la policía informática, con la Fiscalía contra Delitos Informáticos y provee medios para denunciar en línea la comisión de tales ilícitos, pero asimismo brinda consejos sobre prevención contra los ciberdelincuentes, los cuales son clasificados por características o rangos de edades, de tal manera que para los jóvenes recomienda configurar la privacidad de su perfil en Facebook y redes sociales, así como no compartir sus datos sensibles o privados.(Protección Online.com, s/f, parr. 2 y 3)

La Policía Metropolitana de Cartagena, recomienda que "En los perfiles de tus redes sociales nunca publiques información personal, por ejemplo, tu nombre completo, domicilio, número telefónico, o el de otras personas que tú conozcas ni compartas fotos de tus familiares o amigas y amigos, o cualquier información tuya de manera pública", "Limita el acceso a tu información sólo a las personas más cercanas a ti" o "Nunca compartas información que sirva para identificarte o localizarte fuera de internet, por ejemplo, los lugares que frecuentas, los días y la hora en que lo haces, los horarios en que estás en tu casa o los momentos en que te quedas a solas", tal como nos lo refiere el Diario Universal (2015, p. 1).

Especial cuidado en las actividades de prevención, está circunscrita a los niños y adolescentes, toda vez que los menores son más ingenuos y por tanto, en términos generales, más proclives a facilitar cierto tipo de información personal que les puede poner en peligro a ellos y sus familias (Abogados Portaley, 2007), es por ello que el Gobierno de Argentina, ha editado una serie de videos dirigidos a los menores de edad,

relacionados a la protección de datos personales, como medio para prevenirse de los delincuentes informáticos. (Ver: https://www.youtube.com/watch?v=lswxUTFOTaQ)

Como podemos observar, existe la difusión, de que entre las diferentes formas de prevención de los delitos informáticos, se encuentra el no brindar la información personal que te identifica o te hace identificable, en otras palabras, hablamos de proteger tus datos personales; que es un aspecto fundamental en nuestra investigación, puesto que se presenta en forma generalizada, la idea de que proteger los datos personales previene los delitos informáticos, lo cual se está convirtiendo en una premisa aceptada por la población, pero que no cuenta con un sustento teórico o doctrinario bien estructurado, que explique la relación entre la protección de los datos personales y los delitos informáticos.

3.2.3 BASES LEGALES

Las principales normas vigentes de carácter general en el Perú sobre protección de datos personales y delitos informáticos, son las siguientes:

- Ley Nº 29733 "Ley de Protección de Datos Personales".
- Decreto Legislativo N° 1353, modifica la Ley de Protección de Datos Personales.
- Ley Nº 30096 "Ley de Delitos Informáticos".
- Ley Nº 30171, modifica la Ley de Delitos Informáticos.
- Reglamento de la Ley de Protección de Datos Personales, aprobado con Decreto Supremo Nº 003-2013-JUS.
- Decreto Supremo N° 019-2017-JUS, que modifica el Reglamento de la Ley de Protección de Datos Personales.

3.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

Vamos a presentar los conceptos ordenados alfabéticamente, dividiéndolos en dos grupos, el primero en que introducimos los conceptos fundamentales respecto a la temática de nuestra investigación y que se encuentran vinculados a nuestras variables, y el segundo en donde agregamos otros conceptos relacionados con nuestra materia de investigación.

3.3.2 CONCEPTOS PRINCIPALES

- **Banco de Datos Personales.**

  Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso. (Ley N° 29733, 2011, Art. 2, Inc. 1)

- **Dato Personal.**

  Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 4)

- **Delito Informático.**

  Aquella conducta típica, antijurídica y culpable, en que se tiene a las computadoras e Internet como instrumento o fin. (Definición propia)

- **Delincuencia Informática.**

  Son todos aquellos actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de las computadoras y a través del mundo virtual del internet. (Ugarte, 2015, Parr. 15)

- **Dirección General de Protección de Datos Personales.**

  Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones. (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 8)

- **Protección de Datos Personales.**

  Es aquel derecho fundamental de la persona que tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que

representa el uso y la eventual manipulación de los datos a través de las computadoras y el Internet. (Definición propia, derivada de la definición del Tribunal Constitucional en la STC N° 1797-2002-HD/TC).

- **Titular de los Datos Personales.**
  Persona natural a quien corresponde los datos personales. (Ley N° 29733, 2011, Art. 2, Inc. 16)

3.3.3 CONCEPTOS SECUNDARIOS

- **Antivirus.**
  Programas que se utilizan con el fin de prevenir y detectar posibles infecciones producidas por virus y todo tipo de programas maliciosos, y reparar los daños que éstas hayan podido causar. (Computer Forensic, 2015, Parr. 2)

- **Autodeterminación informativa.**
  Es un derecho fundamental que tiene por objeto defender la intimidad personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. (Tribunal Constitucional, 2003, Sentencia N° 01797-2002-HD/TC)

- **Bloqueo.**
  Es la medida por la que el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión, en concordancia con lo que dispone el tercer párrafo del artículo 20 de la Ley. (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 2)

- **Bomba Lógica.**
  Programa que se instala en un equipo y se mantiene inactivo, en espera de que se cumplan una serie de requisitos o condiciones, como por ejemplo: que el usuario pulse una tecla o una combinación de teclas concretas, que el reloj del sistema marque una hora determinada, etc. Cuando se ejecutan las condiciones de activación, el

programa comienza a llevar a cabo las acciones para las que ha sido diseñado, que pueden ser: ordenar que se realice una transferencia bancaria, dañar el sistema, borrar datos del disco duro, etc. (Computer Forensic, 2015, Parr. 4)

- **Cancelación.**

  Es la acción o medida que en la Ley se describe como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos. (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 3)

- **Computadora.**

  Una computadora, computador u ordenador (computer en inglés) es un dispositivo electrónico compuesto básicamente de procesador, memoria y dispositivos de entrada/salida, y permite procesar información. Técnicamente una computadora es una máquina programable, esto significa que puede ejecutar una lista de instrucciones y responder a nuevas instrucciones que le son dadas. De todas maneras, hoy en día, el término computadora se asocia coloquialmente a las PCs de escritorio y las notebook; son computadoras también las tabletas y teléfonos inteligentes. (Alegsa, 2017)

- **Datos Informáticos.**

  Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. (Ley N° 30096, 2013, 9ª DCF)

- **Datos sensibles.**

  Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad. (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 6)

- **Encargado del Banco de Datos Personales.**

  Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra, realiza el tratamiento de los datos personales por encargo del titular de banco de datos personales. (Ley N°29733, 2011, Art. 2, Inc. 7)

- **Firewall.**

  Firewall o cortafuegos es un mecanismo de seguridad que regula el acceso entre dos o más redes, teniendo en cuenta la política de seguridad establecida por la organización responsable de la red. Habitualmente se utilizan los cortafuegos para proteger redes internas de accesos no autorizados. (Computer Forensic, 2015, Par. 9)

- **Flujo Transfronterizo de Datos Personales.**

  Transferencia Internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentres, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciba. (Ley N° 29733, 2011, Art. 2, Inc. 10)

- **Grooming.**

  Hace referencia a una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. (Ley N° 30096, 2013, Art. 5°)

- **Gusano.**

  Los gusanos o worms son programas capaces de realizar copias de sí mismos y propagarse, a través de la red para infectar otros equipos, sin la intervención de un usuario. Una de las formas más habituales de propagación de gusanos es el envío masivo de correos electrónicos a los contactos de las libretas de direcciones de los usuarios. (Computer Forensic, 2015, Parr. 11)

- **Hacker.**

  Se denominan hackers a los especialistas en tecnologías de la información y telecomunicaciones en general, aunque actualmente, se utiliza este término para

referirse a aquellos que utilizan sus conocimientos con fines maliciosos como el acceso ilegal a redes privadas, el robo de información, etc. Según algunos expertos, es incorrecto asociar este término únicamente con aquellas prácticas fraudulentas, ya que existen dos tipos de hackers:

- "White Hat": especialistas en informática que utilizan sus conocimientos con el fin de detectar cualquier tipo de vulnerabilidad, errores o fallos de seguridad, etc. para poder solucionarlos y evitar posibles ataques.
- "Black Hat" o "Cracker": expertos en seguridad informática que tratan de detectar las debilidades o deficiencias de programas y equipos informáticos, para obtener algún tipo de beneficio. (Computer Forensic, 2015, Parr. 12)

- **Hoax.**

  Un hoax es un mensaje de correo electrónico con información engañosa, que pretende avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Los hoaxes se caracterizan por solicitar al destinatario que reenvíe el mensaje a todos sus contactos, así logran captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, spam, phishing, etc. (Computer Forensic, 2015, Parr. 14)

- **Keylogger.**

  Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios, y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes de correo, etc. La información almacenada se suele publicar o enviar por internet. (Computer Forensic, 2015, Parr. 15)

- **Malware.**

  El término Malware (Acrónimo en inglés de: "Malcious software") engloba a todos aquellos programas "maliciosos" (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático o al usuario del mismo. (Computer Forensic, 2015, Parr. 16)

- **Nivel suficiente de protección para los datos personales.**

  Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de quien se trate. (Ley N° 29733, 2011, Art. 2, Inc. 12)

- **Pharming.**

  Modalidad de estafa online que utiliza la manipulación de los servidores DNS (Domine Name Server) para redireccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales del usuario, como contraseñas, datos bancarios, etc. (Computer Forensic, 2015, Parr. 17)

- **Phishing.**

  Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios como contraseñas o claves de acceso a cuentas bancarias. Para lograr esta información, se realizan envíos masivos de correos electrónicos, que simulan proceder de entidades de confianza. En el mensaje se pide al usuario que, por "motivos de seguridad" o con el fin de "confirmar su cuenta", facilite sus datos personales, claves, etc. En ocasiones, este tipo de datos se solicitan en el mismo mensaje, o se indica al usuario que acceda a la página web de la entidad en cuestión, que es una copia idéntica de la original, donde deberá completar dicha información. Actualmente están surgiendo numerosas versiones de este delito, que se sirven de otro tipo de medios para conseguir los mismos fines. Un ejemplo del nuevo phishing es el SMiShing. (Computer Forensic, 2015, Parr. 18)

- **Procedimiento de Anonimización.**

  Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible. (Ley N° 29733, 2011, Art. 2, Inc. 14)

- **Procedimiento de Disociación.**

  Tratamiento de datos personales que impide la identificación o que no hace identificables al titular de estos. El procedimiento es reversible. (Ley N° 29733, 2011, Art. 2, Inc. 15)

- **Rectificación.**

  Es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo incluir información en él o específicamente rectificar su contenido con datos exactos. (Reglamento de la Ley N° 29733, 2013, Art. 2, Inc. 12)

- **Sistema Informático.**

  Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. (Ley N° 30096, 2013, 9na DCF, Inc. a)

- **Spyware o Programa Espía.**

  Es un tipo de programa cuyo objetivo es recopilar información del usuario del sistema en el que se instala. Los datos que se recogen suelen estar relacionados con los hábitos de navegación del usuario y se utilizan con fines publicitarios. Aunque la instalación de los programas espías puede realizarse con el consentimiento expreso del usuario, en muchos casos, se instalan sin la autorización de éste, al instalar otro programa supuestamente inofensivo, o mediante virus o un troyano, distribuidos por correo electrónico. (Computer Forensic, 2015, Parr. 23)

- **Titular del Banco de Datos Personales.**

  Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad. (Ley 29733, Art. 2.17)

- **Transferencia de Datos Personales.**

  Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional de una persona jurídica de derecho privado a una entidad pública o a una persona natural distinta del titular de datos personales. (Ley N° 29733, 2011, Art. 2, Inc. 18)

- **Tratamiento de Datos Personales.**

  Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procedimiento que facilite el acceso, recolección o interconexión de los datos personales. (Ley N° 29733, 2011, Art. 2, Inc. 19)

- **Troyano.**

  Programa ejecutable que aparenta realizar una tarea determinada, para engañar al usuario, con el fin de llevar a cabo acciones como controlar el equipo informático, robar información confidencial, borrar datos, descargar otro tipo de malware, etc. La principal diferencia entre los troyanos y los virus es que los troyanos no pueden replicarse a sí mismos. (Computer Forensic, 2015, Parr. 24)

- **Virus.**

  Código informático que se replica a sí mismo y se propaga de equipo en equipo por medio de programas o archivos a los que se adjunta. Para que se produzca la infección, es necesaria la intervención humana, es decir, el usuario debe realizar algún tipo de acción como enviar un correo o abrir un archivo. Los virus pueden producir todo tipo de daños en el propio equipo y en la información y programas que éste contiene. (Computer Forensic, 2015, Parr. 25)

CAPÍTULO IV: HIPÓTESIS Y VARIABLES

4.1 HIPÓTESIS GENERAL

La Protección de Datos Personales, sí se relaciona en forma directa con la prevención de los Delitos Informáticos en el Perú.

4.2 HIPÓTESIS ESPECÍFICAS

Se plantean dos hipótesis específicas relativas a la variable independiente, que guardan correlato con los problemas y objetivos específicos, así como con las dimensiones de la variable independiente o causal.

a) El titular de los datos personales, sí los expone relacionando directamente su uso indebido para la comisión de delitos informáticos.

b) La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú.

4.3 DEFINICIÓN CONCEPTUAL Y OPERACIONAL DE LAS VARIABLES

Hay que diferenciar la definición conceptual de la operacional, precisando que la primera se refiere a lo que se entiende usualmente en el mundo jurídico, por cada una de

las variables materia de estudio; mientras que la segunda, son definiciones apropiadas para los fines de la investigación y que se recogen con tal fin.

4.3.1 DEFINICIÓN CONCEPTUAL DE VARIABLES.

La variable independiente es la "Protección de Datos Personales", cuya definición conceptual es la siguiente: Es aquel derecho fundamental de la persona que tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de las computadoras y el Internet.

La variable dependiente son los "Delitos Informáticos", cuya definición conceptual es la siguiente: Aquella conducta típica, antijurídica y culpable, en que se tiene a las computadoras e Internet como instrumento o fin.

4.3.2 DEFINICIÓN OPERACIONAL DE VARIABLES.

La variable independiente es la "Protección de Datos Personales", cuya definición operacional es la siguiente: La Protección de Datos Personales en el Perú, es la regulación normativa que incluye los medios legales para su protección y las actividades de los titulares de los datos personales para evitar su uso indebido. La variable dependiente son los "Delitos Informáticos", cuya definición operacional es la siguiente: Los Delitos Informáticos en el Perú, son los delitos contra los datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidad y secreto de las comunicaciones, contra el patrimonio y contra la fe pública.

4.4 CUADRO DE OPERACIONALIZACIÓN DE VARIABLES

En el cuadro de operacionalización de variables, podemos identificar con claridad a cada una de las variables, con sus respectivas definiciones conceptuales y operacionales, mencionando las dimensiones que coinciden con los problemas y objetivos específicos, plasmando los indicadores que permitirán medir a través del instrumento de investigación, cada una de las variables de estudio, como apreciamos a continuación:

Tabla: 11				
VARIABLE	**DEFINICIÓN CONCEPTUAL**	**DIMENSIONES**	**DEFINICIÓN OPERACIONAL**	**INDICADORES**
INDEPENDIENTE (X): **PROTECCIÓN DE DATOS PERSONALES**	Es aquel derecho de la persona que tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de las computadoras y el Internet.	1. El titular de los datos personales.	La Protección de Datos Personales en el Perú, es la regulación normativa que incluye los medios legales para su protección y las actividades de los titulares de los datos personales para evitar su uso indebido.	• Medios de exposición de datos. • Razones de exposición de datos.
		2. La Ley de Protección de Datos Personales		• Consentimiento. • Tratamiento de Datos Personales. • Registro de Bancos de Datos. • Infracciones y sanciones.
DEPENDIENTE (Y): **DELITOS INFORMÁTICOS**	Aquella conducta típica, antijurídica y culpable, en que se tiene a las computadoras e Internet como instrumento o fin.	1. Delitos Informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171.	Los Delitos Informáticos en el Perú, son los delitos contra los datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidad y secreto de las comunicaciones, contra el patrimonio y contra la fe pública.	• Delitos contra los datos y sistemas informáticos.
				• Delitos contra la libertad e indemnidad sexual.
				• Delitos contra la Intimidad y secreto de las Comunicaciones.
				• Delitos contra el Patrimonio
				• Delitos contra la Fe Pública.

CAPÍTULO V: METODOLOGÍA DE LA INVESTIGACIÓN

5.1 TIPO Y NIVEL DE INVESTIGACIÓN

5.1.1 TIPO DE INVESTIGACIÓN

Las investigaciones pueden ser básicas o aplicadas, una investigación es de tipo básica, porque está orientada a lograr un nuevo conocimiento de manera sistemática metódica, con el objetivo de ampliar el conocimiento de una nueva realidad, mientras que la investigación es aplicada cuando está orientada a lograr un nuevo conocimiento, destinado a procurar soluciones de problemas prácticos (Alzamora De Los Godos, 2009, p. 13); en tal sentido, por la finalidad de la presente investigación, consideramos que es básica, también denominada, teórica o dogmática, porque busca ampliar el conocimiento de la Protección de Datos Personales y la relación causal que tiene con los Delitos Informáticos para colaborar en su prevención en el Perú.

Asimismo, la investigación es transversal, toda vez que se van a estudiar las variables en un tiempo determinado y único (Gavagnin, 2009, p. 117), habiéndose escogido en este caso el período de tiempo de enero del 2017 a julio del 2018.

5.1.2 NIVEL DE INVESTIGACIÓN

Hernández Sampieri nos dice que los estudios explicativos van más allá de la descripción de conceptos o fenómenos, sino que están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales (Hernández, 2014, p. 95); en tal sentido, el presente estudio es explicativo en función de que se va a buscar la causa de un fenómeno social, toda vez que a partir del uso indebido de los datos personales, se busca explicar en qué medida el conocimiento y la aplicación integral de la ley de protección de datos personales, nos permitirá percibir la influencia que tiene en el control y reducción de la autoría y comisión de los delitos informáticos; en otras palabras, se busca establecer una relación causal entre la variable independiente, que es la protección de datos personales, con la variable dependiente, que son los delitos informáticos, en el Perú.

5.2 MÉTODOS Y DISEÑO DE LA INVESTIGACIÓN

5.2.1 MÉTODOS DE INVESTIGACIÓN

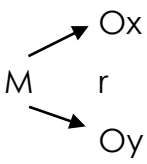
En el método deductivo se aplican los principios descubiertos a casos particulares, en el método inductivo se crea leyes a partir de la observación de los hechos, Behar también nos habla del método hipotético deductivo. (Behar, 2008, p. 39-40); en tal sentido, la inducción consiste en ir de los casos particulares a la generalización y la deducción, en ir de lo general a lo particular. La combinación de ambos métodos significa la aplicación de la deducción en la elaboración de hipótesis, y la aplicación de la inducción en los hallazgos; en consecuencia, vamos a aplicar como método de la investigación el deductivo - inductivo, considerando que la hipótesis se ha formulado en base a casos particulares observados en la realidad, que se han generalizado en la misma, mientras que, del estudio de casos específicos se buscará llegar a reglas generales, considerando que el área de la presente investigación se enmarca dentro del derecho constitucional (derechos fundamentales – derecho a la protección de datos personales) y derecho penal (delitos – delitos informáticos), mixturados dentro de un área del derecho menos conocida que es el derecho informático, hoy también llamado derecho informático y de las nuevas tecnologías.

Asimismo dentro de la clasificación que efectúa el Dr. Carlos Ramos Núñez de los métodos de investigación jurídica, podemos afirmar que se utilizará el método dogmático, respecto al cual nos dice que: "Una investigación jurídica - dogmática concibe el problema jurídico desde una perspectiva estrictamente formalista, descontando todo elemento fáctico o real que se relacione con la institución o especie legislativa". Nos agrega, que una tesis inspirada en el método dogmático, visualizará el problema jurídico a la luz de las fuentes formales, que incluye el estudio de las normas legales, la doctrina, el derecho comparado y ocasionalmente la jurisprudencia. (2007, p. 112).

5.2.2 DISEÑO DE LA INVESTIGACIÓN

El diseño es el plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema. El diseño de investigación es de dos tipos, experimental y no experimental, el cual puede ser a su vez longitudinal o transversal, siendo los tipos del transversal, los exploratorios, descriptivos, correlacionales y causales (Hernández, 2014, p. 127-128). De conformidad con lo señalado por el prestigioso investigador mexicano, el diseño de la presente investigación es no experimental – transversal - causal. Esta investigación es de tipo relacional causal, debido a que se va a relacionar la variable independiente con la dependiente, es decir se va a relacionar la protección de datos personales como causa de influencia en la prevención de la variable dependiente que son los delitos informáticos, cuyos efectos se podrán medir a partir del análisis cuantitativo a realizar de la relación causal entre cada uno de sus indicadores previstos en la investigación. Como ya señalamos es transversal debido a que se estudian las variables en un tiempo determinado y único (Gavagnin, 2009, p. 117). Es no experimental debido a que no se genera ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación por quién la realiza (Hernández, 2014, p. 152).

Esquema.



Donde.

M = Muestra.

Ox = Observación a la Variable Independiente.

Oy = Observación a la Variable Dependiente.

r = Relación entre las Variables

5.3 POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

5.3.1 POBLACIÓN

En el Perú, la única especialización que existe en Derecho Informático es la que brindan durante dos ciclos de estudio los Colegios de Abogados o de Notarios, que brindan el curso de preparación para ser Fedatario Juramentado con Especialización en Informática. Al no existir en nuestro país, información estadística sobre el aumento o disminución de los delitos informáticos, a partir de la fecha en que se empieza a aplicar en su integridad los mecanismos de control de protección de datos personales; hemos considerado pertinente, como la mejor forma de obtener información de calidad sobre la temática de investigación, el elegir como población de estudio, a expertos en la materia, constituida al inicio del estudio, por 135 abogados fedatarios juramentados con especialización en informática (FJEI), debidamente registrados en el Ministerio de Justicia, los cuales, por su formación especializada, son expertos en derecho informático, como ya he señalado, que es el área específica materia de estudio en la presente investigación.

5.3.2 MUESTRA

Considerando que la población es finita, se ha utilizado el muestreo aleatorio simple, cuya fórmula a utilizar fue:

$$n_0 = \frac{NZ^2pq}{i^2(N-1)+Z^2pq}$$

Reemplazando los valores:

N= 135

Z = 1.96 (confiabilidad del 95%)

i = 0.05 (error muestral)

pq= 0.5 (proporción, para obtener la máxima muestra)

$$n_0 = \frac{135*1.96^2*0.5*0.5}{0.05^2(135-1)+1.96^2*0.5*0.5}$$=100.08=100 abogados FJEI

Como $\frac{n_0}{N}$ = 0.74 y es mayor que 0.05, se procedió a corregir la muestra:

$$n = \frac{n_0}{1+\frac{n_0}{N}} = \frac{100}{1+\frac{100}{135}}$$ = 57.4 ≈ 57 abogados FJEI

Como resultado de las formulas aplicadas para la obtención de la muestra aleatoria simple para poblaciones finitas, encontramos que la muestra a la cual se le aplicará el instrumento de investigación está conformada por 57 abogados fedatarios juramentados con especialización en informática.

5.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

5.4.1 TÉCNICAS

En la demostración de las hipótesis y respuesta a los problemas de la investigación, se utilizará la técnica de la Encuesta; por ser la que mejor se adapta a las posibilidades de la investigación, para poder obtener la información de los expertos que conforman la muestra.

5.4.2 INSTRUMENTOS

El instrumento elaborado para la presente investigación es el Cuestionario, el cual nos permitirá obtener información pertinente, confiable y segura para la demostración de las hipótesis y cumplimiento de los objetivos del presente trabajo.

5.4.3 VALIDEZ Y CONFIABILIDAD

Para la validez de contenido del instrumento de investigación, se ha aplicado la técnica de juicio de cinco expertos validada con la prueba V de Aiken, todos abogados con el grado de doctor en derecho, en primer lugar el Dr. José Antonio Rodríguez Ulloa, doctor en derecho en la Universidad Alas Peruanas, en segundo lugar el Dr. Wander Saúl Muñoz Pantigoso, doctor en derecho en la Universidad Alas Peruanas, en tercer lugar el Dr. Kennedy Peter Pacheco Montes, doctor en derecho en la Universidad San Martín de Porres, en cuarto lugar el Dr. Vladimir Villarreal Balbín, doctor en derecho en la Universidad Alas Peruanas y por último el Dr. Roger Cabrera Paredes, doctor en derecho en la Universidad Nacional de la Amazonía Peruana, cuyos formatos de validación de expertos constan como anexo 3 y la prueba V de Aiken como anexo 4 del presente informe de tesis, cuyo resultado es el que indicamos a continuación:

En la prueba V de Aiken, aplicada a cada uno de los ítems de la prueba de validez de contenido por juicio de expertos, se utilizó el coeficiente con la fórmula siguiente:

$$V = \frac{S}{(n(c.1))}. \qquad 1.00 = \frac{25}{(5(5x1))}. \qquad 0.96 = \frac{24}{(5(5x1))}. \qquad 0.92 = \frac{23}{(5(5x1))}.$$

Como se aprecia en los resultados de la prueba V de Aiken, todos los ítems individualmente fueron válidos, toda vez que cuatro de ellos fue de 1.00, en 3 ítems se obtuvo 0.96 y en los otros 3 ítems 0.92; en consecuencia, todos ellos nos brindan la validez de contenido del instrumento de investigación, con un resultado final cuantitativo de 19.28 en sistema vigesimal o porcentual de 96.4 %, teniendo como resultado cualitativo el de excelente.

Para la Confiabilidad del instrumento de investigación se ha utilizado la prueba Alfa de Cronbach o KR-20, cuya fórmula estadística a aplicar fue la siguiente:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

Donde:
K: El número de ítems
Vi: Sumatoria de Varianzas de los Ítems
Vt: Varianza de la suma de los Ítems
α: Coeficiente de Alfa de Cronbach

Su aplicación y resultados detallados los podemos observar en la tabla que presentamos a continuación, con los resultados estadísticos totales de cada elemento:

Tabla: 12

N° de Pregunta del instrumento de investigación	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
PREGUNTA 2	36.61	15.277	.401	.689
PREGUNTA 3	36.93	15.995	.093	.721
PREGUNTA 4	37.09	15.689	.194	.708
PREGUNTA 5	36.75	16.474	.024	.724
PREGUNTA 6	37.25	14.403	.497	.676
PREGUNTA 7	36.65	15.232	.397	.689
PREGUNTA 8	36.81	15.730	.207	.706
PREGUNTA 9	37.23	13.965	.425	.681
PREGUNTA 10	37.04	13.784	.500	.671
N° de Pregunta del instrumento de investigación	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
PREGUNTA 12	37.39	14.241	.498	.674
PREGUNTA 13	37.42	14.462	.519	.675
PREGUNTA 14	37.42	14.462	.519	.675
PREGUNTA 15	36.63	15.915	.186	.707
PREGUNTA 16	37.14	15.980	.181	.708
PREGUNTA 17	36.65	15.589	.240	.703
PREGUNTA 18	36.72	16.598	.007	.724
PREGUNTA 19	37.61	15.384	.217	.707

Para medir la confiabilidad mediante la prueba estadística Alfa de Cronbach, seguimos los criterios que detallamos a continuación:

Coeficiente alfa de Cronbach mayor a 0,9 es ***Excelente***
Coeficiente alfa de Cronbach mayor a 0,8 y menor a 0,9 es ***Bueno***
Coeficiente alfa de Cronbach mayor a 0,7 y menor a 0,8 ***Aceptable***
Coeficiente alfa de Cronbach mayor a 0,6 y menor a 0,7 ***Cuestionable***
Coeficiente alfa de Cronbach mayor a 0,5 y menor a 0,6 ***Pobre***
Coeficiente alfa de Cronbach menor a 0,5 es ***Inaceptable***

En tal sentido, aplicando la fórmula en el programa informático estadístico SPSS 23, hemos tenido un resultado estadístico de fiabilidad considerado como aceptable, debido a que nuestro resultado total lo apreciamos a continuación:

Estadísticas de fiabilidad

Alfa de Cronbach	N° de elementos
0,710	17

En consecuencia, aplicando las pruebas estadísticas V de Aiken y Alfa de Cronbach, hemos obtenido un resultado de EXCELENTE en la prueba de validez de contenido del instrumento de investigación y un resultado de ACEPTABLE en la prueba de confiabilidad del instrumento de investigación.

5.4.4 PROCESAMIENTO Y ANÁLISIS DE DATOS

El procedimiento para la obtención, procesamiento y análisis de los datos, ha sido el que indicamos a continuación:

Para la Obtención.

- Se elaboró el cuestionario de la encuesta, en base a los indicadores y dimensiones de las variables, conforme a la matriz que presentamos a continuación:

Tabla: 13				
VARIA-BLE	**DIMEN-SIONES**	**INDICADORES**	**PREGUNTAS DE CONTENIDO**	**PREGUNTAS DE FILTRO Y CONTROL**
INDE-PEN-DIENTE (X): **PRO-TEC-CIÓN DE DATOS PERSO-NALES**	El titular de los datos personales	• Medios de Exposición de datos. • Razones de Exposición de datos.	Preguntas 3 y 7, 4 y 5	Preguntas 1, 11 y 2
	La Ley de Protección de Datos Personales	• Consentimiento. • Tratamiento de Datos Personales. • Registro de Bancos de Datos. • Infracciones y sanciones.	Preguntas 6, 9, 8 y 10	Preguntas 1, 11 y 2
DEPEN-DIENTE (Y): **DELI-TOS INFOR-MÁTI-COS**	Delitos Informá-ticos previstos en la Ley N° 30096 modifica-da por la Ley N° 30171	• Delitos contra los datos y sistemas informáticos.	Preguntas 12 a 14	Preguntas 11, 20 y 2
		• Delitos contra la libertad e indemnidad sexual.	Pregunta 15	Preguntas 11, 20 y 2
		• Delitos contra la Intimidad y Secreto de las Comunicaciones.	Pregunta 16	Preguntas 11, 20 y 2
		• Delitos contra el Patrimonio	Pregunta 17	Preguntas 11, 20 y 2
		• Delitos contra la Fe Pública.	Preguntas 18 y 19	Preguntas 11, 20 y 2

- Se remitió por correo electrónico, el cuestionario de la encuesta, a sesenta fedatarios juramentados con especialización en informática, tres de los cuestionarios fueron descartados por no ser fiables al no estar correctamente contestadas las tres preguntas de filtro, quedando un total de cincuenta y siete (57) cuestionarios de encuestas, que corresponde a la cantidad de personas que conforman la muestra.

- También vía correo electrónico, fueron devueltos la totalidad de cuestionarios de la encuesta, de los cuales los 57 sujetos de la muestra los remitieron debidamente contestados.

Para el procesamiento.

- Se vació la información de las respuestas en una base de datos general, en el programa informático SPSS 22.

- Asimismo, se vació la información en tablas independientes para cada pregunta, convirtiéndolos en diversos gráficos que permitan apreciar mejor el resultado.

Para el análisis de los datos.

- A fin de realizar el análisis univariado, se analizó la información en tablas independientes con tres ítems de valoración, para cada pregunta.

- De acuerdo a la matriz del instrumento de investigación señalada anteriormente, se analizó cada variable por separado, analizando primero cada indicador, a fin de determinar si confirmaban la dimensión y por ende hipótesis específica.

- Con el objeto de realizar el análisis bivariado o inferencial, se interrelacionaron los resultados globales de cada variable, verificando la hipótesis general, en la medida que también cada hipótesis específica había sido verificada, cuyo resultado fue validado con la prueba chi cuadrado de Pearson.

5.4.5 ÉTICA EN LA INVESTIGACIÓN

Se incluye como anexo ocho la declaratoria de autenticidad del informe de tesis, aspecto ético fundamental en la investigación, la cual es original y de total autoría del postulante al grado de Doctor, quién la ha redactado en su integridad, habiendo contado para su ejecución, con un asesor temático y metodológico y con un asesor estadístico.

CAPÍTULO VI: RESULTADOS

6.1 ANÁLISIS DESCRIPTIVO

En este ámbito, vamos a describir el análisis univariado, es decir el análisis individual de cada una de las variables, a partir del vaciado de los datos obtenidos en cada pregunta del cuestionario, organizados por las dimensiones e indicadores de cada variable.

El análisis univariado, es un análisis de tipo descriptivo, a realizarse en cada una de las variables individualmente, el cual se desarrollará en base a tablas diseñadas utilizando la frecuencia de Likert con tres ítems o valores de medición, para la presentación de los resultados obtenidos con el cuestionario de la encuesta.

6.1.1 ANALISIS VARIABLE X

La variable X, es la "Protección de Datos Personales", habiéndose elaborado el instrumento de investigación con ocho preguntas de contenido para esta variable, cuatro para cada dimensión. A continuación, presentaremos los resultados organizándolos en dos grupos por las dimensiones de esta variable, y dentro de cada dimensión, revisaremos los resultados respecto a cada uno de sus respectivos indicadores.

6.1.1.1 EL TITULAR DE LOS DATOS PERSONALES

Esta dimensión de la variable independiente, que corresponde a nuestra primera hipótesis específica "El titular de los datos personales, relaciona su uso indebido para la comisión de delitos informáticos", la hemos trabajado en base a dos indicadores, que son los siguientes:

- Medios de exposición de datos.
- Razones de exposición de datos.

6.1.1.1.1 Medios de Exposición de Datos

A través del primer indicador, se han establecido los medios mediante los cuales el titular de los datos personales expone sus datos, facilitando de esa manera que sean utilizados indebidamente para la comisión de delitos informáticos.

Las preguntas 3 y 7 del cuestionario de la encuesta, son las que se utilizaron para este indicador, con los resultados estadísticos siguientes:

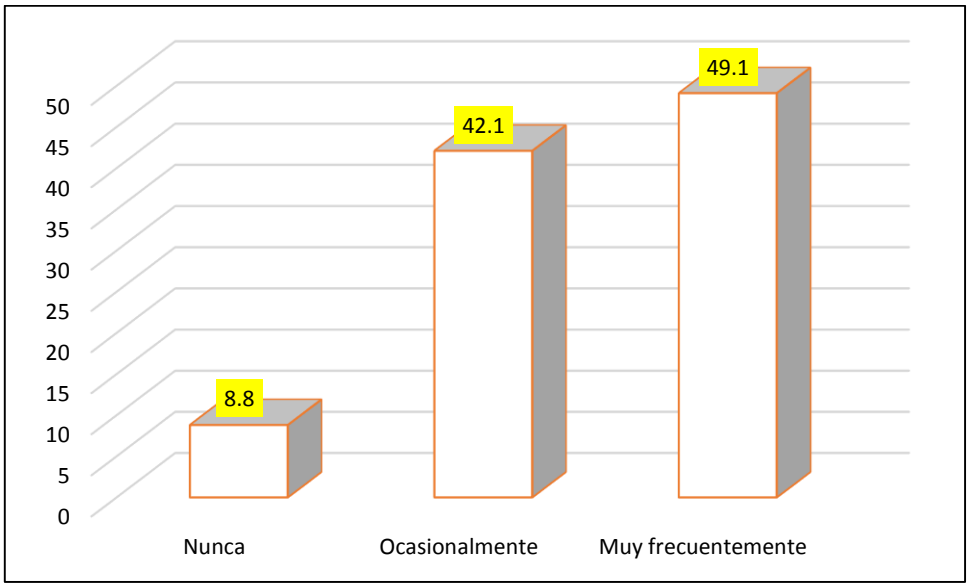
TABLA N° 14

El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en actividades de entretenimiento, como juegos on line, redes sociales, chats y otros medios de entretenimiento.

	Frecuencia	**%**
Nunca	5	8.8
Ocasionalmente	24	42.1
Muy frecuentemente	28	49.1
Total	57	100.0

GRÁFICO N° 1

El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en actividades de entretenimiento, como juegos on line, redes sociales, chats y otros medios de entretenimiento



En la Tabla N° 14 y el Gráfico N° 1, se presenta que el titular de los datos personales expone sus datos y por lo tanto los pone en riesgo, facilitando que sean utilizados por delincuentes informáticos, por su uso en actividades de entretenimiento, como juegos on line, redes sociales y chats, en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 49.1% (28) muy frecuentemente expone sus datos y los ponen en riesgo, el 42.1% (24) lo hacen ocasionalmente y el 8.8% (5) nunca ponen en riesgo sus datos.

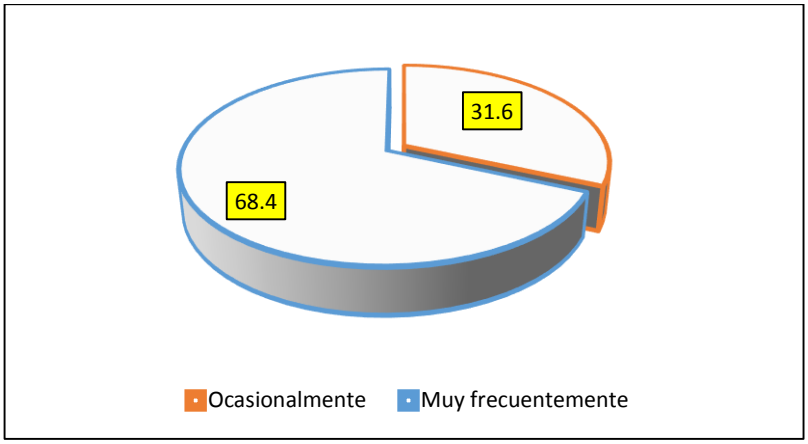
TABLA N° 15

El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en compras y ofertas de bienes y servicios por Internet y actividades de comercio electrónico en general.

	Frecuencia	**%**
Ocasionalmente	18	31.6
Muy frecuentemente	39	68.4
Total	57	100.0

GRÁFICO N° 2

El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en compras y ofertas de bienes y servicios por Internet y actividades de comercio electrónico en general.



En la Tabla N° 15 y el Gráfico N° 2 se presenta que el titular de los datos personales expone sus datos y por lo tanto los pone en riesgo, facilitando que sean utilizados por delincuentes informáticos, por su uso en compras y ofertas de bienes y servicios por Internet y actividades de comercio electrónico en general, en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 68.4% (39) muy frecuentemente expone sus datos y en consecuencia los pone en riesgo y el 31.6% (18) ocasionalmente lo hace.

De la descripción realizada, se puede observar que los titulares de los datos personales sí exponen sus datos y los ponen en riesgo, facilitando su uso por los delincuentes informáticos, apreciándose que contra lo comúnmente pensado, respecto a que el mayor riesgo de la exposición de los datos personales se presenta en medios de entretenimiento como juegos on line, redes sociales y chats; se encuentra que la forma considerada como de más alto riesgo en que los titulares exponen sus Datos Personales, es en las compras y ofertas de bienes y servicios por Internet, puesto que el resultado estadístico nos muestra que son 68.4% de las personas que exponen sus datos muy frecuentemente por ese medio, siendo esa cantidad mayor a los 49.1% que lo hacen muy frecuentemente a través de juegos on line, redes sociales, chats y otros medios de entretenimiento.

6.1.1.1.2 Razones de Exposición de Datos

El segundo indicador, relativo a las razones de exposición de datos personales, poniéndolos en riesgo y facilitando su uso indebido para la comisión de delitos informáticos, lo hemos planteado desde dos perspectivas, la primera formulada en la pregunta 4 del instrumento de investigación, dirigida a determinar si es por el desconocimiento de las personas de que pueden ser utilizados por los delincuentes informáticos, y la segunda contenida en la pregunta 5, respecto a si es por el desconocimiento y desinterés por proteger sus datos, habiéndose obtenido los resultados estadísticos que se presentan a continuación:

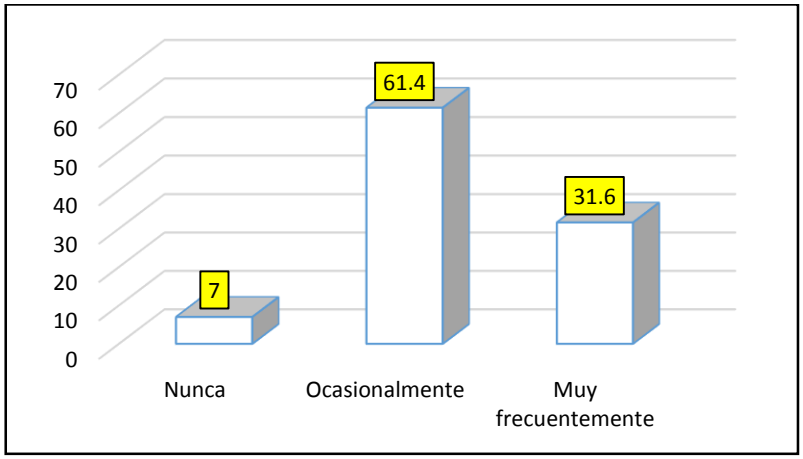
TABLA N° 16

El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento de que pueden ser utilizados por delincuentes informáticos.

	Frecuencia	%
Nunca	4	7
Ocasionalmente	35	61.4
Muy frecuentemente	18	31.6
Total	57	100.0

GRÁFICO N° 3

El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento de que pueden ser utilizados por delincuentes informáticos.



En la Tabla N° 16 y el Gráfico N° 3 se presenta que el titular de los datos personales expone sus datos y por lo tanto los pone en riesgo, facilitando que sean utilizados por delincuentes informáticos, por su desconocimiento de las consecuencias delictivas que puede acarrear, es decir que sean utilizados para la comisión de delitos informáticos, en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 31.6% (18) muy frecuentemente exponen sus datos personales y los ponen en riesgo por desconocimiento de que pueden ser usados por delincuentes informáticos, el 61.4% (35) lo hace ocasionalmente y el 7% (4) nunca los ponen en riesgo.

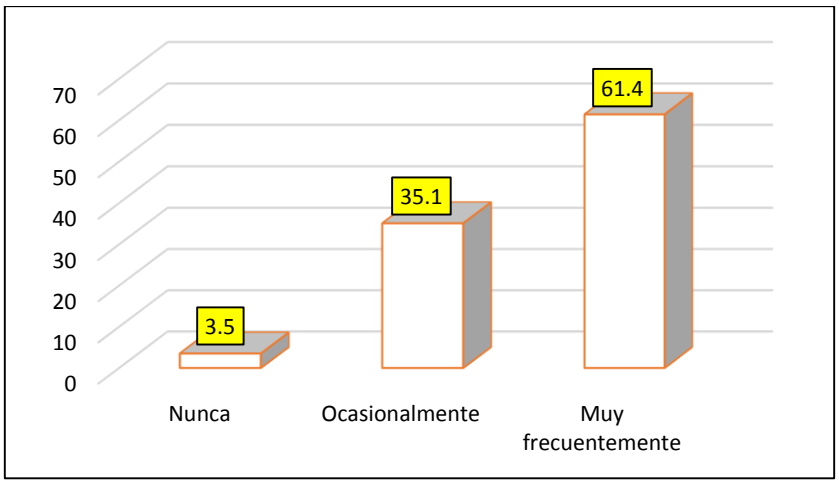
TABLA N° 17

El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento y desinterés en proteger sus datos personales

	Frecuencia	**%**
Nunca	2	3.5
Ocasionalmente	20	35.1
Muy frecuentemente	35	61.4
Total	57	100.0

GRÁFICO N° 4

El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento y desinterés en proteger sus datos personales



En la Tabla N° 17 y el Gráfico N° 4 se presenta que el titular de los datos personales expone sus datos y por lo tanto los pone en riesgo, facilitando que sean utilizados por delincuentes informáticos, por su desconocimiento y desinterés en proteger sus datos personales, en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 61.4% (35) muy frecuentemente exponen sus datos personales y los ponen en riesgo por desconocimiento y desinterés en protegerlos, el 35.1% (20) lo hace ocasionalmente y el 3.5% (2) nunca los ponen en riesgo.

De la descripción realizada en este segundo indicador, se puede observar que los titulares de los datos personales exponen sus datos y los ponen en riesgo, facilitando su uso por los delincuentes informáticos, principalmente por su desconocimiento y desinterés en proteger sus datos personales, puesto que el resultado estadístico nos muestra que son 61.4% de las personas que exponen muy frecuentemente sus datos personales por esa razón, siendo esa cantidad mayor al 31.6% que lo hacen muy frecuentemente por el desconocimiento de que puedan ser utilizados para la comisión de delitos informáticos.

6.1.1.2 LA LEY DE PROTECCIÓN DE DATOS PERSONALES.

La segunda dimensión de la variable independiente, que guarda coherencia con la segunda hipótesis específica, la hemos trabajado en base a cuatro indicadores, que son los siguientes:

- Consentimiento.
- Tratamiento de datos personales.
- Registro de Bancos de Datos.
- Infracciones y sanciones.

6.1.1.2.1 Consentimiento

Respecto al primer indicador, planteamos de manera directa la sexta pregunta, para conocer la opinión de los expertos, respecto a si la aplicación del principio de consentimiento y cumplimiento de sus requisitos, servía como un mecanismo regulado por la Ley de Protección de Datos Personales, y que permitía prevenir la comisión de

delitos informáticos, habiéndose obtenido los resultados estadísticos que se presentan a continuación:

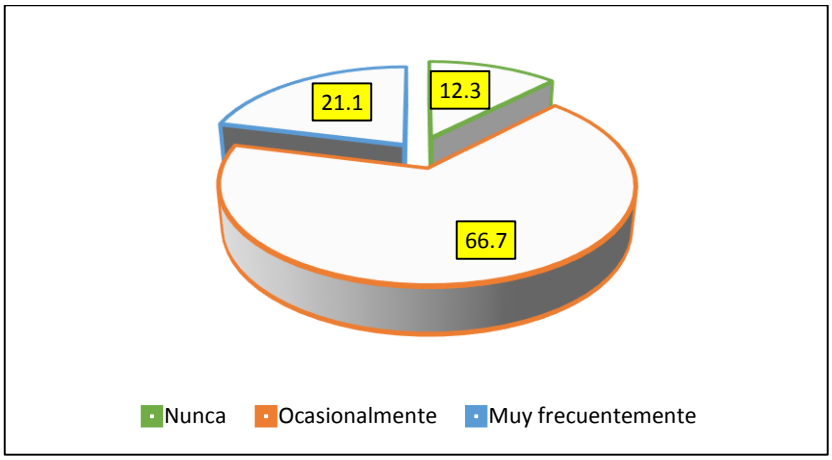
TABLA N° 18

La aplicación estricta del principio de consentimiento y la observancia de sus requisitos de libre, previo, expreso e inequívoco, y en el caso de los datos sensibles que sea por escrito, implica que se prevendrá la comisión de delitos informáticos

	Frecuencia	%
Nunca	7	12.3
Ocasionalmente	38	66.7
Muy frecuentemente	12	21.1
Total	57	100.0

GRÁFICO N° 5

La aplicación estricta del principio de consentimiento y la observancia de sus requisitos de libre, previo, expreso e inequívoco, y en el caso de los datos sensibles que sea por escrito, implica que se prevendrá la comisión de delitos informáticos



En la Tabla N° 18 y el Gráfico N° 5 se presenta que la Ley de Protección de Datos Personales, provee como un medio de protección de los datos personales, el principio de consentimiento y los requisitos para que el titular de los datos personales emita su consentimiento, es decir que sea libre, previo, expreso e inequívoco, sirviendo para prevenir la comisión de los delitos informáticos; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 21.1% (12) muy frecuentemente piensan que el principio de consentimiento y la observancia de sus requisitos, si van a prevenir la

comisión de delitos informáticos, una cantidad mayoritaria, el 66.7% (38) piensan que lo hace ocasionalmente y el 12.3% (7) piensa que nunca sirve el principio de consentimiento y sus requisitos para prevenir la delincuencia informática.

6.1.1.2.2 Tratamiento de Datos Personales

Para este segundo indicador, se planteó la pregunta nueve, relativa a si las medidas de seguridad sobre el tratamiento de los datos personales, conforme lo establece la ley en la materia, garantiza que no sean utilizados ilegalmente y en consecuencia se utilicen para la comisión de delitos informáticos, habiéndose obtenido los resultados estadísticos que se presentan a continuación:

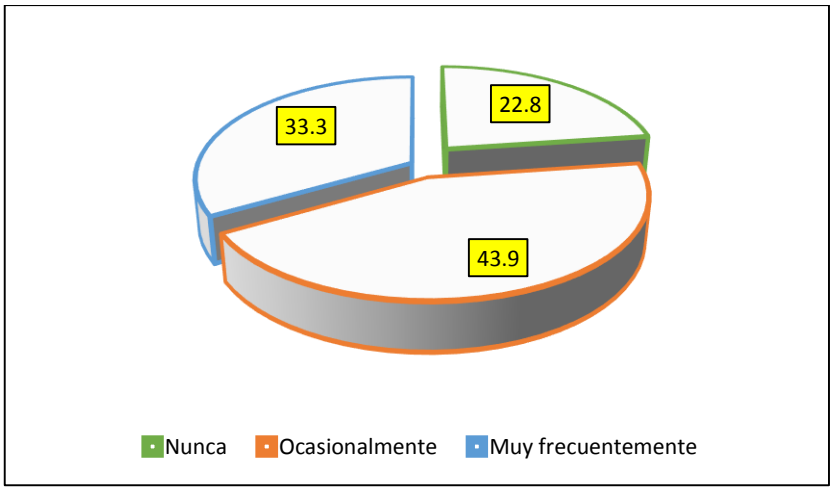
TABLA N° 19

Las medidas de seguridad para sobre el tratamiento de los datos personales, garantizan que estos no sean accesibles a delincuentes informáticos.

	Frecuencia	%
Nunca	13	22.8
Ocasionalmente	25	43.9
Muy frecuentemente	19	33.3
Total	57	100.0

GRÁFICO N° 6

Las medidas de seguridad para sobre el tratamiento de los datos personales, garantizan que estos no sean accesibles a delincuentes informáticos.



En la Tabla N° 19 y el Gráfico N° 6, se presenta que la Ley de Protección de Datos Personales, provee como un medio de protección de los datos personales, las normas sobre tratamiento de datos personales, cuyas medidas de seguridad previstas en la referida Ley, van a servir o garantizar que no sean accesibles a delincuentes informáticos y por ende no se utilicen en la comisión de ciberdelitos; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 33.3% (19) muy frecuentemente piensa que las medidas de seguridad en el tratamiento de los datos personales si ayuda a proteger los datos, mientras que el 43.9% (25) piensa que ocasionalmente protege los datos y el 22.8% (13) piensa que esas medidas de seguridad nunca ayudarán a proteger los datos de los ciberdelincuentes.

6.1.1.2.3 Registro de Bancos de Datos

El tercer indicador alude a otro mecanismo que ofrece nuestra legislación sobre protección de datos personales, consistente en la creación de un Registro de los Bancos de Datos Personales, inexistente hasta ese entonces en nuestro país, estando obligadas todas las instituciones públicas o privadas a inscribir sus Bancos de Datos en el Registro a cargo de la Autoridad Administrativa a nivel nacional. En este sentido se formuló la pregunta ocho (08), respecto a si la inscripción obligatoria en el referido Registro de Bancos de Datos, servía para ayudar en la prevención de los delitos informáticos, habiéndose obtenido los resultados estadísticos que se presentan a continuación:

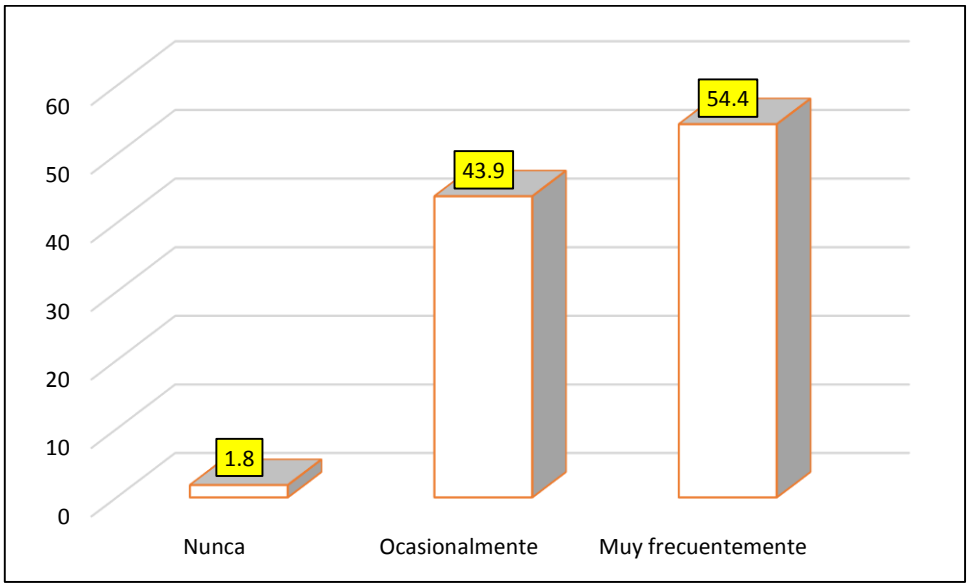
TABLA N° 20

La inscripción obligatoria de los bancos de datos personales en el registro nacional, es una medida que ayudará a la prevención de los delitos informáticos.

	Frecuencia	**%**
Nunca	1	1.8
Ocasionalmente	25	43.9
Muy frecuentemente	31	54.4
Total	57	100.0

GRÁFICO N° 7

La inscripción obligatoria de los bancos de datos personales en el registro nacional, es una medida que ayudará a la prevención de los delitos informáticos



En la Tabla N° 20 y el Gráfico N° 7 se presenta que la Ley de Protección de Datos Personales, mediante la inscripción obligatoria de los bancos de datos en el registro nacional, es una medida que ayudará a la prevención de los delitos informáticos; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 54.4% (31) muy frecuentemente piensan que la disposición legal de que todo Banco de Datos Personales tiene que ser inscrito en el Registro Nacional, si es una medida que ayuda a la prevención de los delitos informáticos, el 43.9% (25) piensan que ocasionalmente lo hace y el 1.8% (1) piensa que nunca ayudará a prevenir los delitos informáticos.

6.1.1.2.4 Infracciones y Sanciones

En cuanto al cuarto indicador, relativo a que las infracciones y sanciones previstas por la Ley de Protección de Datos Personales y modificadas por el D. Leg. N° 1145, tipificadas en la actualidad en su Reglamento, el que identifica una serie de conductas clasificadas como infracciones leves, graves o muy graves, con diferentes parámetros de sanción económica o multa que puede llegar a las 100 UITs, es decir más de trescientos mil soles, tienen una capacidad disuasiva que coadyuva en la prevención

de los delitos informáticos; habiéndose obtenido los resultados estadísticos que se presentan a continuación:

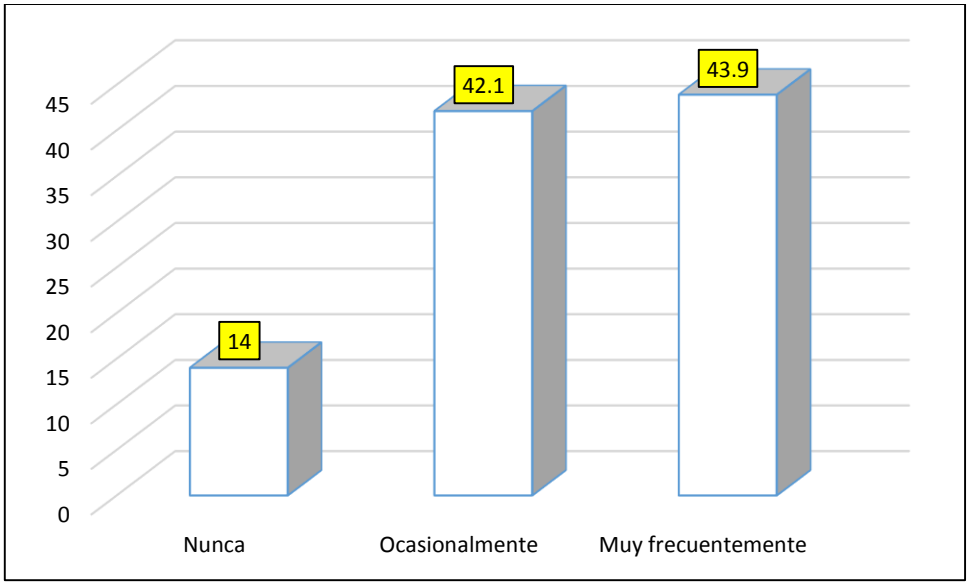
TABLA N° 21

Las infracciones y sanciones que prevén las normas de protección de datos personales, garantizan que estos no sean accesibles a delincuentes informáticos

	Frecuencia	**%**
Nunca	8	14
Ocasionalmente	24	42.1
Muy frecuentemente	25	43.9
Total	57	100.0

GRÁFICO N° 8

Las infracciones y sanciones que prevén las normas de protección de datos personales, garantizan que estos no sean accesibles a delincuentes informáticos



En la Tabla N° 21 y el Gráfico N° 8, se presenta que la Ley de Protección de Datos Personales, al establecer una serie de infracciones con sus respectivas sanciones, van a servir para garantizar que estos no sean utilizados de manera ilegal, facilitando su acceso a delincuentes informáticos; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 43.9% (25) muy frecuentemente piensa que esas infracciones y sanciones, sí ayudan a proteger los datos de los delincuentes informáticos, el 42.1% (24)

piensa que ocasionalmente lo hace y el 14% (8) piensa que nunca ayuda a proteger los datos de los delincuentes informáticos.

En resumidas cuentas, el análisis univariado de la variable independiente "X", permite encontrar que la opinión de los especialistas se inclina a determinar que la Ley de Protección de Datos Personales, sí coadyuva en la prevención de los delitos informáticos, por presentar mecanismos que van a redundar en prevenir que los delincuentes informáticos no accedan a los mismos, existiendo a pesar de ello, exposición a riesgo de los datos personales por parte de sus titulares, especialmente cuando compran por Internet, desconociendo o teniendo desinterés en proteger sus datos personales.

6.1.2. ANALISIS VARIABLE Y

La variable Y, es los "Delitos Informáticos", habiéndose elaborado el instrumento de investigación con ocho preguntas de contenido para esta variable, una para cada delito que en su integridad conforman una sola dimensión, "Los Delitos Informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171".

6.1.2.1 DELITOS INFORMÁTICOS PREVISTOS EN LA LEY N° 30096 MODIFICADA POR LA LEY N° 30171

La dimensión de la variable dependiente, la hemos trabajado en base a cinco indicadores, los cuales en esta sección describiremos uno a uno, en la medida que son afectados por la variable independiente, es decir, en qué medida influye la protección de los datos personales, afectando o no la posibilidad de comisión de los delitos informáticos.

Los cinco indicadores obedecen a la misma organización que tiene la presente dimensión los cuales detallamos a continuación:

- Delitos contra los datos y sistemas informáticos.
- Delitos contra la libertad e indemnidad sexual.
- Delitos contra la intimidad y secreto de las comunicaciones.
- Delitos contra el patrimonio.
- Delitos contra la fe pública.

6.1.2.1.1 Delitos contra los datos y sistemas informáticos

Dentro de este indicador era necesario analizar tres delitos diferentes, el de acceso ilícito, el de atentado contra la integridad de sistemas informáticos y el de atentado contra la integridad de datos informáticos, considerados en las preguntas 12, 13 y 14 del instrumento de investigación, presentando a continuación, los resultados estadísticos aplicados para cada uno de esos tres índices del presente indicador, como detallamos a continuación:

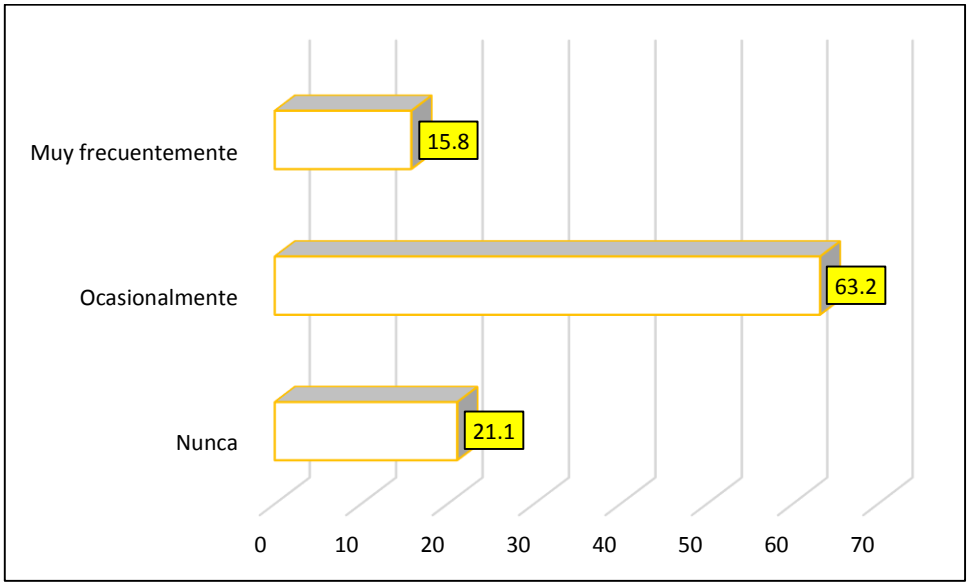
TABLA N° 22

El delito de acceso ilícito a un sistema informático, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	12	21.1
Ocasionalmente	36	63.2
Muy frecuentemente	9	15.8
Total	57	100.0

GRÁFICO N° 9

El delito de acceso ilícito a un sistema informático, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 22 y el Gráfico N° 9, se presenta que el delito informático de acceso ilícito a un sistema informático, se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 15.8% (9) muy frecuentemente piensa que sí se ve facilitado, el 63.2% (36) piensa que ocasionalmente se ve facilitado y el 21.1% (12) consideran que nunca se ve facilitado.

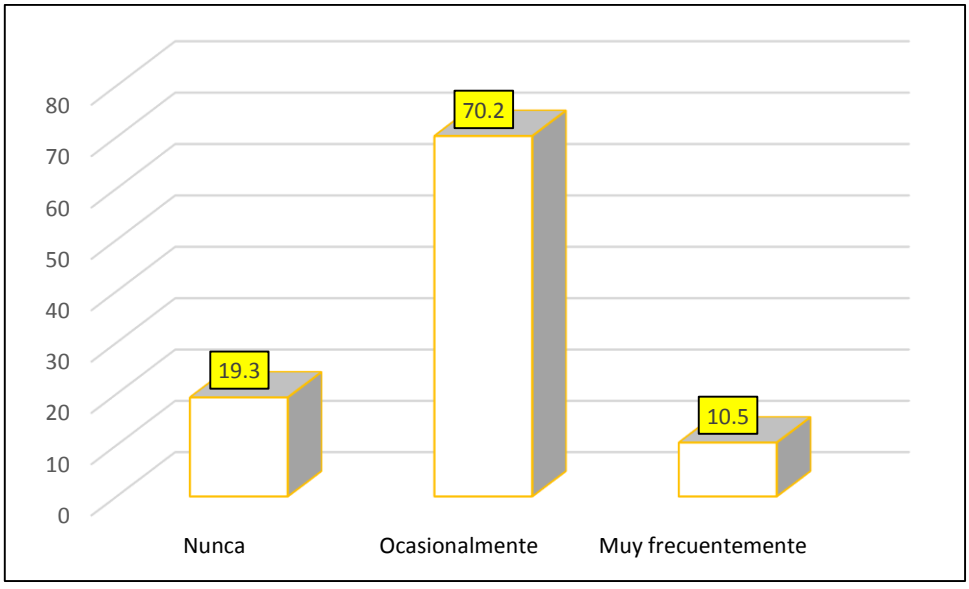
TABLA N° 23

El delito de atentado contra la integridad de sistemas informáticos, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	11	19.3
Ocasionalmente	40	70.2
Muy frecuentemente	6	10.5
Total	57	100.0

GRÁFICO N° 10

El delito de atentado contra la integridad de sistemas informáticos, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 23 y el Gráfico N° 10, se presenta que el delito informático de atentado contra la integridad de sistemas informáticos, se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%)

personas, el 10.5% (6) muy frecuentemente piensa que sí se ve facilitado, el 70.2% (40) piensa que ocasionalmente se ve facilitado y el 19.3% (11) consideran que nunca se ve facilitado

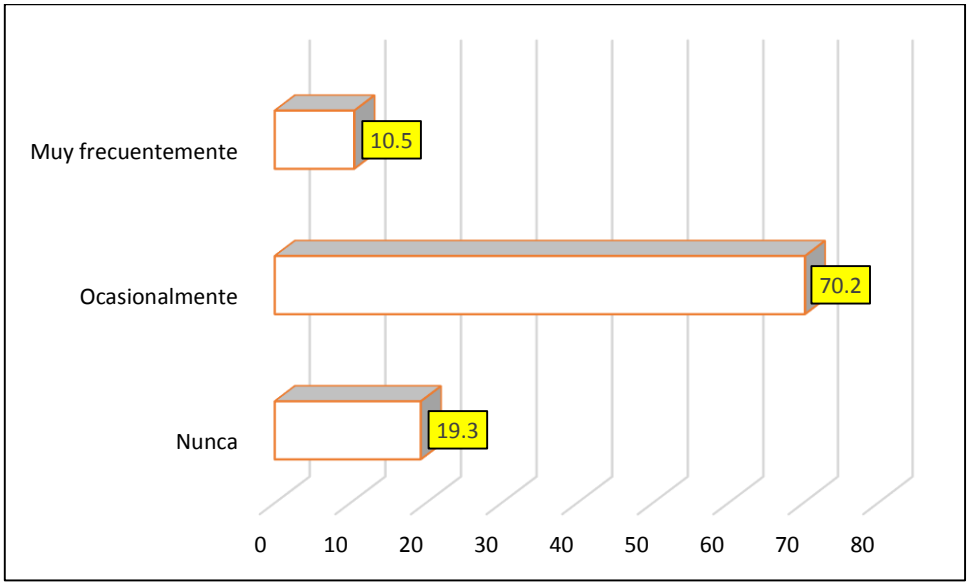
TABLA N° 24

El delito de atentado contra la integridad de datos informáticos, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	11	19.3
Ocasionalmente	40	70.2
Muy frecuentemente	6	10.5
Total	57	100.0

GRÁFICO N° 11

El delito de atentado contra la integridad de datos informáticos, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 24 y el Gráfico N° 11 se presenta que el delito informático de atentado contra la integridad de datos informáticos, se ve facilitado con el acceso a los datos

personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 10.5% (6) muy frecuentemente piensa que sí se ve facilitado, el 70.2% (40) piensa que ocasionalmente se ve facilitado y el 19.3% (11) consideran que nunca se ve facilitado.

Cabe agregar que, dentro de la teoría, estos tres delitos que integran el presente indicador, integran los llamados delitos informáticos per se, más en la práctica, es poco común que se presenten individualmente, pues suelen tener la condición de actos preparatorios o delitos en concurso, con otros que afectan bienes jurídicos que no sólo son la información, sino el patrimonio o la indemnidad sexual por citar a los dos que se presentan con mayor frecuencia como ejemplo.

Si examinamos los resultados estadísticos presentados en las tres tablas y tres gráficos precedentes, nos permiten describir que el indicador referido a los delitos contra los datos y sistemas informáticos, tiene una fuerte tendencia a que se vean influenciados ocasionalmente por la variable independiente; es decir, la falta de protección de datos personales, ocasionalmente facilita su acceso a los ciberdelincuentes, lo cual coadyuva a la comisión de los tres delitos que se encuentran clasificados como delitos contra los datos y sistemas informáticos e integran el presente indicador.

6.1.2.1.2 Delitos contra la libertad e indemnidad sexual

Si bien existen en el Código Penal una serie de delitos contra la libertad e indemnidad sexual, como son por ejemplo la Pornografía Infantil, Exhibiciones Obscenas, Turismo Sexual Infantil, cuya comisión también puede darse por medios informáticos, dentro de este indicador, encontramos sólo el delito de proposiciones a niños, niñas o adolescentes con fines sexuales por medios tecnológicos, también conocido como “grooming” o “child grooming”, que se encuentra tipificado en la Ley de Delitos Informáticos, habiendo planteado para su estudio la pregunta 15 del instrumento de investigación, cuyos resultados estadísticos son los que detallamos a continuación:

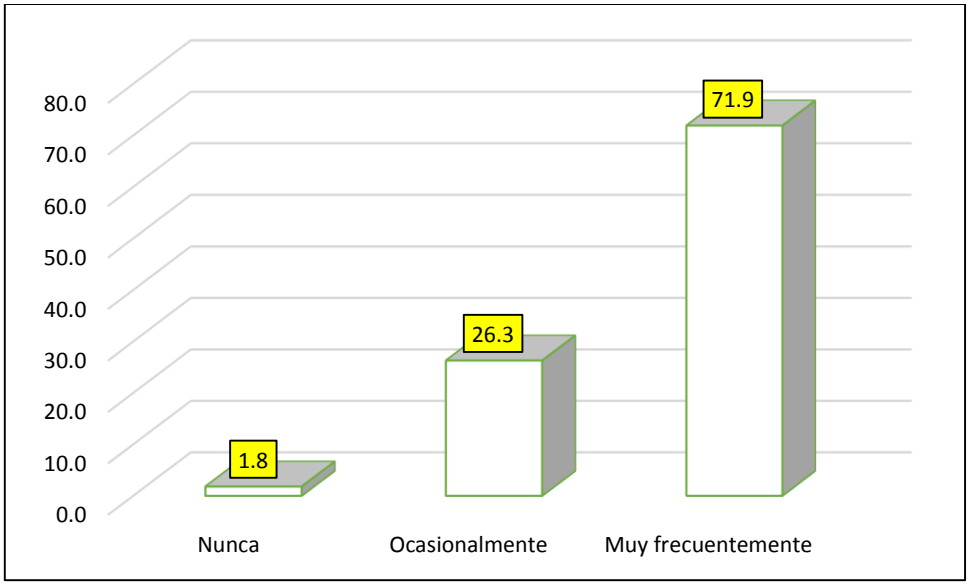
TABLA N° 25

El Delito de "Grooming" (Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos), se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	1	1.8
Ocasionalmente	15	26.3
Muy frecuentemente	41	71.9
Total	57	100.0

GRÁFICO N° 12

El Delito de "Grooming" (Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos), se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 25 y el Gráfico N° 12 se presenta que el delito informático de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos o Grooming, se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 71.9% (41) muy frecuentemente piensa que sí se ve facilitado, el 26.3% (15) piensa que ocasionalmente se ve facilitado y el 1.8% (1) considera que nunca se ve facilitado.

6.1.2.1.3 Delitos contra la intimidad y secreto de las comunicaciones

Después de que fuese derogado el art. 6° de la Ley de Delitos Informáticos, el único delito que ha quedado dentro de este indicador, es el de "Interceptación de Datos Informáticos", previsto en el art. 7° de la referida Ley de Delitos Informáticos modificada por la Ley N° 30171. Tal como en el caso anterior, existen otras figuras penales previstas en el Código Penal, cuya comisión puede realizarse por medios tecnológicos, como es la interceptación telefónica, cuyo estudio individualizado puede ser materia de tesis, pero en esta oportunidad, nuestro indicador debe referirse sólo al artículo reseñado, para lo cual se formuló la pregunta 16 del instrumento de investigación, cuyos resultados estadísticos son los que detallamos a continuación:

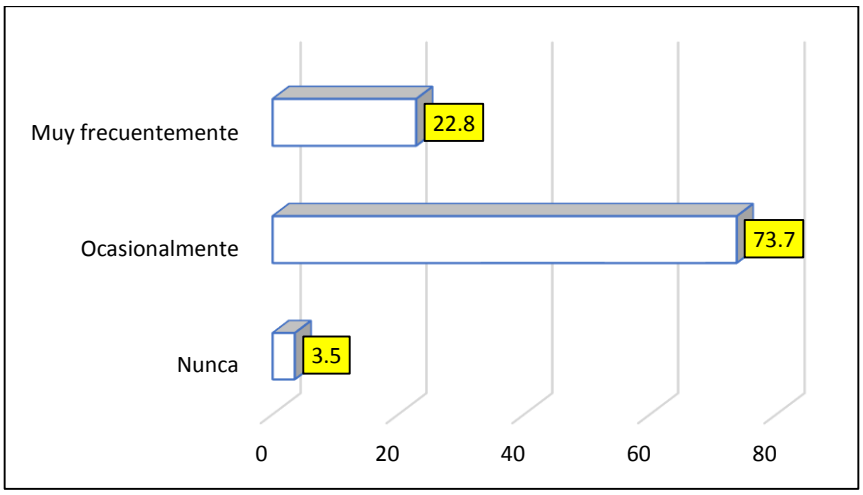
TABLA N° 26

El delito de intercepción de datos informáticos, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	2	3.5
Ocasionalmente	42	73.7
Muy frecuentemente	13	22.8
Total	57	100.0

GRÁFICO N° 13

El delito de intercepción de datos informáticos, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 26 y el Gráfico N° 13 se presenta el delito informático de intercepción de datos informáticos, el cual se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 22.8% (13) muy frecuentemente piensa que sí se ve facilitado, el 73.7% (42) piensa que ocasionalmente se ve facilitado y el 3.5% (2) consideran que nunca se ve facilitado.

6.1.2.1.4 Delitos contra el patrimonio

A diferencia de los casos anteriores, el delito de Fraude Informático no coexiste con otros delitos contra el patrimonio que puedan cometerse por medios informáticos, tipificados en el Código Penal, debido a que el legislador redactó la conducta ilícita de este delito, buscando cubrir el universo de posibilidades y derogando por ende, las figuras delictivas que existían en el Código Penal, como era la de Hurto Agravado cuando se efectuaba por medio de dispositivos informáticos.

Para el estudio de este indicador, al igual que en los casos anteriores, se formuló una pregunta por cada delito en nuestro instrumento de investigación, correspondiendo a este caso la pregunta 17, cuyos resultados estadísticos son los que presentamos a continuación:

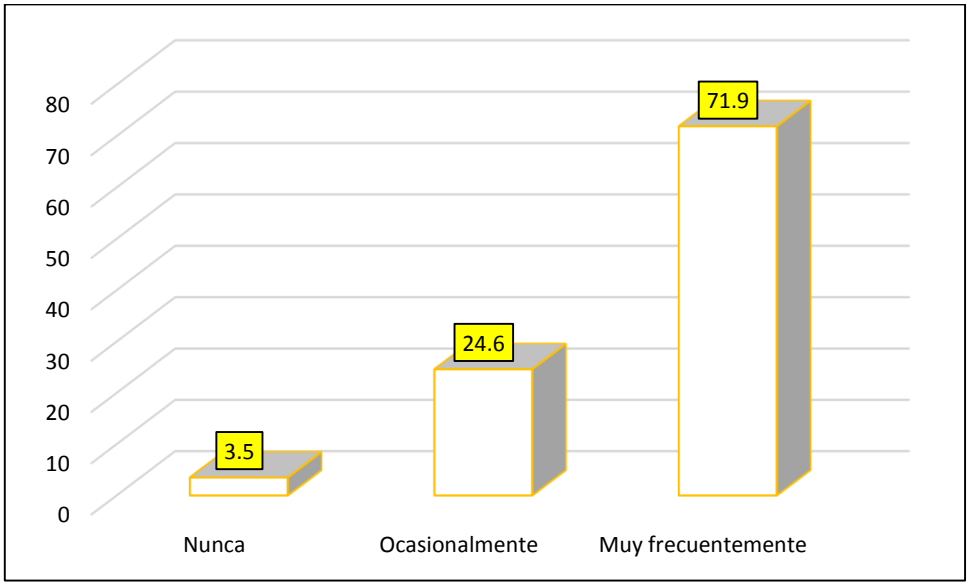
TABLA N° 27

El delito de fraude informático, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	**%**
Nunca	2	3.5
Ocasionalmente	14	24.6
Muy frecuentemente	41	71.9
Total	57	100.0

GRÁFICO N° 14

El delito de fraude informático, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 27 y el Gráfico N° 14 se presenta el delito informático de fraude informático, el cual se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 71.9% (41) muy frecuentemente piensa que sí se ve facilitado, el 24.6% (14) piensa que ocasionalmente se ve facilitado y el 3.5% (2) consideran que nunca se ve facilitado.

6.1.2.1.5 Delitos contra la fe pública

En este quinto indicador, hemos agrupado a dos delitos, por una parte el de suplantación de identidad, cuyo bien jurídico protegido es la fe pública y por otro lado el de abuso de mecanismos y dispositivos informáticos, que bien podría considerarse como actos preparatorios en lugar de un delito, pero que por su ubicación en la Ley de Delitos Informáticos, hemos decidido incluirlos dentro de este indicador, aunque pueda ser cuestionable que el bien jurídico que protege dista de ser la fe pública.

Para ello, hemos diseñado en nuestro instrumento de investigación las preguntas 18 y 19, cuyos resultados estadísticos detallamos a continuación:

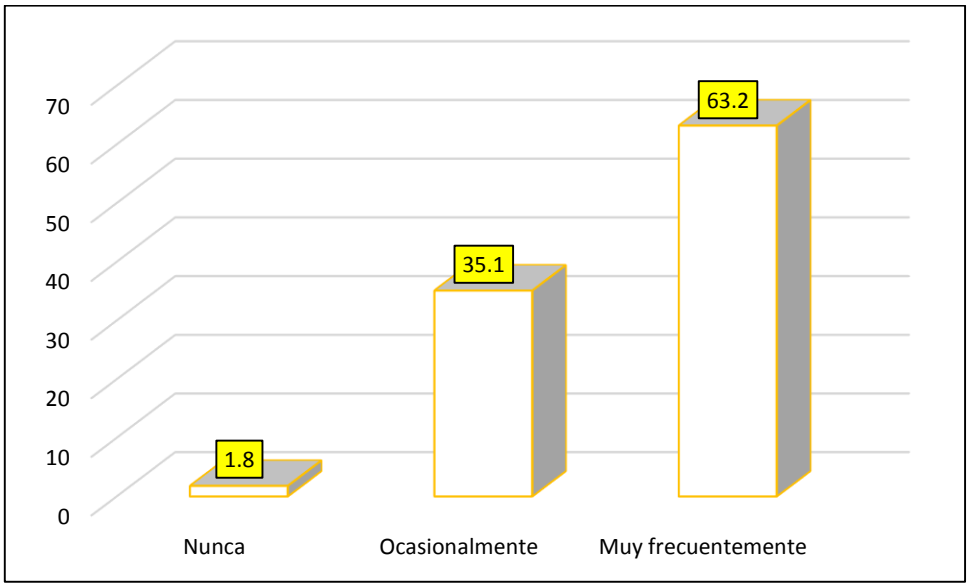
TABLA N° 28

El delito de suplantación de identidad mediante las tecnologías de la información y la comunicación, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	1	1.8
Ocasionalmente	20	35.1
Muy frecuentemente	36	63.2
Total	57	100.0

GRÁFICO N° 15

El delito de suplantación de identidad mediante las tecnologías de la información y la comunicación, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 28 y el Gráfico N° 15 se presenta el delito informático de suplantación de identidad mediante las tecnologías de la información y la comunicación, el cual se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 63.2% (36) muy frecuentemente piensa que sí se ve facilitado, el 35.1% (20) piensa que ocasionalmente se ve facilitado y el 1.8% (1) considera que nunca se ve facilitado.

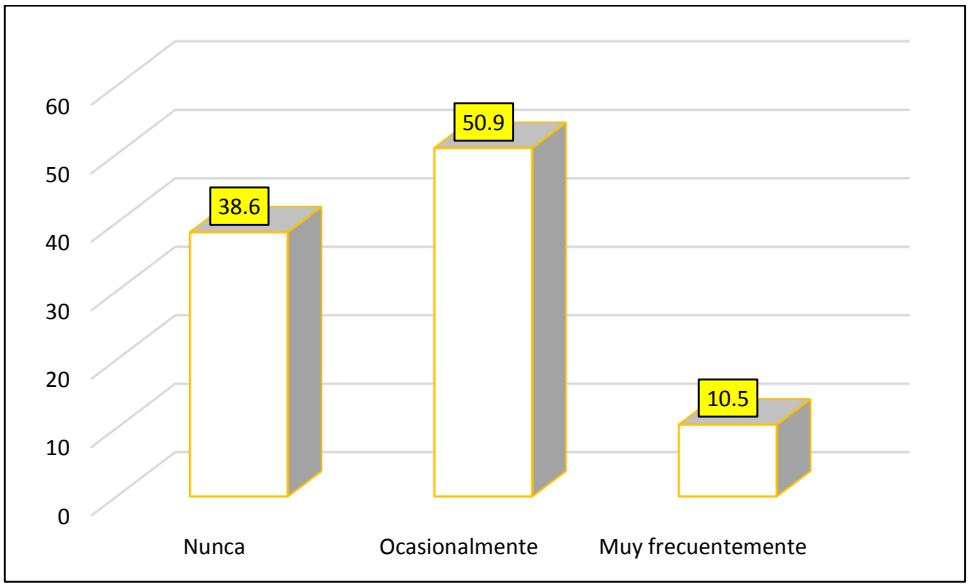
TABLA N° 29

El delito de abuso de mecanismos y dispositivos informáticos, se ve facilitado con el acceso a los datos personales de la víctima

	Frecuencia	%
Nunca	22	38.6
Ocasionalmente	29	50.9
Muy frecuentemente	6	10.5
Total	57	100.0

GRÁFICO N° 16

El delito de abuso de mecanismos y dispositivos informáticos, se ve facilitado con el acceso a los datos personales de la víctima



En la Tabla N° 29 y el Gráfico N° 16 se presenta el delito informático de abuso de mecanismos y dispositivos informáticos, el cual se ve facilitado con el acceso a los datos personales de la víctima; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 10.5% (6) muy frecuentemente piensa que sí se ve facilitado, el 50.9% (29) piensa que ocasionalmente se ve facilitado y el 38.6% (22) consideran que nunca se ve facilitado.

Como se puede apreciar, los especialistas abogados fedatarios juramentados con especialización en informática, consideran que los delitos que se ven facilitados con

mayor frecuencia con el acceso a los datos personales de los agraviados, son los de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (71.9%), , Fraude Informático (71.9%). y Suplantación de Identidad (63.2%).

6.2. ANALISIS INFERENCIAL

En el análisis inferencial, vamos a correlacionar los resultados obtenidos de nuestras dos variables, contrastando la hipótesis desde una perspectiva estadística y analizándola también con un enfoque lógico jurídico, que nos servirán para determinar la confirmación de la hipótesis (H_1) de nuestro trabajo de investigación, o en caso contrario, comprobar la hipótesis nula (H_0).

6.2.1. ANALISIS ESTADÍSTICO DE CONTRASTACIÓN DE LA HIPÓTESIS GENERAL

Lo vamos a realizar a partir de la aplicación de la prueba estadística de normalidad Kolmogorov-Smirnov, aplicable a muestras mayores a 50, y la prueba de hipótesis bivariadas chi cuadrado de Spearson.

6.2.1.2.PRUEBA ESTADÍSTICA DE NORMALIDAD

Para la prueba de Kolmogorov-Smirnov, se ha realizado el análisis estadístico siguiente:

Hipótesis

- **H_0** : Los datos de las variables siguen una distribución normal
- **H_1** : Los datos de las variables no siguen una distribución normal

Nivel de significancia

Para efectos de la investigación se determinó $\alpha = 0{,}05$

Estadístico

El valor estadístico de prueba que se ha considerado para la presente Hipótesis es Kolmogorov – Smirnov

TABLA N° 30

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Protección de datos personales	,484	57	,000	,503	57	,000
Delitos informáticos	,539	57	,000	,168	57	,000

a. Corrección de significación de Lilliefors

Decisión

Como el valor p de significancia del estadístico de prueba de normalidad tiene el valor de 0,000 y 0,000 entonces para valores Sig. < 0,05; se cumple que: se rechaza la Hipótesis nula y se acepta la Hipótesis alternativa, los datos de las variables no siguen una distribución normal.

6.2.1.2.PRUEBA DE HIPÓTESIS CON CHI CUADRADO

Para la prueba de hipótesis bivariada, se va a utilizar la prueba no paramétrica Chi cuadrado, cuyo desarrollo estadístico detallamos a continuación:

Hipótesis General

H_1 : La protección de datos personales, sí se relaciona en forma directa con la prevención de los delitos informáticos en el Perú.

H_0: La protección de datos personales, no se relaciona en forma directa con la prevención de los delitos informáticos en el Perú.

Nivel de significancia

Para la presente investigación se ha determinado que $\alpha = 0.05$

Estadístico de prueba

Con el propósito de establecer el grado de relación entre cada una de las variables objeto de estudio, se utilizó la prueba no paramétrica chi–cuadrado de Pearson

TABLA N° 31

Prueba de chi-cuadrado de la Hipótesis General

	Valor	gl	Sig. asintótica (2 caras)	Significación exacta (2 caras)	Significación exacta (1 cara)
Chi-cuadrado de Pearson	4,676[a]	1	,031		
Corrección de continuidad[b]	2,977	1	,084		
Razón de verosimilitud	4,835	1	,028		
Prueba exacta de Fisher				,073	,042
Asociación lineal por lineal	4,594	1	,032		
N de casos válidos	57				

Para contrastar la hipótesis general, los resultados fueron sometidos a la prueba estadística no paramétrica de chi–cuadrado, encontrando para la protección de datos y los delitos informáticos: $X^2_C = 4.676$, gl.= 1, p= 0.031 < 0.05 siendo significativo se rechaza H_0 y se acepta H_1

Toma de decisión

Se verifica que: La protección de datos personales, sí se relaciona en forma directa con la prevención de los delitos informáticos en el Perú.

La prueba chi-cuadrado, también se ha aplicado a las dos Hipótesis Específicas, las mismas que también han sido verificadas, con lo cual también se corrobora metodológicamente la hipótesis general, toda vez que la sumatoria de las hipótesis específicas permite confirmar la hipótesis general.

Para aplicar la prueba chi-cuadrado a las hipótesis específicas, se ha utilizado el grado de relación con tabulación cruzada entre cada una de las variables objeto de estudio, con los resultados confirmatorios de las mismas, que detallaremos a continuación.

Hipótesis Específica 1

La hipótesis específica alterna 1, es la siguiente:
El titular de los datos personales, los expone relacionando directamente su uso indebido para la comisión de delitos informáticos.

La hipótesis específica nula 1, es la siguiente:
El titular de los datos personales, no los expone relacionando directamente su uso indebido para la comisión de delitos informáticos.

Nivel de significancia

Para la presente investigación se ha determinado que $\alpha = 0.05$

TABLA N° 32

Prueba de chi-cuadrado Hipótesis Específica 1

	Valor	Gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	5,961[a]	2	.031
Razón de verosimilitud	5.976	2	.050
Asociación lineal por lineal	5.570	1	.018
N de casos válidos	57		

Como hemos señalado, para contrastar la hipótesis específica 1, los resultados fueron sometidos a la prueba estadística no paramétrica de chi–cuadrado, encontrando para la protección de datos y los delitos informáticos: $X^2_C = 5.961$, gl.= 2, p= 0.031 < 0.05 siendo significativo se rechaza la Hipótesis Específica Nula 1 y se acepta la Hipótesis Específica Alterna 1.

Toma de decisión

Se verifica que: El titular de los datos personales, los expone relacionando directamente su uso indebido para la comisión de delitos informáticos.

Hipótesis Específica 2

La hipótesis específica alterna 2, es la siguiente:
La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú.

La hipótesis específica nula 2, es la siguiente:
La Ley de Protección de Datos Personales, no se relaciona de manera directa con la prevención de los delitos informáticos en el Perú.

Nivel de significancia

Para la presente investigación se ha determinado que $\alpha = 0.05$

TABLA N° 33

Prueba de chi-cuadrado Hipótesis Específica 2

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	9,381[a]	4	.022
Razón de verosimilitud	13.377	4	.010
Asociación lineal por lineal	.905	1	.342
N de casos válidos	57		

Para contrastar la hipótesis específica 2, los resultados fueron sometidos a la prueba estadística no paramétrica de chi–cuadrado, encontrando para la protección de datos y los delitos informáticos: $X^2_C = 9.381$, gl.= 4, p= $0.022 < 0.05$ siendo significativo se rechaza se rechaza la Hipótesis Específica Nula 2 y se acepta la Hipótesis Específica Alterna 2.

Toma de decisión

Se verifica que: La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú.

6.2.2. ANÁLISIS BIVARIADO DE LA HIPÓTESIS GENERAL

El análisis que vamos a desarrollar en esta sección, es complementaria al análisis estadístico, mediante el cual ya se verificó la hipótesis general; pero consideramos pertinente agregar este análisis adicional, desde una doble perspectiva, una metodológica

que permite integrar las hipótesis específicas con la hipótesis general, y otra jurídica, que nos permite aportar al análisis desde nuestro campo del conocimiento, una comprensión de políticas normativas integrales que son características dentro de un ordenamiento jurídico.

6.2.2.1. PERSPECTIVA METODOLÓGICA

La metodología de investigación jurídica nos plantea una coherencia e interrelación de todos sus elementos, que le brindan coherencia y calidad a un trabajo de investigación, en el presente análisis vamos a efectuar el análisis bivariado, a partir de la premisa de que la sumatoria de las hipótesis específicas nos conducen a confirmar la hipótesis general, para lo cual también nos vamos a apoyar en los resultados estadísticos recogidos en el cuestionario de la encuesta.

La primera hipótesis específica nos dice que, "El titular de los datos personales, los expone relacionando directamente su uso indebido para la comisión de delitos informáticos"; que corresponde a la primera dimensión de la variable independiente (variable *X*), para cuyo análisis utilizamos dos indicadores, los cuales fueron objeto en el instrumento de investigación de dos preguntas cada uno, conforme presentamos en la tabla siguiente:

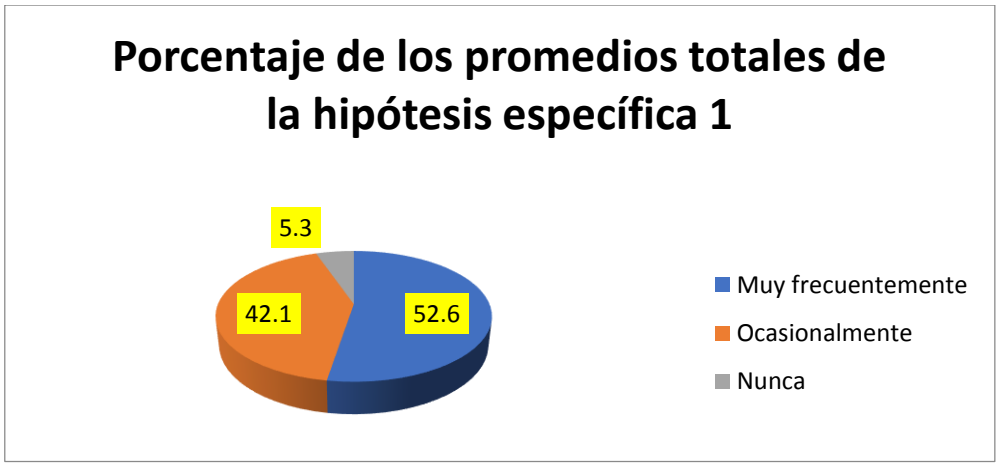
TABLA N° 34

DIMENSIÓN	**FRECUENCIA**			**TOTAL**
Titular de los Datos Personales	**Muy Frecuen-temente**	**Ocasional-mente**	**Nunca**	
Indicador: Medios de exposición de datos. (Pregunta 3)	49.1% (28)	42.1% (24)	8.8% (5)	100% (57)
Indicador: Medios de exposición de datos. (Pregunta 7)	68.4% (39)	31.6% (18)	0% (0)	100% (57)
Indicador: Razones de exposición de datos. (Pregunta 4)	31.6% (18)	61.4% (35)	7% (4)	100% (57)
Indicador: Razones de exposición de datos. (Pregunta 5)	61.4% (35)	35.1% (20)	3.5% (2)	100% (57)
PROMEDIOS TOTALES	**52.6% (30)**	**42.1% (24)**	**5.3% (3)**	100% (57)

Respecto a la Dimensión "El titular de los datos personales", en los promedios totales de la tabla precedente, se aprecia que 52.6% (30) de los abogados sometidos al cuestionario de la encuesta, consideran que muy frecuentemente los titulares de los datos personales exponen sus datos, poniéndolos en riesgo y facilitando su uso indebido para la comisión de delitos informáticos, 42.1% (24) consideran que ocasionalmente existe esta exposición de datos y el 5.3% (3) piensan que los titulares de los datos personales nunca los exponen.

Esos resultados para su mejor comprensión, los presentamos en el gráfico siguiente:

GRAFICO N° 17



Interpretando esos resultados, nos permite concluir que sí existe una opinión mayoritaria, superior al 50%, respecto a que los titulares de datos personales exponen sus datos, facilitando así su uso para la comisión de delitos informáticos; cuya diferencia es ampliamente notoria con los que piensan que nunca se produce esa situación.

En tal sentido, los datos estadísticos nos permiten colegir que, se ha confirmado la primera hipótesis específica, confirmando que "El titular de los datos personales, los expone relacionando directamente su uso indebido para la comisión de delitos informáticos".

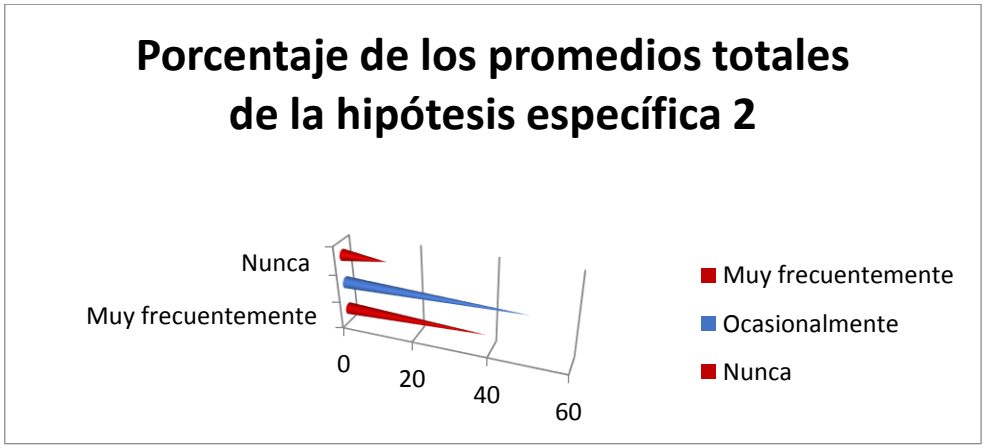
La segunda hipótesis específica nos dice que, "La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú"; que corresponde a la segunda dimensión de la variable independiente (variable *X*), para

cuyo análisis utilizamos cuatro indicadores, los cuales fueron objeto en el instrumento de investigación de una pregunta cada uno, conforme presentamos en la tabla siguiente:

TABLA N° 35				
DIMENSIÓN	**FRECUENCIA**			**TOTAL**
Ley de Protección de Datos Personales	**Muy Frecuen-temente**	**Ocasional-mente**	**Nunca**	
Indicador: Consentimiento. (Pregunta 6)	21.1% (12)	66.7% (38)	12.3% (7)	100% (57)
Indicador: Tratamiento de datos personales. (Pregunta 9)	33.3% (19)	43.9% (25)	22.8% (13)	100% (57)
Indicador: Registro de bancos de datos. (Pregunta 8)	54.4% (31)	43.9% (25)	1.8% (1)	100% (57)
Indicador: Infracciones y sanciones. (Pregunta 10)	43.9% (25)	42.1% (24)	14% (8)	100% (57)
PROMEDIOS TOTALES	**38.6% (22)**	**49.1% (28)**	**12.3% (7)**	100% (57)

Respecto a la Dimensión "La Ley de Protección de Datos Personales", en los promedios totales de la tabla precedente, se aprecia que 38.6% (22) de los abogados sometidos al cuestionario de la encuesta, consideran que muy frecuentemente la Ley de Protección de Datos Personales, ofrece medios de protección de datos personales ,que coadyuvan a prevenir los delitos informáticos, 49.1% (28) consideran que ocasionalmente existen estos medios de protección de datos y el 12.3% (7) piensan que la referida ley nunca provee medios de protección de los datos personales.

GRAFICO N° 18



Interpretando esos resultados, apreciamos que el 38.4% de abogados fedatarios juramentados con especialización en informática, que consideran que muy frecuentemente la Ley de Protección de Datos Personales ofrece medios de protección para esos datos, es superior al 12.3% que nunca considera que existen esos medios de protección.

En tal sentido, los datos estadísticos nos permiten colegir que, se ha confirmado la segunda hipótesis específica, confirmando que "La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú".

Habiendo confirmado cada una de las dos hipótesis específicas, aplicamos la premisa metodológica respecto a que la sumatoria de las hipótesis específicas nos conducen a confirmar la hipótesis general; en consecuencia, habiendo confirmado las hipótesis específicas, el resultado es que también se confirma la hipótesis general de que "La Protección de Datos Personales, sí se relaciona en forma directa con la prevención de los delitos informáticos en el Perú".

6.2.2.2. PERSPECTIVA JURÍDICA

Para analizar las hipótesis desde una perspectiva jurídica, vamos a utilizar lo que se denomina razonamiento jurídico, para lo cual, debemos recordar que se relaciona en la hipótesis general dos elementos, el primero de ellos la protección de datos personales, contenido en la Ley N° 29733 – Ley de Protección de Datos Personales, y el segundo que son los delitos informáticos, tipificados en la Ley N° 30096 – Ley de Delitos Informáticos.

La Ley N° 29733 "Ley de Protección de Datos Personales", y su normatividad complementaria, regulan un aspecto amplio y totalmente nuevo en el Perú, que anteriormente sólo tenía el reconocimiento constitucional gracias a la interpretación plasmada por el Tribunal Constitucional en diferentes Sentencias interpretativas.

Al ser bastante amplia, tuvimos que centrarnos en la persona que es el titular de los datos personales, quién los expone, relacionándolos de esa manera con su uso indebido por delincuente informáticos, así como en los medios que nos ofrece la ley en mención, para proteger los datos personales, relacionándola así como la prevención en la comisión de delitos informáticos en el Perú, por parte de ciberdelincuentes.

En ese sentido, de los diferentes mecanismos que ofrece la indicada Ley, regula el principio de consentimiento, que era algo desconocido en el Perú, es decir que te pidan autorización para registrar tus datos, también regula sobre el tratamiento de datos personales, otro de los aspectos novedosos que regula esta ley, es la creación del Registro Nacional de Bancos de Datos Personales y el cuarto que elegimos, fueron las diferentes infracciones y sanciones que establece esa ley ante su incumplimiento.

Si bien el proyecto legislativo para promulgar dicha ley data de principios de siglo, fue recién el año 2011 que se promulgó la Ley de Protección de Datos Personales, publicándose su reglamento en el año 2013, entrando en vigencia ambas el 08 de Mayo de 2013, no siendo casual que ese mismo año se apruebe la nueva Ley de Delitos Informáticos, lo que es parte de una política normativa, a cargo en la materia del Ministerio de Justicia y Derechos Humanos.

Por lo señalado, se infiere que ambas normas tienen una estrecha relación, que han dado lugar en diferentes países, a que se realice una importante difusión de sus normas sobre protección de datos personales, por su poder disuasivo y preventivo frente a los delincuentes que utilizan las redes informáticas para cometer sus actividades ilícitas

Como apreciamos, el análisis temporal relativo a la aprobación de ambas normas, su coincidencia sectorial para las iniciativas legislativas, así como la concordancia de sus normas, para las cuales aplicamos la interpretación jurídica, nos permiten demostrar también la hipótesis general, aplicando el método sistemático por comparación de normas, que nos permite entender la regulación de una de las leyes, concordándolas con las que se expresan en la otra.

A lo señalado, también recurrimos a la opinión especializada de los 57 abogados fedatarios juramentados con especialización en informática, expertos en derecho informático, especialidad que incluye el estudio de ambas leyes, a quienes se les planteó una pregunta de control, en la que se buscó conocer su opinión sobre nuestra hipótesis general, cuyos resultados se los detallamos a continuación:

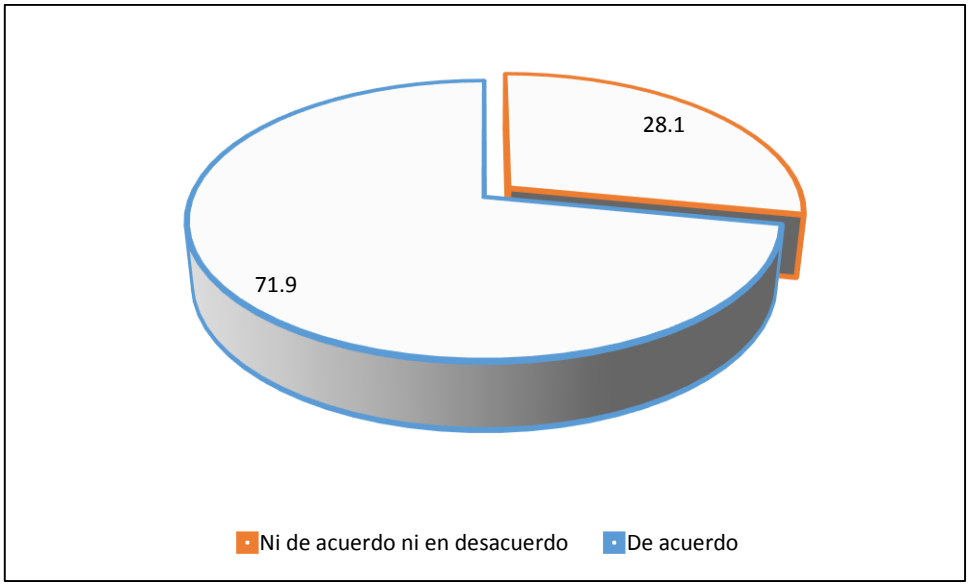
TABLA N° 36

La protección de datos personales permite ayudar en la prevención de los delitos informáticos

	Frecuencia	**%**
De acuerdo	41	71.9
Ni de acuerdo ni en desacuerdo	16	28.1
En desacuerdo	0	0
Total	57	100.0

GRÁFICO N° 19

La protección de datos personales permite ayudar
en la prevención de los delitos informáticos



En la Tabla N° 36 y el Gráfico N° 19 se presenta la opinión coherente y mayoritaria de los abogados fedatarios juramentados con especialización en informática, que piensan que la protección de datos personales, sí permite ayudar en la prevención de los delitos informáticos; en ese sentido los hallazgos indican que de un total de 57 (100%) personas, el 71.9% (41) están de acuerdo y el 28.1% (16) están ni de acuerdo ni en desacuerdo, siendo cero el resultado ante la alternativa de estar en desacuerdo.

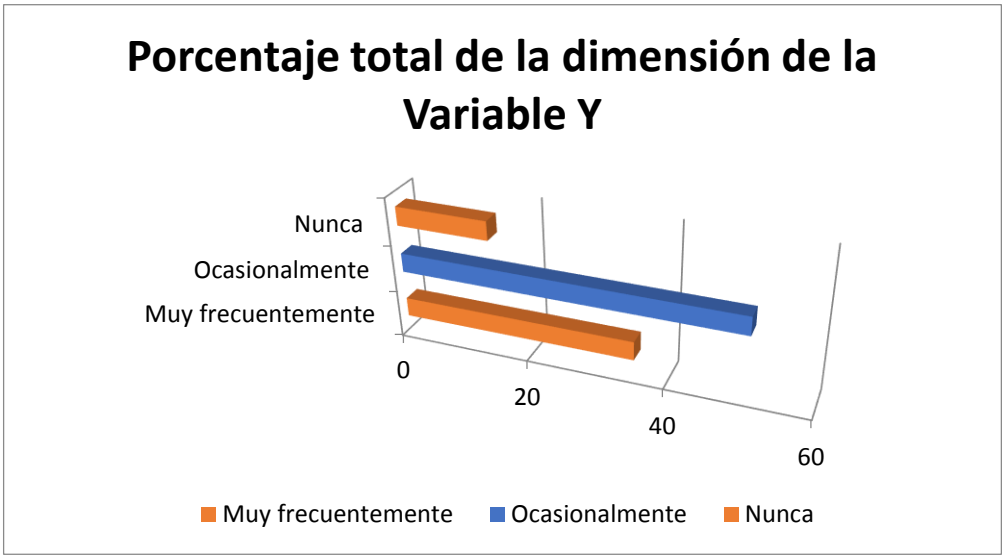
Consideramos conveniente como un aporte adicional, mencionar los indicadores de la variable dependiente (variable *Y*), cuya dimensión es "Los delitos informáticos previstos en la Ley N° 30096, modificada por la Ley N° 30171", lo cual nos permitirá diferenciar el porcentaje de influencia que tiene la Protección de Datos Personales, respecto de cada uno de los delitos informáticos previstos en las normas antes señaladas, para cuyo análisis utilizamos cinco indicadores, formulándose ocho preguntas en el instrumento de investigación, conforme presentamos en la tabla siguiente:

TABLA N° 37

DIMENSIÓN	**FRECUENCIA**			**TOTAL**
Delitos Informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171	**Muy Frecuen-temente**	**Ocasional-mente**	**Nunca**	
Indicador: Delitos contra los datos y sistemas informáticos. (Pregunta 12)	15.8% (9)	63.2% (36)	21.1% (12)	100% (57)
Indicador: Delitos contra los datos y sistemas informáticos. (Pregunta 13)	10.5% (6)	70.2% (40)	19.3% (11)	100% (57)
Indicador: Delitos contra los datos y sistemas informáticos. (Pregunta 14)	10.5% (6)	70.2% (40)	19.3% (11)	100% (57)
Indicador: Delitos contra la libertad e indemnidad sexual. (Pregunta 15)	71.9% (41)	26.3% (15)	1.8% (1)	100% (57)
Indicador: Delitos contra la intimidad y secreto de las comunicaciones. (Pregunta 16)	22.8% (13)	73.7% (42)	3.5% (2)	100% (57)
Indicador: Delitos contra el patrimonio. (Pregunta 17)	71.9% (41)	24.6% (14)	3.5% (2)	100% (57)
Indicador: Delitos contra la fe pública. (Pregunta 18)	63.2% (36)	35.1% (20)	1.8% (1)	100% (57)
Indicador: Delitos contra la fe pública. (Pregunta 19)	10.5% (6)	50.9% (29)	38.6% (22)	100% (57)
PROMEDIOS TOTALES	**35.1% (20)**	**50.9% (29)**	**14% (8)**	100% (57)

Respecto a la Dimensión "Delitos informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171", en los promedios totales de la tabla precedente, se aprecia que 35.1% (20) de los abogados sometidos al cuestionario de la encuesta, consideran que muy frecuentemente los ocho delitos informáticos previstos en las leyes antes mencionadas, se ven facilitados con el acceso a los datos personales de la víctima, 50.9% (29) consideran que ocasionalmente se ven facilitados y el 14% (8) piensan que los referidos delitos informáticos nunca se ven facilitados con el acceso a los datos personales de la víctima.

GRÁFICO N° 20



Interpretando esos resultados, apreciamos que el 35.1% de abogados fedatarios juramentados con especialización en informática, que consideran que los delitos informáticos si se ven facilitados con el acceso a los Datos Personales de la víctima, es superior al 14% que nunca considera que se vean facilitados.

En tal sentido, los datos estadísticos nos permiten colegir que, se ha confirmado la dimensión de la variable dependiente, encontrándose como los delitos informáticos más susceptibles de ser facilitados, el delito de Grooming (Proposiciones a niñas, niños y adolescentes con fines sexuales por medios tecnológicos), como lo considera 71.9% (41) de los especialistas a los que se aplicó el instrumento de investigación, el delito de Fraude Informático, que también tiene un 71.9% (41) que lo considera así, y el delito de Suplantación de Identidad, respecto al cual 63.2% (36) opinó que se facilitaba con el acceso indebido a los datos personales de la víctima.

CAPÍTULO VII: DISCUSIÓN DE RESULTADOS

La discusión de resultados de este capítulo, la vamos a desarrollar en base a los resultados obtenidos sobre nuestra hipótesis general e hipótesis específicas, contrastándolos con los planteamientos teóricos existentes sobre la materia, los cuales hemos explicado con mayor detalle en el marco teórico.

Nuestra Hipótesis General, relaciona causalmente a la Protección de Datos Personales (Ley N° 29733), con la delincuencia informática (Ley N° 30096), la misma que hemos verificado con la prueba estadística no paramétrica de chi–cuadrado, en la que se ha encontrado para la protección de datos y los delitos informáticos: $X^2_C = 4.676$, gl.= 1, p= $0.031 < 0.05$ siendo significativo se rechaza H_0 y se acepta H_1, es decir, se ha aceptado que la protección de datos personales, sí se relaciona en forma directa con la prevención de los delitos informáticos. Ello nos permite verificar coincidencias importantes con el planteamiento teórico, que nos muestra la importancia que se brinda a la protección de datos personales en la prevención de delitos informáticos en diferentes países, como lo hemos detallado en el marco teórico, por ejemplo, autoridad de protección de datos personales de un país próximo como Argentina, ha generado diversas actividades de prevención, dirigidas a todas las edades pero poniendo énfasis en los menores de edad, a los cuales se instruye que sepan proteger de personas extrañas sus datos personales, a fin

de que los mismos no sean utilizados en actos ilícitos e inclusive generando la comisión de delitos informáticos, en el que la víctima resulta ser la persona, el menor de edad muchas veces, que permitió el acceso innecesariamente de sus datos personales e incluso los de su círculo más íntimo como son sus datos sensibles.

Conforme a la teoría que hemos estudiado, hoy en día con la difusión de las redes sociales como Facebook, Twitter, LinkedIn, Instagram y otras, la variedad de chats que encuentran en el WhatsApp, el Messenger y el Skype a los que encabezan la lista, en los cuales la mayoría de los usuarios, público de todas las edades, usa estas herramientas virtuales todos los días sin mayor reparo de señalar su ubicación en el preciso momento en que se encuentra realizando alguna actividad, a través de alguna foto, un tweet o un comentario, sin percatarse que en realidad están compartiendo información personal que puede ser utilizada fácilmente por delincuentes informáticos, lo que se ha agravado con los múltiples aplicativos que utilizan la ubicación de nuestro celular y que están dando lugar a un creciente comercio electrónico móvil, en la cual se aceptan condiciones de privacidad sin mayor cuidado e ingresamos con facilidad nuestros datos personales.

Esto permite establecer que es necesario proteger al individuo, instruyéndolo para que sus datos no circulen o sean transmitidos indebidamente; sin embargo, como hemos determinado a lo largo de la investigación, son los propios titulares de los datos que en situaciones diversas los ponen en riesgo, porque existe un desconocimiento y desinterés por protegerlos (así opina 61.4% de los encuestados), actuando inconscientemente de los riesgos que acarrea el proporcionarlos y ponerlos en circulación por Internet sin mayor precaución, lo que da lugar a que se haga necesario que el Estado y las Instituciones Privadas en la materia, realicen campañas de prevención que lleguen a toda la población.

Lo señalado anteriormente se ha corroborado con la investigación, en la medida que se ha confirmado la hipótesis específica 1, ya que los titulares de los datos personales, los exponen relacionando directamente su uso indebido para la comisión de delitos informáticos, lo que ha sido verificado a través de la prueba estadística no paramétrica de chi–cuadrado, cuyos resultados para la hipótesis específica 1 fueron los siguientes: X^2_C =

5.961, gl.= 2, p= 0.031 < 0.05, lo que permite rechazar la Hipótesis Específica Nula 1 y aceptar la Hipótesis Específica Alterna 1.

Como apreciamos en el marco teórico, el titular de los datos los relaciona con su uso ilícito, al exponer sus datos innecesariamente, lo que permite la comisión de delitos informáticos, facilitando el accionar ilegal del ciberdelincuente. Si bien la percepción general apunta a que las redes sociales y otras actividades de entretenimiento, son el medio principal por el cual los titulares de los datos personales los exponen, eso no es tan cierto, ya que si comparamos nuestros resultados, se observa que un 49.1% (28) de los abogados a los que se aplicó el cuestionario, considera que la exposición de los datos por sus titulares a través de medios de entretenimiento es muy frecuente, facilitando su uso por delincuentes informáticos, pero es mayor el 68.4% (39), que considera que esa exposición de los datos se realiza muy frecuentemente por actividades de comercio electrónico, como son las compras por Internet.

Esto se puede explicar debido a que el público que realiza compras por Internet, está constituido por jóvenes y adultos, que cuentan con medios de pago como tarjeta de crédito; los cuales no tienen la misma formación que niños y adolescentes, que han crecido en un mundo digital y por lo tanto están estrechamente vinculados a las nuevas tecnologías de la información y la comunicación.

Es evidente, que la percepción general se ve influenciada por la cantidad de personas que usan redes sociales y chats, que es mucho mayor a los que compran por internet, a pesar del aumento significativo del comercio electrónico, durante los últimos 8 años en nuestro país, lo cual amerita por sí sólo un trabajo de investigación de pre o post grado.

En este análisis de los riesgos sobre el uso de los datos personales, hay que apreciar también que existe una mayor difusión sobre cómo manejar de forma segura redes sociales, chats, foros, videos, fotos, páginas web, emails, blogs, en relación a la difusión para realizar con seguridad compras por internet y en general todos los aspectos que tienen que ver con el comercio electrónico.

Lo señalado en los párrafos precedentes, son aspectos teóricos importantes que coinciden con el resultado de nuestra hipótesis específica 1, en la que se ha determinado que es el titular de los datos personales, quién los expone, relacionando directamente su uso ilícito en la comisión de delitos informáticos.

En virtud a ello, la teoría también nos permite apreciar que, a través del sistema de protección de datos personales que brinda la Ley Nº 29733, se plantean medidas de control para evitar que ese tipo de información privada, que debemos aprender a proteger, sea mezclada con bancos de datos accesibles a todo el público, lo que se ha corroborado en la hipótesis específica 2, cuyos resultados al ser sometidos a la prueba estadística no paramétrica de chi–cuadrado, son los siguientes: $X^2_C = 9.381$, gl.= 4, p= 0.022 < 0.05, con lo que se rechaza la Hipótesis Específica Nula 2 y se acepta la Hipótesis Específica Alterna 2, es decir, se acepta que la Ley de Protección de Datos Personales se relaciona con la prevención de los delitos informáticos en el Perú.

Del análisis dogmático de la Ley N° 29733 "Ley de Protección de Datos Personales", que hemos desarrollado en el marco teórico, concordado con lo señalado en el párrafo anterior, consideramos que el uso de los datos de las personas para la comisión de delitos informáticos, es posible prevenirlo si se toman algunos mecanismos de control, lo cual coincide con nuestra hipótesis específica 2, que la Ley de Protección de Datos Personales se relaciona con la prevención de delitos informáticos, como detallamos a continuación.

En principio, la referida Ley ofrece mecanismos de control con la propia aplicación de la normativa que tiene sobre Datos Personales, entre los que destacamos la implantación e implementación de un completo y eficiente Registro Nacional de los Bancos de Datos Personales (Así opinó 54.4% de los encuestados), y una regulación de las sanciones por las infracciones contempladas en la legislación de datos personales, cuyas multas pueden llegar hasta las 100 UITs, es decir S/. 415,000.00 en el año 2018, lo que previene la comisión de delitos informáticos (Así opinó 43.9% de los encuestados).

En este sentido, la teoría relativa a los medios de protección de los datos personales que ofrece nuestra ley, coincide con nuestros resultados empíricos, puesto que en efecto, la relación de la Ley de Protección de Datos Personales con la prevención de los delitos

informáticos, se presenta a través de los principales medios que ofrece para proteger los datos personales, como son el establecer un registro de los mismos e infracciones sancionables por incumplimiento a la Ley, quedando en segundo lugar el requerimiento obligatorio de que el consentimiento sea informado y expreso, así como las medidas de seguridad en el tratamiento de los datos personales, cuyo extremo fue prioritariamente considerado por los especialistas a los que se aplicó el instrumento de investigación, como un mecanismo que los protege ocasionalmente. (Así opinó 43.9% de los encuestados).

Adicionalmente, respecto a los mecanismos de control, debe enfatizarse su aplicación en la relación con los delitos de Grooming, Fraude Informático y Suplantación de Identidad, toda vez que tuvieron una importante mayoría dentro de los especialistas encuestados, que consideraron que se veían facilitados con el uso de los datos personales de las víctimas, un 71.9% (41) para los dos primeros delitos y 63.2% (36) para el tercero.

En ese sentido, las campañas de difusión para que las personas no expongan innecesariamente sus datos personales, deben realizarse principalmente en función a que estos pueden ser utilizados para la comisión de los tres delitos mencionados anteriormente. Hay que tener presente, que la víctima en el delito de Grooming, siempre será un menor de edad, es decir un niño o adolescente, lo cual es coherente con la teoría sobre la materia, que busca informar y crear conciencia prioritariamente en este público para que no entreguen o expongan sus datos personales, lo cual ayudará en el largo plazo a que se prevengan también los otros dos delitos, pues ese público de niños y adolescentes serán los mayores de edad del futuro; lo cual confirma una vez más nuestra hipótesis general, respecto a que la protección de datos personales se relaciona con la prevención de los delitos informáticos.

CONCLUSIONES

Las conclusiones, nos permiten responder las preguntas planteadas como problema general y problemas específicos del presente trabajo de investigación, por lo que la primera conclusión se refiere a la hipótesis general de la investigación, y las otras dos aluden a las hipótesis específicas 1 y 2, conforme enumeramos a continuación:

1. Como respuesta a nuestro problema general, hemos encontrado que la protección de datos personales, sí se relaciona en forma directa con la prevención de los delitos informáticos, toda vez que 71.9% (41) de las personas a las que se aplicó el instrumento de investigación, están de acuerdo con esa premisa, corroborado con la prueba estadística no paramétrica de chi cuadrado, cuyo resultado fue $X^2_C = 4.676$, gl.= 1, p= 0.031 < 0.05.

2. El titular de los datos personales, los expone relacionando directamente su uso indebido para la comisión de delitos informáticos, toda vez que 68.4% (39) de las personas a las que se aplicó el instrumento de investigación, considera que los pone en riesgo muy frecuentemente a través de actividades de comercio electrónico, como las compras por Internet, el 49.1% (28) considera que los expone a través de medios de entretenimiento, como el uso de redes sociales y chats, asimismo 61.4% (35) considera que los pone en riesgo por su desconocimiento y desinterés en protegerlos y 31.6% (18) debido al desconocimiento de que pueden ser utilizados con fines delictivos, hipótesis específica 1 que igualmentese ha corroborado con la prueba

estadística no paramétrica de chi cuadrado, cuyo resultado fue $X^2_C = 5.961$, gl.= 2, p= 0.031 < 0.05.

3. La Ley de Protección de Datos Personales, Ley N° 29733, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú, toda vez que 54.4% (31) consideran que el Registro Nacional de Bancos de Datos Personales, cumple muy frecuentemente con esa función, y 43.9% (25) piensa que el régimen de infracciones, clasificadas como leves, graves y muy graves que pueden ser sancionadas en este último caso, hasta con 100 UITs de multa (S/. 415,000.00 en el año 2018) muy frecuentemente sirve como medio de protección de los datos personales, hipótesis específica 2 que asimismo se ha corroborado con la prueba estadística no paramétrica de chi cuadrado, cuyo resultado fue $X^2_C = 9.381$, gl.= 4, p= 0.022 < 0.05.

RECOMENDACIONES

Las recomendaciones que planteamos, son producto de las conclusiones de nuestra investigación, conforme detallamos a continuación:

1. El tema de la Protección de Datos Personales, parte del Derecho Constitucional, adquiere mayor importancia al haberse establecido que sí se relaciona en forma directa con la prevención de los delitos informáticos; por lo que, las universidades peruanas a nivel nacional, deberían replantear su modelo de enseñanza, implementando como una asignatura de cultura general, en sus diferentes planes de estudio, el curso de Derecho Constitucional y Protección de Datos Personales, y adicionalmente en el Plan de Estudios de la Facultad de Derecho, dentro de los últimos ciclos de la carrera, la asignatura de especialidad "Derecho Informático", que incluya el estudio del derecho fundamental a la Protección de Datos Personales y de los Delitos Informáticos, entre otros aspectos como son el Comercio Electrónico y el Gobierno Electrónico, temas que no son estudiados en los cursos generales de Derecho Constitucional, Derecho Penal, Derecho Mercantil o Derecho Administrativo, o lo son muy superficialmente en el curso de Informática Jurídica.

2. Al haberse determinado que, el titular de los datos personales los expone, relacionando directamente su uso indebido para la comisión de delitos informáticos, las universidades peruanas deberían colaborar con la reducción de ese problema, implementando dentro de sus sistemas de evaluación, una nota o calificación referida a actividades de proyección social con la población, a fin de dar a conocer la importancia y los derechos que implica la protección de nuestros datos personales, y otra calificación de extensión universitaria, que permita difundir académicamente los temas relativos a la protección de datos personales y su relación con los delitos informáticos.

3. Habiéndose comprobado que en Perú, la Ley de Protección de Datos Personales (Ley N° 29733), sí se relaciona de manera directa con la prevención de los delitos informáticos, al proveer diferentes medios de protección de los datos personales; las escuelas de posgrado de las universidades peruanas, deberían promover el desarrollo de investigaciones jurídicas, relacionadas con el derecho fundamental a la Protección de Datos Personales o los delitos informáticos, a través de concursos de investigación con becas de estudio como premios, a fin de ampliar su conocimiento doctrinario y legislativo, así como incentivar al estudio más específico, de los diversos problemas que se pueden deducir a partir del estudio general de la presente tesis.

FUENTES DE INFORMACIÓN

I. BIBLIOGRAFÍA

1. ALTMARK, D. y MOLINA, E. (2012) *Tratado de Derecho Informático*. Buenos Aires, Argentina: Editorial la Ley. Tres Tomos.
2. ALZAMORA DE LOS GODOS, L., CALDERÓN, J. y DEL AGUILA, E. (2009) *Guía de Elaboración de Proyectos de Tesis Doctoral.* Lima: Universidad Alas Peruanas – Vicerrectorado de Investigación y Postgrado.
3. BEHAR; D. (2008) *Introducción a la Metodología de la Investigación Científica.* Lima: Editorial Shalom.
4. BLOSSIERS, J. (2003) *Derecho Informático: Contratación Civil & Comercial*. Lima: Editorial Portocarrero.
5. BLOSSIERS, J. (2003) *Informática Jurídica*. Lima: Editorial Portocarrero.
6. CARRASCO, L. (2008) El Hábeas Data frente a los abusos del poder informático. Lima: Industria Gráfica Libertad.
7. DAVARA, M. (1993) *Derecho Informático*. Madrid - España: Editorial Aranzandi.
8. GAVAGNIN TAFFAREL, Osvaldo. (2009). *La Creación del Conocimiento. Plan y Elaboración de una Tesis de Post Grado.* Lima: Editorial Unión.

9. HERNÁNDEZ, R. (2014) *Metodología de la Investigación.* México: Editorial McGraw-Hill/Interamericana Editores. Sexta Edición.
10. IRIARTE, E. (2013) *Derecho informático.* Lima - Perú: Editorial de la Academia de la Magistratura.
11. LLAMBÍAS, M. (2008) *Informática Jurídica*. Lima: Ediciones Jurídicas.
12. NÚÑEZ, J. (1996) *Derecho informático: nueva disciplina jurídica para una sociedad moderna.* Lima - Perú: Editorial Marsol.
13. OSSORIO, M. (1974). *Diccionario de Ciencias Jurídicas, Políticas y Sociales de Manuel Ossorio*. Buenos Aires, Argentina: Heliasta.
14. PEÑA-CABRERA, A. (2007). *Delitos contra la libertad e intangibilidad sexual.* Lima - Perú: Editorial Idemsa.
15. PÉREZ, A. (1996) *Manual de informática y derecho*. Argentina: Editorial Ariel.
16. QUERALT, J. (1996) *Derecho Penal Español*. *Parte Especial.* Madrid - España.
17. RAMOS, C. (2007). *Cómo hacer una tesis de derecho y no envejecer en el intento.* Lima: Gaceta Jurídica, 4ta edición revisada y aumentada.
18. TELLEZ, J. (2009) *Derecho Informático*. México: Editorial McGraw-Hill. Cuarta Edición.
19. TIEDEMANN, K. (1986) *Criminalidad mediante Computadoras*. España: Editorial Ariel S.A.

II. WEBGRAFÍA

1. ABOGADOS PORTALEY (2007) *Protección de los menores en su utilización de Internet.* En Revista Delitos Informáticos.com. Disponible en: https://delitosinformaticos.com/02/2007/ciberderechos/proteccion-de-los-menores-en-su-utilizacion-de-internet
2. ACADEMIA DE LA MAGISTRATURA - AMAG (2000) *Temas de Derecho Penal Especial. Cap III.* Lima – Perú. Disponible en: http://sistemas.amag.edu.pe/publicaciones/dere_pen_proce_penal/tema_dere_pen_espe/capituloIII.pdf

3. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018) *Internet y Redes Sociales*. Disponible en: https://www.aepd.es/areas/internet/index.html
4. ALEGSA. L (1998-2017) *Diccionario de Informática y Tecnología.* Argentina. Disponible en: http://www.alegsa.com.ar/Dic/i.htm
5. CASTRO, K. (2008) *El Derecho Fundamental a la Protección de Datos Personales: Aportes para su Desarrollo en el Perú.* Publicado en Revista Ius Et Veritas N° 37. Lima – Perú. Disponible en:

   http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12229

5. CENTRO DE INTEGRACIÓN CIUDADANA (S/F) *11 recomendaciones para protegerte de los delitos cibernéticos.* México. Disponible en: http://www.cic.mx/11-recomendaciones-para-protegerte-de-los-delitos-ciberneticos/
6. CEPAL (2003) *Los caminos hacia una Sociedad de la Información en América Latina y el Caribe*. Disponible en:

   http://www.eclac.org/publicaciones/xml/9/12899/lcg2195e2.pdf

7. CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN (2003-2005) *Resolución N° 56/183.* Suiza – Túnez. Disponible en:

   http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002-es.pdf

8. DIVINDAT (2012). *Policía Informática del Perú*. Lima - Perú: Disponible en: http://www.4law.co.il/peru1.htm
9. DIVISION COMPUTER FORENSIC (2015) *Delitos Informáticos. Glosario*. España. Disponible en:
   http://www.delitosinformaticos.info/delitos_informaticos/glosario.html
10. EL UNIVERSAL (2015) *¿Cómo protegerse de los delitos informáticos?*. Colombia. Disponible en: http://www.eluniversal.com.co/tecnologia/como-protegerse-de-los-delitos-informaticos-201859
11. ENCICLOPEDIA DE CONCEPTOS (2018) *Misión y Visión*. Disponible en: https://concepto.de/mision-y-vision/

12. ESLAVA, P. (2016) *Tesis "El Principio Constitucional de la Resocialización de los Penados en la Era del Internet: Entre el Tratamiento de Datos Personales y el Derecho al Olvido, a propósito de la Sentencia C-131/12 del Tribunal de Luxemburgo"*. Trujillo – Perú. Disponible en: http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/5864/EslavaMorales_P.pdf?sequence=1

13. FIGARI, R. (S/F) *Código Penal comentado de acceso libre – Delitos Contra la Fe Pública.* Argentina. Disponible en: http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc40205.pdf

14. GACITÚA, A. (2014) *Tesis "El Derecho Fundamental a la Protección de Datos Personales en el Ámbito de la Prevención y Represión Penal Europea"*. Barcelona – España. Disponible en: https://ddd.uab.cat/pub/tesis/2014/hdl_10803_284352/alge1de1.pdf

15. GARCÍA, A. (2007) *Artículo "La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un estudio comparado",* publicado en el N° 120 del Boletín Mexicano de Derecho Comparado - UNAM. México. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4972

16. GARCÍA, N. (2014) *Tesis "Victimización de Menores por Actos de Ciberacoso y Actividades Cotidianas en el Ciberespacio"*. España. Disponible en: https://digitum.um.es/xmlui/bitstream/10201/40868/1/Tesis%20Natalia_Garcia_Guilabert_Victimizaci%C3%B3n%20de%20menores%20por%20ciberacoso%20continuado.pdf

17. GHIRARDOTTI, I. (2007) *Sociedad de la Información. Concepto y Características.* Disponible en: http://inesghirardotti.blogspot.pe/2007/09/concepto-y-caracteristicas.html

18. GUZMÁN, M. (2013) *Tesis "El Derecho Fundamental a la Protección de Datos Personales en México: Análisis desde la Influencia del Ordenamiento Jurídico Español"*. España. Disponible en: http://eprints.ucm.es/22817/1/T34727.pdf

19. LA ROSA, G. (2002) *Tesis "Los Desafíos Jurídicos frente a las Nuevas Tecnologías de la Información y Comunicación: El Caso de la Firma Digital".* Lima - Perú.

Disponible en: http://www.ac-firma.com/biblioteca/opac_css/index.php?lvl=author_see&id=1842

20. LESTLAW (2017) *Delitos Informáticos. Difusión de Datos Personales y/o Familiares.* España. Disponible en: https://letslaw.es/delitos-informaticos-difusion-datos-personales-familiares/
21. MEJÍA, I. (2010) *Tesis "La Globalización en el Desarrollo de una Cultura de Protección de los Derechos Humanos y su Influencia en el Perú"*. Lima. Disponible en: http://cybertesis.unmsm.edu.pe/bitstream/cybertesis/195/1/Mejia_vi.pdf
22. MEZZASALMA, M. y PÉREZ, N. (2001) *Delitos Informáticos: Cuestiones Dogmáticas y Desafíos Político Criminales de la Modernidad Tardía*. España. Disponible en: http://www.derechoareplica.org/index.php/control-social/119-delitos-informaticos-cuestiones
23. MINISTERIO DE JUSTICIA (2014-2017) *Dirección General de Protección de Datos Personales del Perú*. Lima - Perú: Disponible en: http://www.minjus.gob.pe/proteccion-de-datos-personales/
24. MORALES, D. (2016) *Tesis "La Inseguridad al Utilizar los Servicios de Redes Sociales y la Problemática Judicial para Regular los Delitos Informáticos en el Perú"*. Pimentel, Lambayeque – Perú. Disponible en: http://repositorio.uss.edu.pe/bitstream/uss/3161/6/MORALES_DELGADO_DEIVID_1%20YULY-1.%20turnitin.pdf
25. NARANJO, R. (2013). *Manual de Derecho Constitucional*. En Derecho en Red. España. Disponible en: http://www.derechoconstitucional.es/2013/03/derecho-al-secreto-de-las-comunicaciones.html
26. NIETO, P. (2007) *La Sociedad de la Información*. En Alfa-Redi Revista de Derecho Informático N° 106. Lima - Perú: Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=9220
27. NÚÑEZ, J. (2016) *Tesis "Derecho de Identidad Digital en Internet".* Lima - Perú. Universidad Nacional Mayor de San Marcos. Disponible en: http://cybertesis.unmsm.edu.pe/bitstream/cybertesis/6252/2/Nunez_pj.pdf

28. ONGEI (2017) *Normas Legales sobre Derecho Informático*. Lima – Perú. Disponible en: http://www.ongei.gob.pe/normas/

29. ORGANIZACIÓN DE LAS NACIONES UNIDAS (2010) *Objetivos del Desarrollo del Milenio Informe 2010*. EUA, Código del Informe A/64/665. Disponible en: http://www.un.org/es/comun/docs/?symbol=A/64/665

30. PALOMINO, W. (2014). *El Intrusismo y los otros Delitos Informáticos regulados en la Ley N° 30096*. En Boletín N° 42 Oré Guardia. Lima – Perú. Disponible en: http://www.oreguardia.com.pe/media/uploads/BOLET%C3%8DN-ACAD%C3%89MICO-N%C2%B0-42.pdf

31. PASCUAL, P. (2017). *Tesis: "La Génesis del Derecho Fundamental a la Protección de Datos Personales"*. España. Disponible en: http://eprints.ucm.es/43050/1/T38862.pdf

32. PEÑA, D. (2014). *Aproximación criminógena: delitos informáticos contra la indemnidad y libertades sexuales Ley Nº 30096*. Disponible en: https://www.uigv.edu.pe/fileadmin/facultades/derecho/Archivos/ARTICULOS_DOCENTES/ARTICULO_DELITOS_INFORMATICOS_INDEMNIDAD_SEXUAL_2014.pdf

33. PROTECCIÓN ONLINE.COM (S/F) *10 Consejos para evitar ser engañados en redes sociales como Facebook.* Gobierno de Argentina. Disponible en: http://www.protecciononline.com/10-consejos-para-evitar-ser-enganados-en-redes-sociales-como-facebook/

34. QUIROGA, A. (2013) *Los principios de finalidad y proporcionalidad.* En Oficio N° 262-2013-JUS/DGPDP del 22 de agosto de 2013 absolviendo la consulta sobre la materia. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2014/07/3.-Principios-de-finalidad-y-proporcionalidad.pdf

35. QUIROGA, A. (2013) *El consentimiento para el tratamiento de datos sensibles*. En Oficio N° 950-2013-JUS/DGPDP del 26 de diciembre de 2013, firmado por el Dr. José Alvaro Quiroga León, Director General de Protección de Datos Personales, absolviendo la consulta sobre la materia. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2014/07/7.-Consentimiento-para-el-tratamiento-de-datos-sensibles.pdf

36. RUEDA, M. (2009). *Los Ataques Contra los Sistemas Informáticos: Conductas de Hacking. Cuestiones Político-Criminales*. Publicado en Revista Jurídica Online de la Universidad Católica de Santiago de Guayaquil. Ecuador. Disponible en: http://www.revistajuridicaonline.com/2009/09/los-ataques-contra-los-sistemas-informaticos-conducta-de-hacking-cuestiones-politico-criminales/

37. SALTOR, C. (2013) *Tesis "La Protección de Datos Personales: Estudio Comparativo Europa - América con especial análisis de la Situación Argentina".* España. Disponible en: http://eprints.ucm.es/22832/1/T34731.pdf

38. TRIBUNAL CONSTITUCIONAL (2003). *Sentencia N° 1797-2002-HD/TC*. Perú. Disponible en: http://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

39. VILLAVICENCIO, F. (2014) *Delitos Informáticos*. En Revista ius et veritas. Volumen 49. P. 285-292. Lima – Perú. Disponible en: http://bit.ly/1QoSc75

ANEXOS:

1. MATRIZ DE CONSISTENCIA
2. INSTRUMENTO DE RECOLECCIÓN DE DATOS ORGANIZADO EN VARIABLES, DIMENSIONES E INDICADORES
3. VALIDACIÓN DE EXPERTOS
4. TABLA DE LA PRUEBA DE VALIDACIÓN
5. BASE DE DATOS DE LA DATA PROCESADA
6. CONSENTIMIENTO INFORMADO
7. AUTORIZACIÓN DE LA ENTIDAD DONDE SE REALIZÓ EL TRABAJO DE CAMPO
8. DECLARATORIA DE AUTENTICIDAD DEL INFORME DE TESIS

ANEXO 1

MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS GENERAL	VARIABLES	METODO-LOGÍA
¿Cómo la Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú?	Determinar si la Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú.	La Protección de Datos Personales, sí se relaciona en forma directa con la prevención de los delitos informáticos en el Perú.	**Variable X:** Protección de Datos Personales **Dimensiones Variable X:** 1. El titular de los datos personales. 2. La Ley de Protección de Datos Personales. **Variable Y:** Delitos Informáticos. **Dimensiones Variable Y:** 1. Delitos Informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171.	**Tipo de Investigación:** Básica – Transversal **Nivel de la Investigación:** Explicativo. **Método:** Deductivo – Inductivo – Dogmático **Diseño de la Investigación:** No experimental – Tranversal – Causal **Población y Muestra:** La población es de 135 abogados Fedatarios Juramentados con Especialización en Informática, aplicando la fórmula la muestra equivale a 57 Fedatarios. **Recolección de Datos** Como Técnica se ha utilizado la Encuesta y el Instrumento ha sido el Cuestionario.
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPOTESIS ESPECÍFICAS**		
a) ¿Cómo el titular de los datos personales, relaciona su uso indebido para la comisión de delitos informáticos? b) ¿Cómo la Ley de Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú?	a) Determinar si el titular de los datos personales, relaciona su uso indebido para la comisión de delitos informáticos. b) Establecer si la Ley de Protección de Datos Personales, se relaciona con la prevención de los delitos informáticos en el Perú.	a) El titular de los datos personales, sí los expone relacionando directamente su uso indebido para la comisión de delitos informáticos. b) La Ley de Protección de Datos Personales, sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú.		

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS ORGANIZADO EN VARIABLES, DIMENSIONES E INDICADORES

CUESTIONARIO DE ENCUESTA

INSTRUCCIONES: LEA CON DETENIMIENTO CADA PREGUNTA Y MARQUE CON UN ASPA UNA SOLA RESPUESTA

NOTA: El presente Cuestionario de Encuesta es un instrumento de Recolección de Datos de la Tesis para optar el grado de Doctor en Derecho, titulada "La Protección de Datos Personales como medio de Prevención de los Delitos Informáticos en el Perú, en los años 2017 y 2018".

PREGUNTAS DE FILTRO (No pertenecen a ninguna variable ni dimensión)

1. **¿La Ley Nº 29733 "Ley de Protección de Datos Personales", tiene como objetivo?**
   a. Garantizar el derecho fundamental previsto en el Art. 2 Inc. 6 de la Constitución.
   b. Garantizar el derecho fundamental previsto en el Art. 2 Inc. 7 de la Constitución.
   c. Reducir la posibilidad de que se cometan delitos informáticos.

11. **Se requiere promulgar en el Perú las nuevas leyes de Delitos Informáticos y de Protección de Datos Personales.**

    a. De acuerdo.
    b. En desacuerdo.
    c. Ni de acuerdo ni en desacuerdo.

20. **La Ley N° 30096 "Ley de Delitos Informáticos", modificada con la Ley N° 30171, tipifica todos los delitos informáticos que se pueden dar en el Perú.**

    a. Sí.
    b. No.
    c. En parte, porque existen otros delitos tipificados en el Código Penal que también se realizan a través de medios informáticos.

PREGUNTA DE CONTROL (Sirve en este caso, para verificar la información de todas las preguntas de contenido)

2. **La protección de datos personales permite ayudar en la prevención de los delitos informáticos.**

   a. De acuerdo.
   b. En desacuerdo.
   c. Ni de acuerdo ni en desacuerdo.

PREGUNTAS DE CONTENIDO (Son las planteadas de acuerdo a las variables, dimensiones e indicadores)

VARIABLE INDEPENDIENTE: PROTECCIÓN DE DATOS PERSONALES

DIMENSIÓN 1: Titular de los datos personales.

INDICADOR 1: Medios de Exposición de Datos

3. El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en actividades de entretenimiento, como son juegos on line, redes sociales, chats y otros medios de entretenimiento.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

7. El titular de los datos personales expone sus datos y los pone en riesgo facilitando su uso por delincuentes informáticos, utilizándolos en compras y ofertas de bienes y servicios por Internet y actividades de comercio electrónico en general.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

INDICADOR 2: Razones de Exposición de Datos.

4. El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento de que pueden ser utilizados por delincuentes informáticos.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

5. El titular de los datos personales expone sus datos y los pone en riesgo facilitando la comisión de delitos informáticos, por su desconocimiento y desinterés en proteger sus Datos Personales.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

DIMENSIÓN 2: Ley de Protección de Datos Personales

INDICADOR 3: Consentimiento

6. La aplicación estricta del principio de consentimiento y la observancia de sus requisitos de libre, previo, expreso e inequívoco, y en el caso de los datos sensibles que sea por escrito, implica que se prevendrá la comisión de delitos informáticos.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

INDICADOR 4: Registro de Bancos de Datos

8. La inscripción obligatoria de los Bancos de Datos Personales en el registro nacional, es una medida que ayudará a la prevención de los delitos informáticos.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

INDICADOR 5: Tratamiento de Datos Personales

9. Las medidas de seguridad para el tratamiento de los datos personales, garantizan que estos no sean accesibles a delincuentes informáticos.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

INDICADOR 6: Infracciones y Sanciones

10. Las infracciones y sanciones que prevén las normas sobre protección de datos personales, garantizan que estos no sean utilizados de manera ilegal facilitando su acceso a delincuentes informáticos.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

VARIABLE DEPENDIENTE: DELITOS INFORMÁTICOS

DIMENSIÓN: Delitos Informáticos previstos en la Ley N° 30096 modificada por la Ley N° 30171

INDICADOR 7: Delitos contra los Datos y Sistemas Informáticos

12. El delito de "Acceso Ilícito a un Sistema Informático" se ve facilitado con el acceso a los datos personales de la víctima.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

13. El delito de "Atentado contra la Integridad de Sistemas Informáticos" se ve facilitado con el acceso a los datos personales de la víctima.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

14. El delito de "Atentado contra la Integridad de Datos Informáticos" se ve facilitado con el acceso a los datos personales de la víctima.

a. Muy frecuentemente.
b. Ocasionalmente.
c. Nunca.

INDICADOR 8: Delitos contra la Libertad e Indemnidad Sexual

15. **El delito de "Grooming" (Proposiciones a Niños, Niñas y Adolescentes con Fines Sexuales por Medios Tecnológicos) se ve facilitado con el acceso a los datos personales de la víctima.**
    a. Muy frecuentemente.
    b. Ocasionalmente.
    c. Nunca.

INDICADOR 9: Delitos contra la Intimidad y el Secreto de las Comunicaciones

16. **El delito de "Interceptación de datos informáticos" se ve facilitado con el acceso a los datos personales de la víctima.**
    a. Muy frecuentemente.
    b. Ocasionalmente.
    c. Nunca.

INDICADOR 10: Delitos contra el Patrimonio

17. **El delito de "Fraude Informático" se ve facilitado con el acceso a los datos personales de la víctima.**
    a. Muy frecuentemente.
    b. Ocasionalmente.
    c. Nunca.

INDICADOR 11: Delitos contra la Fe Pública

18. **El delito de "Suplantación de identidad mediante las TIC", se ve facilitado con el acceso a los datos personales de la víctima.**
    a. Muy frecuentemente.
    b. Ocasionalmente.
    c. Nunca.

19. **El delito de "Abuso de mecanismos y dispositivos Informáticos" se ve facilitado con el acceso a los datos personales de la víctima.**
    a. Muy frecuentemente.
    b. Ocasionalmente.
    c. Nunca.

ANEXO 3

VALIDACIÓN DE EXPERTOS

VICERRECTORADO DE INVESTIGACIÓN
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 **Apellidos y nombres del experto:** RODRIGUEZ ULLOA José Antonio
1.2 **Grado Académico:** Doctor en Derecho
1.3 **Cargo e institución donde labora:** Docente Universitario en la Universidad Alas Peruanas y Juez Militar de Tránsito – Ejército del Perú
1.4 **Título de la Investigación:** "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú"
1.5 **Autor del instrumento:** Mg. Fernando Martín Robles Sotomayor
1.6 **Maestría/Doctorado/Mención:** Doctorado.
1.7 **Nombre del Instrumento:** Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		0-20%	21-40%	41-60%	61-80%	81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Está expresado en conductas observables.					
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					
4. ORGANIZACIÓN	Existe una organización lógica.					
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
6. INTENCIONA-LIDAD	Adecuado para valorar aspectos del estudio.					
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					
9. METODOLOGÍA	La estrategia responde al proceso del estudio.					
10.CONVENIENCIA	Genera nuevas, pautas en la investigación y construcción de teorías.					
SUB TOTAL						
TOTAL						

VALORACION CUANTITATIVA (Total x 0.20): ……

VALORACION CUALITATIVA: ……

OPINIÓN DE APLICABILIDAD: ……

LUGAR Y FECHA:……

……..……..……..
Firma y Posfirma del Experto

DNI ……..……...

VICERRECTORADO DE INVESTIGACIÓN
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 **Apellidos y nombres del experto:** MUÑOZ PANTIGOSO Wander Saúl
1.2 **Grado Académico:** Doctor en Derecho
1.3 **Cargo e institución donde labora:** Docente Universitario en la Universidad Alas Peruanas y Asesor Legal en la Procuraduría Pública del Ejército del Perú
1.4 **Título de la Investigación:** "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú"
1.5 **Autor del instrumento:** Mg. Fernando Martín Robles Sotomayor
1.6 **Maestría/Doctorado/Mención:** Doctorado.
1.7 **Nombre del Instrumento:** Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		0-20%	21-40%	41-60%	61-80%	81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Está expresado en conductas observables.					
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					
4. ORGANIZACIÓN	Existe una organización lógica.					
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
6. INTENCIONA-LIDAD	Adecuado para valorar aspectos del estudio.					
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					
9. METODOLOGÍA	La estrategia responde al proceso del estudio.					
10.CONVENIENCIA	Genera nuevas, pautas en la investigación y construcción de teorías.					
SUB TOTAL						
TOTAL						

VALORACION CUANTITATIVA (Total x 0.20): ……

VALORACION CUALITATIVA: ……

OPINIÓN DE APLICABILIDAD: ……

LUGAR Y FECHA:……

……..……..……..
Firma y Posfirma del Experto
DNI ……..……...

VICERRECTORADO DE INVESTIGACIÓN
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 **Apellidos y nombres del experto:** PACHECO MONTES Kennedy Peter
1.2 **Grado Académico:** Doctor en Derecho
1.3 **Cargo e institución donde labora:** Vocal Superior del Tribunal Superior Militar Policial del Oriente – Fuero Militar Policial
1.4 **Título de la Investigación:** "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú"
1.5 **Autor del instrumento:** Mg. Fernando Martín Robles Sotomayor
1.6 **Maestría/Doctorado/Mención:** Doctorado.
1.7 **Nombre del Instrumento:** Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		0-20%	21-40%	41-60%	61-80%	81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Está expresado en conductas observables.					
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					
4. ORGANIZACIÓN	Existe una organización lógica.					
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
6. INTENCIONA-LIDAD	Adecuado para valorar aspectos del estudio.					
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					
9. METODOLOGÍA	La estrategia responde al proceso del estudio.					
10.CONVENIENCIA	Genera nuevas, pautas en la investigación y construcción de teorías.					
SUB TOTAL						
TOTAL						

VALORACION CUANTITATIVA (Total x 0.20): ……

VALORACION CUALITATIVA: ……

OPINIÓN DE APLICABILIDAD: ……

LUGAR Y FECHA:……

……..……..……..
Firma y Posfirma del Experto
DNI ……..……...

VICERRECTORADO DE INVESTIGACIÓN
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 **Apellidos y nombres del experto:** VILLARREAL BALBIN Vladimir
1.2 **Grado Académico:** Doctor en Derecho
1.3 **Cargo e institución donde labora:** Fiscal de Familia en Loreto y Docente Universitario
1.4 **Título de la Investigación:** "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú"
1.5 **Autor del instrumento:** Mg. Fernando Martín Robles Sotomayor
1.6 **Maestría/Doctorado/Mención:** Doctorado.
1.7 **Nombre del Instrumento:** Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		0-20%	21-40%	41-60%	61-80%	81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Está expresado en conductas observables.					
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					
4. ORGANIZACIÓN	Existe una organización lógica.					
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
6. INTENCIONA-LIDAD	Adecuado para valorar aspectos del estudio.					
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					
9. METODOLOGÍA	La estrategia responde al proceso del estudio.					
10.CONVENIENCIA	Genera nuevas, pautas en la investigación y construcción de teorías.					
SUB TOTAL						
TOTAL						

VALORACION CUANTITATIVA (Total x 0.20): ……

VALORACION CUALITATIVA: ……

OPINIÓN DE APLICABILIDAD: ……

LUGAR Y FECHA:……

……..……..……..
Firma y Posfirma del Experto

DNI ……..……...

VICERRECTORADO DE INVESTIGACIÓN
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 **Apellidos y nombres del experto:** CABRERA PAREDES Roger
1.2 **Grado Académico:** Doctor en Derecho
1.3 **Cargo e institución donde labora:** Docente Universitario y Decano de la Facultad de Derecho de la Universidad Científica del Perú
1.4 **Título de la Investigación:** "La Protección de Datos Personales como Medio de Prevención de los Delitos Informáticos en el Perú"
1.5 **Autor del instrumento:** Mg. Fernando Martín Robles Sotomayor
1.6 **Maestría/Doctorado/Mención:** Doctorado.
1.7 **Nombre del Instrumento:** Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		0-20%	21-40%	41-60%	61-80%	81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Está expresado en conductas observables.					
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					
4. ORGANIZACIÓN	Existe una organización lógica.					
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
6. INTENCIONA-LIDAD	Adecuado para valorar aspectos del estudio.					
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					
9. METODOLOGÍA	La estrategia responde al proceso del estudio.					
10.CONVENIENCIA	Genera nuevas, pautas en la investigación y construcción de teorías.					
SUB TOTAL						
TOTAL						

VALORACION CUANTITATIVA (Total x 0.20): ……

VALORACION CUALITATIVA: ……

OPINIÓN DE APLICABILIDAD: ……

LUGAR Y FECHA:……

……..……..……..
Firma y Posfirma del Experto

DNI ……..……...

ANEXO 4

TABLA DE LA PRUEBA DE VALIDACIÓN

Utilizando la prueba V de Aiken, con el coeficiente siguiente:

$V = \frac{S}{(n(c.1))}$. $1.00 = \frac{25}{(5(5x1))}$. $0.96 = \frac{24}{(5(5x1))}$. $0.92 = \frac{23}{(5(5x1))}$.

S: Sumatoria de si
s_1: Valor asignado por el experto
n: Número de expertos
c: Número de valores en la escala de valoración

ITEM	EXPER-TO 1	EXPER-TO 2	EXPER-TO 3	EXPER-TO 4	EXPER-TO 5	ACUERDO	V DE AIKEN	DESCRIP-TIVO
CLARIDAD	**5**	**5**	**5**	**5**	**5**	**25**	**1.00**	Válido
OBJETIVIDAD	**5**	**4**	**4**	**5**	**5**	**23**	**0.92**	Válido
ACTUALIDAD	**5**	**4**	**5**	**5**	**5**	**24**	**0.96**	Válido
ORGANI-ZACIÓN	**5**	**4**	**5**	**4**	**5**	**23**	**0.92**	Válido
SUFICIENCIA	**5**	**5**	**5**	**5**	**5**	**25**	**1.00**	Válido
INTENCIO-NALIDAD	**4**	**5**	**5**	**5**	**5**	**24**	**0.96**	Válido
CONSIS-TENCIA	**5**	**5**	**5**	**5**	**5**	**25**	**1.00**	Válido
COHERENCIA	**5**	**4**	**5**	**5**	**4**	**23**	**0.92**	Válido
METODO-LOGÍA	**5**	**5**	**5**	**5**	**5**	**25**	**1.00**	Válido
CONVE-NIENCIA	**5**	**5**	**4**	**5**	**5**	**24**	**0.96**	Válido

Experto 1: Dr. José Antonio Rodríguez Ulloa

Experto 2: Dr. Wander Saúl Muñoz Pantigoso

Experto 3: Dr. Kennedy Peter Pacheco Montes

Experto 4: Dr. Vladymir Villarreal Balbín

Experto 5: Dr. Roger Cabrera Paredes

ANEXO 5

BASE DE DATOS DE LA DATA PROCESADA

Base de datos de la data procesada obtenida del instrumento de investigación

Variable x: Proteccion de los datos personales

ENC.	PREG 2	PREG 3	PREG 4	PREG 5	PREG 6	PREG 7	PREG 8	PREG 9	PREG 10
1	3	3	2	2	2	2	3	1	2
2	3	2	2	3	2	2	3	1	2
3	2	2	2	3	2	2	3	1	3
4	2	3	3	3	3	3	3	1	3
5	3	3	3	3	3	3	3	3	3
6	3	3	2	3	2	3	3	1	3
7	2	3	2	3	2	3	3	3	2
8	3	2	3	2	3	2	3	3	3
9	3	1	3	2	3	3	3	3	3
10	3	3	2	2	3	3	2	3	3
11	3	3	2	3	2	3	2	3	3
12	3	3	3	3	2	3	3	3	3
13	3	1	3	3	2	2	3	3	3
14	3	2	3	3	2	2	3	1	2
15	3	2	2	1	2	2	3	2	2
16	3	2	2	2	3	3	2	2	3
17	2	2	2	2	1	2	2	1	1
18	2	2	2	2	2	2	2	2	2
19	3	3	2	2	2	3	2	2	2
20	3	3	3	2	2	3	3	2	2
21	3	3	3	3	2	3	3	1	3
22	3	2	3	3	2	3	3	2	3
23	3	3	2	3	2	3	2	2	3
24	3	1	2	2	2	2	2	2	3
25	2	2	2	2	1	2	1	1	1
26	3	3	2	3	2	2	2	1	1
27	3	3	2	3	2	2	2	2	1
28	3	3	2	2	2	3	2	2	3
29	3	3	3	3	2	3	2	3	3
30	3	3	2	3	2	3	2	2	3
31	2	3	2	3	1	3	3	2	1
32	3	3	2	3	2	3	3	2	2
33	3	2	2	3	2	3	3	2	2
34	3	2	3	2	2	3	3	2	1
35	2	2	3	2	2	3	2	2	2
36	2	2	2	3	2	3	2	2	2
37	2	2	2	2	2	2	2	2	2
38	2	3	2	2	2	2	2	3	2
39	2	3	2	3	2	2	3	3	2
40	2	3	2	1	1	2	2	3	2

ENC.	PREG 2	PREG 3	PREG 4	PREG 5	PREG 6	PREG 7	PREG 8	PREG 9	PREG 10
41	3	3	2	3	2	2	3	3	2
42	3	3	3	3	2	3	3	3	2
43	3	2	2	3	1	3	3	2	2
44	3	2	1	3	2	3	3	2	3
45	3	3	1	3	2	3	3	3	3
46	3	2	1	3	2	3	2	3	3
47	2	2	2	3	2	3	2	1	3
48	2	2	3	3	1	3	2	1	2
49	2	2	2	3	1	3	2	1	1
50	3	2	3	3	3	3	2	3	2
51	3	3	3	3	3	3	2	3	3
52	3	3	3	2	3	3	3	3	3
53	3	3	2	2	3	3	3	2	3
54	3	2	2	2	2	3	3	2	2
55	3	1	1	2	2	3	3	2	2
56	3	1	2	3	3	3	3	2	1
57	3	2	2	3	3	3	2	2	2

Base de datos de la data procesada obtenida del instrumento de investigación

Variable y: Delitos Informáticos

ENC.	PREG 12	PREG 13	PREG 14	PREG 15	PREG 16	PREG 17	PREG 18	PREG 19
1	2	2	2	3	2	3	3	1
2	1	2	2	3	2	3	3	2
3	1	1	1	3	2	3	2	2
4	2	2	2	3	2	3	3	2
5	2	2	2	2	2	3	3	2
6	1	1	1	2	2	3	3	2
7	1	2	2	3	3	3	3	1
8	1	3	3	3	1	2	1	2
9	2	2	2	3	2	2	2	3
10	2	2	2	3	2	3	3	2
11	2	2	2	3	3	3	3	2
12	3	2	2	3	2	1	3	2
13	3	2	2	2	2	2	2	1
14	1	2	2	2	2	2	2	2
15	2	2	2	3	2	3	3	2
16	2	2	2	3	2	3	3	2
17	1	2	2	2	2	2	3	2
18	2	2	2	2	2	2	2	1
19	2	2	2	3	2	3	2	1
20	2	2	2	3	2	3	3	1
21	2	1	1	3	3	3	3	2
22	3	3	3	3	3	3	3	3
23	3	2	2	3	3	3	3	2
24	2	2	2	3	2	3	3	2
25	1	1	1	3	2	3	3	1
26	1	1	1	2	2	2	3	1
27	2	2	2	2	2	2	3	1
28	2	2	2	2	2	3	3	1
29	2	2	2	3	1	3	3	1
30	2	2	2	3	2	3	3	2
31	1	1	1	3	2	1	3	1
32	1	1	1	3	2	2	3	1
33	2	1	1	2	2	2	3	2
34	3	3	3	3	3	3	3	3
35	3	2	2	3	3	3	3	2
36	2	2	2	3	3	3	3	2
37	2	2	2	3	2	3	3	2
38	2	2	2	3	3	3	3	2
39	2	2	2	2	2	3	3	2
40	2	2	2	2	2	2	2	2

ENC.	PREG 12	PREG 13	PREG 14	PREG 15	PREG 16	PREG 17	PREG 18	PREG 19
41	2	2	2	3	2	2	2	3
42	2	2	2	3	2	3	2	3
43	2	1	1	3	2	3	2	3
44	2	2	2	3	2	3	3	2
45	2	2	2	3	3	3	3	2
46	3	2	2	3	3	3	3	1
47	2	2	2	3	2	3	2	1
48	2	1	1	3	2	3	2	1
49	2	1	1	2	2	2	2	1
50	2	3	3	2	2	2	2	1
51	3	3	3	2	2	3	2	1
52	3	3	3	3	2	3	2	1
53	2	2	2	3	2	3	2	1
54	2	2	2	3	3	3	2	1
55	1	2	2	3	3	3	2	2
56	2	2	2	3	2	3	2	2
57	2	2	2	1	2	3	3	2

ANEXO 6

CONSENTIMIENTO INFORMADO

TITULO DE LA INVESTIGACIÓN
LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE PREVENCIÓN DE LOS DELITOS INFORMÁTICOS EN EL PERÚ

PROPÓSITO DEL ESTUDIO
Establecer que la protección de datos personales, se relaciona con la prevención de los delitos informáticos en el Perú
PROCEDIMIENTO PARA LA TOMA DE INFORMACIÓN
Entrega individual del cuestionario a cada uno de los encuestados, quienes lo devuelven llenado y de forma anónima
RIESGOS
Ninguno
BENEFICIOS
Beneficios en el ámbito laboral de los encuestados que tendrán una fuente de información seria sobre un tema no investigado en el Perú. No representa ningún tipo de beneficio económico para el encuestado.
COSTOS
Ningún costo para el encuestado y/o institución.
INCENTIVOS O COMPENSACIONES
No se han establecido
TIEMPO
Tiempo de la aplicación de la encuesta un mes.
CONFIDENCIABILIDAD
Participación voluntaria y anónima. Los datos recabados serán utilizados únicamente en la presente investigación, respetando estrictamente su confidencialidad, los cuales serán eliminados al término del estudio.

CONSENTIMIENTO:

Acepto voluntariamente realizar esta investigación. Tengo pleno conocimiento del mismo y entiendo que puedo decidir no participar y que puedo retirarme del estudio si los acuerdos establecidos se incumplen.

En fe de lo cual firmo a continuación

Fernando Martín Robles Sotomayor
DNI N° 06085961

ANEXO 7

AUTORIZACIÓN DE LA ENTIDAD DONDE SE REALIZÓ EL TRABAJO DE CAMPO

No se requirió por haberse aplicado el instrumento de validación a profesionales Fedatarios Juramentados con Especialización en Informática, que no se encuentran reunidos en ninguna institución.

ANEXO 8

DECLARATORIA DE AUTENTICIDAD DEL INFORME DE TESIS

DECLARACIÓN JURADA

Yo, Fernando Martín ROBLES SOTOMAYOR, identificado con Documento Nacional de Identidad N° 06085961, domiciliado en la Villa Militar Moronacocha Casa N° 17, distrito de Iquitos, provincia de Maynas, departamento de Loreto, con teléfono celular N° 954429804 y email roblesabogado@gmail.com

DECLARO BAJO JURAMENTO

Que, el trabajo de Tesis titulado "LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE PREVENCIÓN DE LOS DELITOS INFORMÁTICOS EN EL PERÚ, EN LOS AÑOS 2017 Y 2018" para optar el grado académico de Doctor en Derecho, en la Escuela de Posgrado de la Universidad Alas Peruanas, es un trabajo de mi autoría y original en sus contenidos y elaboración.

Para lo cual firmo la presente declaración.

Iquitos, 14 de Diciembre del 2018.

Mg. Fernando Martín Robles Sotomayor
DNI N° 06085961
Abogado - Docente