UNIVERSIDAD PERUANA LOS ANDES

Facultad de Derecho y Ciencias Políticas

Escuela Profesional de Derecho

TESIS

TITULO: **INSEGURIDAD INFORMATICA Y DELITOS INFORMATICOS DEL USUARIO FISCALÍA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO 2019**

PARA OPTAR: **EL TITULO PROFESIONAL DE ABOGADO**

AUTOR: **MARÍA ISABEL ALANYA RIVERA**

ASESOR: **Dra. HUALI RAMOS JESSICA PATRICIA**

FECHA DE INICIO Y DE CULMINACION: **14/02/2021 A 15/12/2021**

LÍNEA DE INVESTIGACIÓN: **DESARROLLO HUMANO Y DERECHO**

HUANCAYO – PERU
2021

AGRADECIMIENTO

Agradezco a la Universidad Peruana Los Andes por formarme como profesional y por otorgándome a los mejores docentes.

RESUMEN

El presente trabajo partió del problema general: ¿De qué manera la inseguridad informática influye en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019? siendo su objetivo general, determinar la influencia de la inseguridad informática en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019, teniendo como hipótesis general la inseguridad informática influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019. Se empleó como metodología general el método Deductivo-Inductivo; como método especifico se utilizará el método Explicativo y como método particular Sistemático; teniendo como instrumentos la recolección de datos mediante el cuestionario, aplicando la técnica de muestreo de tipo no probabilístico por conveniencia; se contó con 6 fiscales de la Fiscalía Provincial Penal Corporativa de Huancayo. Se desarrolló diversos temas sobre la inseguridad informática con la finalidad de poder determinar cómo este está estrechamente ligado con los delitos informático, debido a que el usuario es el quien permite el acceso a sus datos informáticos. Se concluyó que la inseguridad informática tiene cierta influencia en los delitos informáticos.

PALABRAS CLAVE: Inseguridad Informática y el Delitos Informáticos

ABSTRAC

The present work starts from the general problem: In what way does computer insecurity influence the computer crimes of the user in the Huancayo Provincial Criminal Criminal Prosecutor's Office in the year 2019? Being its general objective, to determine the influence of computer insecurity in the computer crimes of the user in the Provincial Criminal Criminal Prosecutor's Office of Huancayo in the year 2019, taking as a general hypothesis computer insecurity significantly influences the computer crimes of the user in the Provincial Prosecutor's Office Huancayo Corporate Criminal in 2019. The Deductive-Inductive method was used as a general methodology; The Explanatory method will be used as a specific method and the Systematic particular method will be used; having as instruments the data collection through the questionnaire, applying the non-probabilistic sampling technique for convenience; There were 6 prosecutors from the Huancayo Provincial Criminal Criminal Prosecutor's Office. Various topics on computer insecurity were developed in order to determine how this is closely linked to computer crimes, because the user is the one who allows access to their computer data. It was concluded that computer insecurity has some influence on cybercrime

KEY WORDS: Computer Insecurity and Computer Crime

DEDICATORIA

AGRADECIMIENTO

RESUMEN

ABSTRAC

INDICE (Índice de tablas y figuras)

INTRODUCCIÓN

Contenido

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

CAPITULO III

MARCO TEÓRICO

CAPITULO IV

METODOLOGÍA DE LA INVESTIGACIÓN

INTRODUCCION

La presente investigación tiene como titulo la inseguridad informática y delitos informáticos del usuario en la fiscalía Provincial Penal Corporativa De Huancayo 2019, dicho trabajo de investigación tiene el objetivo de demostrar que en nuestra población existe una inseguridad por parte del usuario ya que, es el propio usuario quien proporciona las facilidades para que, se cometa un delito informático, pero en ciertos casos el ciberdelincuente es quien quebranta las medidas de seguridad que pone el usuario para poder protegerse en el ciberespacio de los posibles delitos informáticos.

En estos días para nadie es extraño el enorme cambio que se ha dado gracias a la tecnología ya que, la gran parte de la población maneja un sistema informático en donde ponemos nuestra información digital, en ella se encuentran personas naturales o jurídicas, y con una mayor relevancia e importancia en las organizaciones, donde el papel preponderante que juega para el progreso y desarrollo de una Nación ha sido aun mayor ya que esta ha optado por un mecanismo de solución más rápido de todos sus intereses a través de la tecnología, por ello vemos que varios sectores como es la salud, economía y educación, etc., han ampliado sus alcances de llegar a la población a través de la tecnología.

Junto al avance tecnológico en nuestras necesidades tales como en la industria comercial, educación, salud, en la economía y otros ha acarreado varios conflictos y peligros dentro esta índole en vista de que los delitos han mejorados sus estrategias de poder delinquir, ante ello se han comenzado a realizar delitos mediante estos sistemas informáticos que ahora lo tenemos tipificados en los Delitos Informáticos, para así poder prevenir que se sigan cometiendo estos delitos.

Esto acarrea que se pueda poder obtener un beneficio patrimonial haciendo uso de este recurso, por lo cual cualquier persona que maneje un sistema informático o digital es vulnerable ante estos ataques cibernéticos, por lo cual los ciberpolicias han tratado de contrarrestar estos tipos de delitos es por ellos que se crea una División de Investigación de Alta Tecnología (DIVINDAT), quienes buscan disminuir y proteger a los usuarios de los ciberdelincuentes.

Entendiendo esto, se desarrolla la presente investigación que contiene un estudio de la temática de la Inseguridad Informática teniendo una estrecha relación con el Fraude Informático para poder determinar un mecanismo de prevención frente a esta inseguridad informática y teniendo como eje principal al usuario, ya que para cometer este tipo de delito es indispensable la colaboración del usuario, en vista de que siempre es el usuario quien permite el acceso para poder sustraer la misma pero lo hace sin tener conocimiento de que su actuar acarrea un perjuicio personal sino que surge porque el ciberdelincuente lo mantiene en error.

Se empleó como metodología general el método Deductivo-Inductivo; como método especifico se utilizará el método Explicativo y como método particular Sistemático; teniendo como instrumentos la recolección de datos mediante el cuestionario, aplicando la técnica de muestreo de tipo no probabilístico por conveniencia; se contó con 6 fiscales de la Fiscalía Provincial Penal Corporativa de Huancayo

La presente investigación se va a dividir en 5 partes, las cuales estarán estructurados de la siguiente manera: En la Primera Parte: veremos el Planteamiento del problema: donde hablaremos de la realidad problemática, delimitación del problema, formulación del problema, justificación y objetivos. En la Segunda Parte: En la que consta el Marco Teórico: Antecedentes (Nacionales e Internacionales), Bases teóricas y Marco

Conceptual. En la Tercera Parte: Estudiaremos la Hipótesis y Variables. En la Cuarta Parte: Analizaremos la Metodología que se empleó en el presente trabajo: Método, tipo y nivel de investigación, así mismo la población y muestra, las técnicas de recolección de datos y técnica de procesamiento. En el capítulo V: Discusión de Resultados, conclusión, recomendación, Bibliografía y anexos.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

El Consejo de Europa ha firmado un Convenio sobre la Ciberdelincuencia en Budapest el 23 de noviembre del 2011, a la cual todos los miembros del Consejo y cualquier Estado que desee adherirse a ese pacto, han buscado una manera de contrarrestar la ciberdelincuencia a través de penalidades de ciertas conductas ilegales con carácter tecnológico, así mismo se ha tenido que optar que estas medidas vayan acorde a velar los derechos fundamentales y que estos no vayan en contra del interés de la acción penal.

El Perú se ha adherido al Convenio sobre la Ciberdelincuencia, con Resolución Legislativa Nº 30913 el 13 de febrero del 2019, en la cual esta se adhiere con los artículos 3, 6, 7, 9 y otros, dejando de lado el articulo 8 en la que se establece el Fraude Informático, así mismo en la ley 30171 que modifica la ley 30096, nos establece el Fraude Informático en la cual trata de agregar todo el párrafo que señala en el artículo 8 del Consejo de Europa

en Budapest, generando una confusión en la interpretación del artículo, en vista de que no se detalla que delitos son de resultado y otros que son de hecho.

Pero estas normativas no han sido suficiente para poder erradicar la cibercriminalidad, en razón de que los cibercriminales han optado por otro modus operandi, como son la mala aplicación de dominios que generan confusión a los usuarios para así poder obtener sus datos personales, contraseñas y cualquier información que el usuario proporciona al ciberdelincuente a través de una aplicación falsa.

Así mismo, el uso de una red social, en la cual para tener en cuenta se necesita poner los datos personales del usuario, en donde es posible que cualquier persona puede acceder a nuestros datos personales porque se encuentra en el ciberespacio, así se opte por una medida de seguridad este es vulnerado por el ciberdelincuente a través de los programas de espionaje; por ello es indispensable optar con una medida de seguridad para proteger estos datos informáticos y que no cualquier persona pueda acceder a estos datos informáticos.

Según (Pichihua, 2020) en su artículo señala que el "(…) Coronel de la PNP Orlando Mendieta Jefe de la División de Investigación de Alta Tecnología (DIVINDAT), menciono que la mayor cantidad de denuncias se concentra en delitos contra el patrimonio (…) teniendo un total de 2097 denuncias para el año 2019" (párr. 2).

El año 2020 debido a la coyuntura en la que se vive, todas las actividades económicas se han basado en la tecnología, por lo cual se ha creado varias bases de datos utilizando para eso a los usuarios, ya que para involucrase en una red informática, todos los usuarios deben de ingresar una base de datos, este actuar deja de manera libre a los ciberdelincuentes que puedan cometer cualquier mecanismo de fraude informático, pero este actuar se cumple manteniendo en error al usuario, es decir que el usuario es quien

colabora para que se cometa el ilícito, es por ello que los ciberdelincuentes aprovechan del desconocimiento por parte del usuario y crear un mecanismo para poder ingresar a su sistema informático y sustraer y/o malograr sus datos informáticos.

En este tiempo surge la necesidad de proteger al usuario en vista de que existe una inseguridad informática, que pone en vulnerabilidad a todos los usuarios ante el ciberespacio en donde este es vulnerable y que el ciberdelincuente se apropie de su patrimonio a través de los delitos informáticos y este hecho si no se tipifica bien las normas y si el usuario sigue desconociendo las medidas preventivas estos jamás tendrán límites al delinquir y es factible de que mejoren cada vez su modus operandi, para obtener su beneficio.

1.2. Delimitación del problema

1.2.1. Delimitación espacial

La presente investigación se limitó espacialmente en La Fiscalía Provincial Penal Corporativa de Huancayo.

1.2.2. Delimitación temporal

El ámbito temporal en él se desarrolló la investigación fue en el año 2019.

1.2.3. Delimitación conceptual

La presente investigación estará comprendida conceptualmente de la siguiente manera: Inseguridad Informática, Seguridad Informática, Programas de Espionaje, Dirección IP. Delitos Informáticos, Fraude Informático, Estafa Informática, Derecho a la Intimidad Informática.

1.3. Formulación del problema

1.3.1. Problema general

¿De qué manera la inseguridad informática influye en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019?

1.3.2. Problemas específicos

¿De qué manera la inseguridad informática influye en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019?

¿De qué manera la inseguridad informática influye en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019?

¿De qué manera la inseguridad informática influye en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019?

1.4. Justificación de la investigación

1.4.1. Social

La presente investigación otorgó un beneficio a la población, ya que se dio a conocer las medidas de seguridad necesarias para proteger el sistema informático y así reducir significativamente los delitos informático y proteger al usuario; ya que los delitos informáticos o cibercrimines son delitos que se realizan empleando los diferentes medios informáticos o electrónicos que existen, es decir, cualquier persona que tenga un dispositivo electrónico (ordenador, *smartphone*, reloj inteligente entre otros más) conectado a Internet puede cometer la infracción o ser víctima del mismo.

1.4.2. Científica – Teórica

La presente investigación generó un aporte a las ciencias del Derecho Penal debido a que actualmente nuestra Ley de Delitos Informáticos no se encuentra bien

detallado, en vista de que, en su artículo 8 de la ley N°30171, no se establece cuando son delitos de resultados y de hecho, además de que habiendo una inseguridad informática del usuario genera un mayor índice de cometerse los delitos informáticos y nuestra legislación no tiene ninguna medida de protección contra esto; por lo cual es necesario que se deba implementar una medida de seguridad tanto normativa como informáticamente, para poder disminuir al índice de los delitos informáticos.

Por ende, con el presente trabajo de investigación se aportó en brindar información importante para la adecuada aplicación de la ley 30171, ya que los magistrados podrán tener en consideración los diversos factores en que concurre los delitos informáticos y que existe responsabilidad por parte del usuario.

1.4.3. Metodológica

En la presente investigación se utilizó como instrumento de recolección de datos el cuestionario, el mismo que analizado su validez y confiabilidad servirá para las futuras investigaciones que guardan relación con la presente investigación.

1.4.4. Objetivo General

Determinar la influencia de la inseguridad informática en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019

1.4.5. Objetivos específicos

Determinar la influencia de la inseguridad informática en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

Determinar la influencia de la inseguridad informática en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019

Determinar la influencia de la inseguridad informática en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019

CAPITULO II

HIPOTESIS

2.1.Hipótesis de investigación

2.1.1. Hipótesis General

La inseguridad informática influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

2.1.2. Hipótesis Especifica

La inseguridad informática influye significativamente en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

La inseguridad informática influye significativamente en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

La inseguridad informática influye significativamente en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019.

2.2.Operacionalización de las variables

VARIABLES	DEFINICION	DIMENSIONES	INDICADORES
Inseguridad Informática (VARIABLE INDEPENDIENTE)	(Expertos, 2018): "El proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente." (párr.1)	Sistema Informático	Protege el soporte lógico en todo momento
		Programas maliciosos	Altera el funcionamiento del equipo el programa troyano
			Diseña anuncios maliciosos para robar información el hardware
		Dirección IP	Facilita el ocultamiento del IP
Delitos Informático (VARIABLE DEPENDIENTE)	Según Villavicencio (2014): "Aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que la Tecnología de la Información y Comunicación (TIC) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos (…)"(p.286)	Estafa Informática	Clona las tarjetas de crédito
			Envió de Publicidad engañosa
		Derechos a la intimidad informática	Protege la confidencialidad de los datos personales
		Fraude Informático	Se evalúa el delito por su consecuencia de la acción

CAPITULO III

MARCO TEÓRICO

3.1. Antecedentes de la investigación

INTERNACIONAL

Bermúdez y Bailón (2015); Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. [Tesis de Pregrado]; presentado para optar el Título Profesional de Ingeniero en Sistemas, Universidad Politécnica Salesiana Sede Guayaquil - Ecuador. La presente investigación materia de antecedente se relación con nuestra variable independiente La Inseguridad Informático. En el que formula el siguiente problema de investigación: ¿Cómo se podría minimizar los riesgos de perdida, daño o alteración de la información administrada dentro de la empresa Credigestión?; la misma que consta con el objetivo general: Analizar los procesos críticos de Credigestión respecto a las cuestiones de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basados en la Norma ISO/IEC 27001.

La presente investigación citada presenta la metodología de la modalidad de campo y bibliográfica, en la que consta como tipo de investigación: tipo de investigación de campo en la que se realizó a través de la observación, tipo de investigación descriptiva donde se describe todos los procesos en la que se desarrolla el objeto de estudio, tipo de investigación no experimental demostrando que el objeto de estudio no se va a modificar o alterar y tipo de investigación explicativa en donde se va a explicar las causas del objeto de estudio; así mismo cuenta con una población que se conformó con 230 empleados de los departamentos de la empresa Credigestión.

Llego a la siguiente conclusión: "La seguridad total no existe, pero gestionar controles de seguridad en el proceso y manejo de la información, se vuelve un complemento esencial, pues le permite asegurar información valiosa no sólo de la empresa sino también de los clientes" (p.135).

Del citado antecedente podemos decir que si bien es cierto existe de alguna medida una seguridad informática, esta carece de confiabilidad total en razón de que existe una clara inseguridad informática, donde los datos personales del usuario están a la libre disposición de cualquier usuario o ciberdelincuente.

Dentro del ámbito económico las entidades financieras ponen en riesgo a los clientes y a ellos mismos, ya que estas no cuentan con una seguridad en proteger sus datos personales como son su nombre, domicilio y/o contraseñas de las tarjetas de crédito en vista de que los ciberdelincuentes pueden quebrantar estas medidas, inducir a error al usuario o infectar el programa de la entidad para poder cometer el ilícito; es decir que a pesar de que cada entidad o institución opte por un medio de seguridad informática, no existe una protección total de los datos.

Chauca (2014); El principio de proporcionalidad en la prevención de los delitos informáticos. [Tesis de Pregrado]; presentado para optar el Título Profesional de Abogado, Universidad Regional Autónoma de los Andes, Ibarra-Ecuador. La presente investigación materia de antecedente se relación con nuestra variable dependiente: Los Delitos Informáticos. En el que formula el siguiente problema de investigación: ¿Cuál es el impacto que provoca la no aplicación del principio de proporcionalidad en los delitos informáticos?; la misma que consta con el objetivo general: Elaborar un ensayo acerca de la importancia de la aplicación del principio de proporcionalidad, para la prevención de los delitos informáticos cometidos en las redes sociales.

La presente investigación citada se ha empleado el método Inductivo-Deductivo, porque inicia de lo particular hasta llegar a una conclusión general; así mismo usa el método0 histórico -lógico; ya que el objeto de estudio enmarca varios delitos, en la cual se explica los avances normativos por último se usó el método científico; como técnica de investigación uso la encuesta, teniendo como instrumento el cuestionario, la cual tuvo como una población de 200 abogado y 100 usuarios al emplear la muestra se obtuvo 90 abogados y 45 usuarios, con un total de 135.

Llego a la siguiente conclusión:

> "Concluimos que este trabajo de investigación es importante para dar a conocer que en el país existe un problema muy grave que está afectando a los usuarios, todo esto producto de los delitos informáticos en cual se ve reflejado tanto por la inseguridad informática que existen, así mismo por la falta de conocimiento de las personas sobre este problema." (p.58)

El antecedente mencionado hace referencia de que efectivamente hay una inseguridad informática que pone en riesgo a los usuarios, pero este mismo hecho hace

que, para quebrantar esta seguridad en la gran mayoría de delitos informáticos se requiere de la participación del usuario que es inducido a error por el ciberdelincuente; ya que los cyber-delincuentes necesitan la autorización por parte del usuario para poder ingresar al sistema de este.

Es por ello que el usuario debe de conocer las medidas de seguridad adecuadas, además de que este pueda reconocer que paginas son legales y cuales son servidores de dominio (clonadas). Ahora podemos decir de que no existe una seguridad confiable ya que siempre existe un margen de error que este es aprovechado por los cyber-delincuentes.

Nacionales

León (2018); Bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención de los Delitos Informáticos de la Ley 30096. [Tesis de Grado]; presentado para optar el Título Profesional de Abogado, Universidad Señor de Sipán, Chiclayo-Perú. La presente investigación materia de antecedente se relación con nuestra variable dependiente: Los Delitos Informáticos. En el que formula el siguiente problema de investigación: ¿Cuál es el efecto del bloqueo del IP dinámico dentro del comercio electrónico frente a los delitos informáticos en la ley 30096?; la misma que consta con el objetivo general: Proponer el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos en la ley 30096

La presente investigación citada se ha empleado el Método científico descriptivo, teniendo como tipo de investigación descriptiva en la que consta como diseño no experimental o transversal, por lo cual se tiene como muestra y población: Los Jueces, abogados y catedráticos de Derecho Comercial Penal con un total de 50, en la que se

obtendrá la valides del objeto de estudio por lo cual se utilizó como instrumento de recolección de datos el cuestionario/encuesta.

Llego a las siguientes conclusiones:

> "Que de conforme a lo planteado se asegurara la transacción electrónica a través del bloqueo de la IP dentro del comercio electrónico por cuanto la autenticación a través de un usuario único y el ingreso de interconexión de una IP estática es la forma más eficiente para restringir el acceso a hackers o atentados contra las transacciones de comercio electrónicas ejecutadas en el C2C." (p. 84)

De lo citado podemos empezar a estudiar una posible solución a nuestro problema planteado, en vista de que, al momento de bloquear la IP de cada uno de los usuarios se restringe de alguna manera que el cyber-delincuente pueda tener acceso a nuestra información digital (datos personales, cuentas de correo electrónico, cuentas bancarias, entre otros muchos datos y más), pero no solo abarcarnos o limitarnos al hecho de la transacción de comercio electrónico; sino expandir este mecanismo a cualquier almacenamiento de datos de todo sistema operativo, en vista de que si restringimos el acceso a nuestra IP, el cyber-delincuente no podría tener el control total o parcialmente de nuestro sistema operativo.

A la fecha nuestra legislación no tiene medidas preventivas contra los delitos informáticos es por ello que surge la posibilidad de encontrar medidas de seguridad al usuario para que no incremente las víctimas del fraude informático; es por ello que podemos deducir que si nosotros normamos ciertas conductas informáticas podemos llegar a que no se cometan más fraudes informáticos sin llegar a una norma punitiva.

Pardo (2018); Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. [Tesis de Posgrado]; presentado para optar el Título Profesional de Maestro en Derecho Penal y Procesal Penal, Universidad César Vallejo, Lima-Perú. La presente investigación materia de antecedente se relación con nuestra variable dependiente: Los Delitos Informáticos. En el que formula el siguiente problema de investigación: ¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018?; la misma que consta con el objetivo general: Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

La presente investigación citada se ha empleado mediante la investigación cualitativa de nivel descriptivo explicativo, bajo los parámetros interpretativos y analíticos de la investigación, en razón de que el objeto de investigación jurídica ha sido interpretativo y que estos se han descompuesto para su interpretación y análisis de la investigación, teniendo como método analítico, comparativo, dogmático, descriptivo e inductivo. La misma que para el recojo de información ha utilizado la técnica de la entrevista.

Llego a las siguientes conclusiones:

> "El tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio". (p. 122)

Estamos de acuerdo con lo mencionado por el tesista en lo referido a que en nuestra legislación aún no se encuentra regulado ciertas protecciones mediante las redes sociales más usadas por los usuarios ya que por medio de ellas a través de spam (mensajes no solicitados, de tipo publicitario que son enviados de forma masiva), donde necesariamente para acceder a una de estas páginas se necesita ingresar sus datos personales las cuales cualquier persona puede acceder a las misma, este caso sucede mayormente mediante Facebook, Twitter, Instagram, Gmail y otros aplicativos, en donde para poder ingresar o ser usuario de este aplicativo se debe de ingresar los datos personales para posteriormente todos los demás usuarios de las diferentes redes sociales puedan buscarnos e interactuar con nosotros visualizando nuestro perfil, si nosotros por más que tengamos ocultos estos datos personales cualquier ciberdelincuente puede acceder a este, causando un perjuicio al usuario, por lo cual es necesario poder regular estas conductas de manera eficaz para así evitar cualquier delitos informático.

Rivero (2017); Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017. [Tesis de Pregrado]; presentado para optar el Título Profesional de Abogado, Universidad César Vallejo, Lima-Perú. La presente investigación materia de antecedente se relación con nuestra variable dependiente: Los Delitos Informáticos. En el que formula el siguiente problema de investigación: ¿Cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano?; la misma que consta con el objetivo general: Analizar como la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano

La presente investigación citada se ha empleado el tipo de investigación cualitativo-aplicada ya que buscaba comprender los fenómenos sociales que perjudican la normativa para poder proponer mecanismos de solución, para lo cual utilizo el diseño de teoría fundamentada ya que el tesista desarrolla su objeto de estudio con una amplia

conceptualización; teniendo como población especialistas en ciberdelitos como son; especialistas de la DIVINDAT, Peritos informáticos, Jueces, Fiscales y Abogados, teniendo como muestra 20 especialistas; para lo cual se usó el muestreo o probabilístico y un muestreo intencional.

Llego a las siguientes conclusiones:

> "Se ha analizado como la admisión de la evidencia digital incide positivamente en los procesos penales sobre los delitos informáticos, porque se busca el esclarecimiento adecuado del hecho delictivo, la falencia es el grado de desconocimiento por parte de los operadores jurídicos que no consiguen tener comprensi6n ni del delito ni de las evidencias. Sumados a la existencia de una legislación que tiene carencias y no abarca todos los delitos con sus modalidades. Que, a pesar de tener personal capacitado, peritos informáticos, especialistas de la DIVINDAT, estos no se dan abasto para la carga de investigaciones, tomando en cuenta que no ayudan las herramientas que tienen por no ser optimas o ha vencido su licencia para ser utilizadas. Por lo que genera demoras, por problemas burocráticos, hasta la obtenci6n de una nueva licencia". (p. 103)

De lo citado podemos decir que vivimos en una era digital al cual poco a poco nos vamos adaptando, pero esto resulta ineficiente ya que no se puede regular y optar por las medidas preventivas para así poner fin a la cyber-delincuencia.

Es por ello que debido a la nueva era en la que se vive es necesario poder adecuarnos a estas exigencias como son las evidencias, si bien es cierto se sigue utilizando las evidencias físicas estas no nos limitan a expandir esas evidencias en el ámbito tecnológico, lo cual nos va a permitir esclarecer los hechos suscitados; por ello es

necesario que nuestras autoridades competentes estén capacitadas y tengas todos los medios necesarios para poder contrarrestar la cyber-delincuencia, ya que esta ciberdelincuencia va tomando maneras de no ser ubicados y quedar impune sus delitos.

Romero (2017); Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016 [Tesis de Pregrado]. presentado para optar el Título Profesional de abogada, Universidad de Huánuco - Perú. La presente investigación materia de antecedente se relación con nuestra variable dependiente los Delitos Informáticos. En el que formula el siguiente problema de investigación: ¿Cuáles son los delitos informáticos cometidos a través de las redes sociales y que tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco, 2016?; la misma que consta con el objetivo general: Determinar los delitos informáticos cometidos a través de las redes sociales y el tratamiento que le brinda el Ministerio Publico en la ciudad de Huánuco, 2016.

La presente investigación citada se ha empleado el Método Inductivo, teniendo como numero de variables es descriptivo; teniendo como diseño transversal descriptivo, con un nivel descriptivo; además cuenta con una población de 620 procesos (denuncias), por consiguiente, tiene una muestra de 38 casos, para lo cual las técnicas e instrumentos de investigación que se empleo fue el análisis documental, análisis, la entrevista y encuesta.

Llego a las siguientes conclusiones:

> “Al analizar los delitos informáticos más frecuentes podemos apreciar que la Alteración, daño o destrucción de base de datos representa el 26,1%; el Tráfico ilegal de datos 19,3%; el Atentado a la integridad de datos informáticos el 13,6%; el Atentado a la integridad de sistemas informáticos

> un 12,5%; las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos 10,2%; la Interceptación de datos informáticos el 9,0%; el Fraude informático 4,5%; la Suplantación de identidad el 2,2% y el Abuso de mecanismos y dispositivos informáticos el 2,2%." (p. 63)

El antecedente mencionado nos lleva a la conclusión de que los delitos informáticos cada día van tomando mayor índice de criminalidad el cual no se disminuye en alguna medida, puesto que no existe una normativa acorde a los hechos es por ello que surge la necesidad de tipificar de manera correcta los delitos informáticos.

También podemos mencionar que, si bien en cierto las redes sociales no tiene demasiada implicancia referido a los datos informáticos o la seguridad que estos te dan, pero en cierta medida no se encuentra protección para estos datos personales; así mismo al momento de que cualquier persona ha sufrido un caso de Fraude Informático mediante las redes sociales, las autoridades han dejado de lado el derecho a la privacidad que esta ha sufrido y le dan mayor importancia a patrimonio que puedo haber perdido.

3.2. Bases teóricas de la investigación

Variable Independiente: Inseguridad Informática

A. Concepto de Seguridad Informática

Antes de iniciar a hablar sobre la inseguridad informática debemos de abordar todo lo relacionado con la seguridad informática, ya que si no conocemos que es la seguridad informática no podemos abordar sobre la inseguridad informática, para ello debemos de mencionar por Romero y Otros (2018) en la que señala:

> “La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático”. (p. 13).

Es decir que la seguridad informática es muy importante ya que es aquella encargada de salvaguardar nuestra información privilegiada a través de encriptadores, antivirus originales de paga, anti-malware, etc; y así cuidar nuestra información almacenada y que no solo va a tener que proteger la confiabilidad de estos datos, sino que de todo lo que sea necesario para tener un óptimo funcionamiento de un sistema de seguridad.

Es aquella protección que se da a cualquier sistema informático, en vista de que al tener un sistema informático somos susceptibles de ser víctimas de los ciberdelincuentes, es por ello que debemos optar por un mecanismo de seguridad para protegernos de los ciberdelincuentes, sea mediante software u otros medios pertinentes que dificulte el acceso a nuestra información personal a los ciberdelincuentes.

El objetivo de la protección es poder proteger nuestra base de datos para que nadie pueda acceder; pero no solo debemos de hacerlo con nuestras laptop, Tablet o computadora sino que debemos de proteger también nuestras cuentas en las redes sociales como son Twitter, WhatsApp, Messenger, Facebook, Instagram y Otros; así mismo

proteger nuestros dispositivos celulares en los cuales accedemos a llamadas y mensajes de textos; dispositivos o redes en las que podemos ser un vulnerables de ser víctimas de los ciberdelincuentes; no solo con el ilícito de poder sustraer un fin económico sino también pueden sustraer una información privilegiada, documentos, conversaciones, imágenes, videos, entre otros; vulnerando nuestro derecho a la intimidad la cual es lo primero que se infringe para cometer cualquier ilícito de índole informático.

B. Objetivos de la Seguridad Informática

Para poder garantizar la seguridad de un sistema informático se debe de tener en cuenta tres aspectos importantes para que este se pueda proteger, entre las cuales son:

Confidencialidad o Privacidad:

Para conocer un poco debemos de dar una definición a lo que (GSITIC, 2018) señala: "Es la necesidad de que la información sólo sea conocida por personas autorizadas no convirtiendo esa información en disponible para otras entidades. En casos de falta de confidencialidad, la información puede provocar daños a sus dueños o volverse obsoleta." (párr. 3). Por lo cual el sistema debe de proteger la privacidad y la confidencialidad de los usuarios ante el ciberespacio, por ello este software o hardware hace que sea fiable la navegación a través del sistema, caso contrario no tendríamos la confianza de poder usar un dispositivo.

Esto garantiza que los usuarios puedan usar de manera libre y segura el sistema, pero este sistema no quiere decir que es inquebrantable porque este sistema presenta un margen de inseguridad que este es aprovechado por los ciberdelincuentes para poder cometer su ilícito. Por lo cual no podemos hablar de una seguridad totalmente segura y esta inseguridad es la que debemos de proteger.

La integridad

La cual manifiesta que según (Infosegur, 2013) señala que:

> "Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito". (párr. 5).

Lo que nos trata de decir que garantiza que el sistema informático de manera automática no puede generar cambio en la base de datos o se pueda alterar cualquier tipo de información, así como el autor nos plantea el hecho que el usuario ingresa a su cuenta para realizar un trámite bancario a través del internet en la que el usuario tiene la seguridad de que este no será clonado o alterado dicha información, es decir que se busca la protección de la misma a través de este.

La Disponibilidad u Operatividad:

Este objetivo lo desarrolla de manera más comprensible según (GSITIC, 2018)Señala que:

> "Es la capacidad de que la información esté siempre disponible para ser procesada por personal autorizado. Esto requiere que dicha información se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria." (párr. 3)

Este objetivo es muy importante ya que garantiza al usuario a que este estará en óptimas condiciones cuando el usuario desee hacer uso de este, por ejemplo, cuando los usuarios desean conocer el proceso de sus expedientes judiciales a través de las consultas

de expedientes judiciales, este tiene que estar disponible y en óptimas condiciones para ser empleado por los usuarios.

C. Seguridad Física y Seguridad Lógica

La Seguridad Física:

Para conocer mejor sobre la inseguridad informática, debemos de saber cuáles son las partes que son susceptibles de vulneración o puede sufrir algún ataque para ello en primer lugar debemos de saber que la seguridad física está relacionada a la protección del sistema ante amenazas tangibles, pero estas se presentan a través de vulnerabilidades la cual según Romero y Otros (2018) señala:

> "Las vulnerabilidades físicas son las que van a afectar a la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales, como ejemplo se podría mencionar una vulnerabilidad alta de este tipo si se vive en una zona de alto riesgo de sismos, ya que puede presentarse una negación en el servicio, una afectación en la disponibilidad y a partir de ahí se podría empezar con problemas. Si la organización está en una zona que generalmente se inunda, se tiene también otro tipo de vulnerabilidad." (p. 41)

La seguridad informática física es vulnerable de manera a través de los agentes externo que alterar todo o en parte el sistema informático ya que como el autor menciona los acontecimientos naturales también generar un perjuicio al sistema informático haciendo imposible su recuperación.

La seguridad lógica:

Se basa a la parte interna del sistema conocido como parte lógica ya que se encarga de la protección interna del sistema, en donde este presenta objetivo, según (GSITIC, 2018) señala:

1. "Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no les correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos por el procedimiento correcto.
4. Que la información transmitida sea recibida por el destinatario al que ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información." (párr. 11)

A esta seguridad Lógica es vulnerada por tres factores: Configuración, Actualización y Desarrollo. La primera se relaciona a las configuraciones que el usuario realiza en el dispositivo pero que estas al hacerlo mal genera un defecto al sistema, la segunda es referido a las actualizaciones, por ejemplo, si no se actualiza el dispositivo, las seguridades de este es de fácil vulnerabilidad y por último se basa en el desarrollo que maneja cada dispositivo, haciendo que si se comete un error por parte del usuario este sea inoperativo.

D. Consecuencias de la falta de seguridad

Así mismo debemos de saber qué pasaría si se carece de seguridad tanto en la parte lógica como en la parte física del sistema, se volvería más vulnerable los datos que el usuario podría manejar dentro de un sistema informático.

Si bien es cierto que el mismo sistema protege y hace que un dispositivo sea seguro para su utilización, pero este siempre va a necesitar de otros aplicativos para mejorar el rendimiento de un sistema informático o que este tenga mayor seguridad en su uso, pero que pasaría si nosotros omitimos cualquier tipo de seguridad para proteger nuestros datos, fácilmente cualquier ciberdelincuente podría acceder a nuestra base de datos, así mismo puede destruir todo el sistema informático a través de los programas maliciosos o virus que hagan inoperativo el sistema.

Es decir, a través de la seguridad informática se busca proteger todos los datos que pueda tener el usuario en el sistema informático, protegiendo toda la parte lógica del sistema y la parte física, protegiendo al usuario que pueda utilizar este sistema de manera segura y no sea víctima de ningún ataque a su sistema, por ejemplo, en un sistema bancario, hace que las transacciones que realiza la entidad sea segura, que no sufra ningún tipo de robos; otro caso de protección son los datos que una empresa coloca sobre su producto, la contabilidad que este maneja sea de acceso público o que cualquier persona tenga acceso total a esta información, es por ello que es importante la seguridad informática.

Según Gómez (2014) señala: “A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red (…)” (p. 49)

A lo citado debemos de tener en cuenta que los daños que se ocasionan por la falta de una seguridad informática van a tener varios perjuicios para la organización en razón de que, ocasiona pérdidas económicas además se va a requerir el esfuerzo laboral para poder restablecer la seguridad de un sistema, en el tiempo que esto pase ya es posible que roben datos comerciales como son: las estrategias comerciales, el lanzamiento de un nuevo producto, el inventario de la empresa, egresos e ingresos de la empresa, así mismo, la libertad de acceder a la base de datos de los clientes, personal de la empresa, entre otro tipos de perjuicios que podría acarrear una ineficiente seguridad o la omisión de esta.

Para poder evitar estos riesgos es necesario que se implemente una medida de seguridad acorde a las necesidades del usuario o la utilidad que este le da, para ello se necesita de un especialista que pueda manejar de manera constante la seguridad informática.

E. Inseguridad Informática.

Como hemos estado analizando no existe una seguridad informática totalmente confiable o indestructibles ya que esta seguridad es quebrantable por varias amenazas que estos afrontan.

Antes de avanzar daremos una definición sobre inseguridad informática a lo que (Prácticas.COM, 2017) señala que es:

> "Se denomina inseguridad informática a la ausencia total o parcial de seguridad en un sistema o aplicación informática, lo que puede hacer que un hacker aproveche dicha vulnerabilidad, ya sea su objetivo la ciber-delincuencia o demostrar la falta de seguridad. La inseguridad informática puede deberse a diferentes motivos, tales como falta de conocimientos del

> usuario acerca de las funciones del sistema, falta de conocimiento de las medidas de seguridad disponibles, por comodidad o por no ser consciente de los riesgos de subestimar el criterio de seguridad.” (párr.1)

Es decir que la inseguridad informática es la carencia de seguridad en el sistema informático, facilitando al ciberdelincuente que este acceda de manera libre a toda la base de datos del usuario.

F. Causas de la Inseguridad Informática

Pero que esta inseguridad es causada debido a que este estado esta direccionado a la falta de conocimiento por parte del usuario de acuerdo a las funciones que debería de emplear para un adecuado uso del sistema informático, estas acciones son de acuerdo al estado:

Estado de Inseguridad Activo:

Este estado se refiere a que el usuario desconoce de las funciones que debería de hacer en el sistema informático produciendo una inseguridad o el quebrantamiento del sistema informático.

Entre estas acciones encontramos, por ejemplo, la carga excesiva de una computadora, esto hace que la batería explote o se vuelva inoperativo el dispositivo.

Según Saraviia (2020) señala: “es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita).” (párr. 1)

Es por ello que cada usuario debe de saber cómo utilizar un sistema informático ya que el desconocimiento genera la pérdida total o parcial del sistema informático, esta protección es de manera externa ya que no involucra la alteración, supresión o el ingreso de un tercero al sistema si no que se basa por el mero desconocimiento de las funciones que desconoce el usuario frente al sistema informático.

Estado de Inseguridad Pasivo:

Mientras que el estado de inseguridad pasivo estado está referido al desconocimiento que el usuario tiene frente los mecanismos de seguridad informática, causando que este sistema informático tenga carencias de seguridad.

Cada usuario debe de conocer los mecanismos de seguridad para poder proteger su sistema informático, para poder así evitar que los ciberdelincuentes accedan a nuestra base de datos; así mismo el usuario debe de saber emplear bien estas medidas de seguridad para no mal utilizar los mecanismos de seguridad informática.

El hecho que un usuario desconozca las medidas de seguridad genera un perjuicio a su sistema informático ya que lo deja desprotegido ante el ciberespacio.

G. El dualismo de la Seguridad Informática y la Inseguridad Informática

Por ello debemos de hablar del dualismo de la Seguridad Informática y la Inseguridad Informática ya que este dualismo lo vamos a enfocar desde el punto de vista de un causa y efecto para poder comprender sobre el tema del dualismo; para ello Cano (2004) señala que:

> “Presentamos la estrategia de la dualidad, como una manera complementaria de explorar los hechos mismos en el mundo, para

> reconocer las causas y los efectos en su contexto, sin negar la posibilidad de considerar que uno surge a partir del otro, es decir, reconocer que la seguridad informática surge a partir de considerar la inseguridad informática y viceversa; un continuo de aprendizaje que muchas veces no corresponde a una causa específica sino a las relaciones existentes entre los componentes objeto del análisis." (párr. 2).

Es decir que si bien es cierto la seguridad informática se preocupa por todo lo que está relacionado a la protección del sistema informático este va a presentar ciertas inseguridades como lo es el mismo usuario, quien amenaza el sistema informático.

Por lo cual el sistema dual trata de explicar cuáles serían las consecuencias de no tener un adecuado uso de la seguridad informática, sino que también se va analizar ciertas deficiencias que el usuario no ha podido prever, es decir que si el usuario ha implementado un mecanismo de seguridad este no es del totalmente seguro ya que presenta márgenes de error, que es aprovechado por los ciberdelincuentes, es por ello que la inseguridad informática trata de demostrar como mecanismo preventivo la seguridad informática.

PRIMERA DIMENSIÓN: Sistema Informático

Según el Convenio de Budapest (2001) "Se entenderá 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." (párr. 1), es decir que un sistema informático es todo dispositivo capaz de almacenar información y que esta tenga la utilidad de procesar estos datos en tiempo real, así como las laptops, computadoras, celulares y/u otros dispositivos capaces de almacenar

información y que esta misma procese los datos, es decir debe de contar con un software y un hardware.

A. Componentes

En el Sistema Informático debe de estar compuesto por los siguientes elementos los cuales son:

El Hardware:

Para conocer bien el sistema informático debemos de saber que el sistema informático está compuesto por el hardware que es la parte física del sistema informático encargado de almacenar y procesar la información, según Villar (2006) define como: "El conjunto de dispositivos y componentes electrónicos de los que consta el ordenador, es decir, es la parte "física" o "mecánica". Proporciona un marco para el desarrollo de soluciones a problemas concretos" (p. 16)

El software:

Quien es la encargada de la parte lógica del sistema informático cuya función es el procesamiento de datos para poder transformar y extraer información que el usuario desea emplear.

Este software presenta tipos, las cuales las más importantes que son amenazas del sistema informático es software de sistema, quien es el encargado del cumplimiento y el funcionamiento de todas las aplicaciones que maneja el sistema informático para su adecuada aplicación.

Así mismo el software de programación, es quien permite el acceso de un nuevo software, pero este por propia mano del usuario no lo puede emplear ya que se requiere

conocer la parte del sistema del software que se va a implementar, es decir que se debe de conocer de informática para emplear este software.

Por otro lado, el software malicioso, es quien nos importa más, ya que estos están creados para destruir o alterar el sistema informático, comúnmente se le conoce como malware ya que su finalidad es que un tercero ingrese al sistema informático con fines ilegales.

B. Tipos de Sistema Informático

Ahora dentro del sistema informático presenta sus tipos, los cuales entre los principales usos de sistema informático tenemos al:

Sistema de procesamiento básico de la Información:

Ya que esta se encarga de las funciones primarias que el usuario realiza en el sistema informático, por ejemplo, el procesamiento de información

Este sistema presenta entre las funciones que tiene este cuenta con dos principales, quien a través del sistema de procesamiento de transacciones comúnmente llamado como (TPS) señala que según (ECURED, 2020) señala que:

> Estos se dedican al proceso físico de los datos relacionados con ciertas transacciones rutinarias y aisladas en el trabajo habitual de las entidades socioeconómicas, tales como el control de inventarios, control de activos fijos o la nómina de sueldos o salarios, explotan poco las posibilidades de las máquinas y el software actual. (párr. 9)

Es decir que se basa a la simple del sistema que se encarga de la clasificación y guardado de información, demostrando la poca utilidad que se le da a este.

Mientras que sistema de automatización de oficinas, conocidas por OAS manifiesta que según (ECURED, 2020) señala que:

> “Incluye el empleo de procesadores de texto, hojas electrónicas de datos, preparadores de exposiciones, calendarización, comunicación mediante correos electrónicos, videoconferencias, implican la búsqueda y captación de operaciones y en muchos casos, la preparación de decisiones para ejecutivos y directivos. Pueden solucionar tareas típicas de las oficinas, como la programación y control de actividades mediante agendas electrónicas individuales y colectivas, registro y control de acuerdos y directrices, escritura y conformación de textos en informes, folletos, creación, actualización y consulta de bases de datos relacionadas con clientes y vendedores. (párr.10)

A través de este sistema se genera más funciones al sistema ya que se le va otorgar fechas específicas como recordatorios que no deben de estar desactualizados.

Sistemas basados en la técnica WEB

Mientras que sistemas basados en la técnica WEB, en nuestra actualidad la función que le hemos dado a la web como servicio de internet se ha ido incrementando, por lo cual tenemos que hablar de intranets, (ECURED, 2020) señala que es: “Una intranet es una red particular, basada en redes de comunicación de área local o en redes de área amplia, que utiliza tecnología estándar y servicios o productos que se pueden encontrar o han sido desarrollados para Internet.” (párr.25)

A través de los intranets, el cyber-delincuente pueden los acceder al sistema informático del usuario a través del intranet que este puede o no tener conexión a internet, pero este puede seleccionar accesos que el usuario no ha permitido.

C. Amenazas del Sistema Informático

Antes de definir algunas de las amenazas que presenta el sistema informático daremos una definición de amenaza, a lo que Gómez (2014) señala que: “Se considera amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.” (p. 60).

Amenazas naturales

Ahora debemos de saber las amenazas que sufre el sistema informático, lo cual uno de las amenazas que no pueden ser predecibles es amenazas naturales como su mismo nombre lo define son causados por la naturaleza, por ejemplo, la falla de la red debido a truenos, tormentas, inundación, fallos electrónicos, incendios entre otros desastres que destruye total o parcialmente el sistema informático.

Programas maliciosos:

Mientras que uno de las amenazas que son predecibles, pero que comúnmente el usuario desconoce que dentro de su sistema informático se encuentra un programa malicioso, ya que no son de difícil reconocimiento, así mismo estos atacan la parte lógica del sistema informático a través de virus, troyanos alterando el funcionamiento de todo el sistema informático, así mismo estos también pueden robar datos informáticos, mantenerse ocultos para que el usuario no se percate de que este se encuentra en su sistema, además pueden a través de la cámara web que presenta el sistema informático como las computadoras, Tablet, entre otros, visualizar al usuario, captando cada uno de los movimientos que este realiza.

A este suceso también debemos de agregar que los cyber-delincuentes pueden cometer el sabotaje, chantaje y otros delitos que emana de los programas maliciosos,

como es el mero hecho de la indemnización, demandas por venta de identidad, en razón de que el cyber-delincuente al ingresar al sistema a través de los programas maliciosos, pueden robar información personal del usuario y si nos encontramos ante una empresa, este desencadenas mayores pérdidas económicas, tanto en la restauración del sistema como los posibles daños causados a terceros.

El usuario

Por ultimo como una de las amenazas más "letales" es el mismo usuario ya que como señala (Prakmatic, 2017):

> "El propio personal de la organización podría comprometer la seguridad de los equipos, exempleados descontentos con la empresa que podrían aprovechar las debilidades de un sistema. Juntos a ellos, podemos incluir a los crackers, que se refiere a las personas que intentan obtener acceso no autorizado a los recursos de la red con intención maliciosa y, por supuesto, los hackers o piratas informáticos" (párr.7)

Si bien es cierto es quien manipula y el único que maneja este sistema debemos de tener en cuenta que el usuario es el principal agente que pone en riesgo al sistema informático, ya que este es quien de manera inconsciente o por error acepta los programas maliciosos, es decir que los ciberdelincuentes pueden crear varios programas maliciosos, pero estos no pueden hacer mucho ya que necesitan la aprobación indirecta del usuario para poder ingresar al sistema, por ello estos sujetos inducen a error al usuario para que así estos puedan acceder al sistema.

SEGUNDA DIMENSIÓN: Programas Maliciosos

A. Concepto

Para abordar sobre los programas malicioso haremos mención a lo que dice Arreola (2019) sobre los programas maliciosos:

> “El termino programas maliciosos hace referencia a todos aquellos programas utilizados por los criminales cibernéticos para robar información, dañar dispositivos o hacerse con el control de instalaciones. El termino en inglés se compone de dos palabras: *malicious* y *software*, que juntos significan programas maliciosos. Por eso se dice que el término hace referencia a cualquier programa que tiene como propósito interferir, evitar, destruir o controlar el buen funcionamiento de las computadoras y sus programas” (p. 250)

Estos programas son utilizados por los cyber-delincuentes para poder apropiarse de los datos que posee el usuario para así vender esta información, extorsionar al usuario, alterar la información, suprimir, clonar la información, entre otros delitos con la finalidad de obtener un fin económico o un perjuicio al usuario.

Los programas maliciosos debemos de entender que ataca a todo sistema informático, capaz de almacenar y procesar información, como son los dispositivos móviles, Tablet, computadora y otros dispositivos. por ejemplo, a través de mensajes de textos, llamadas telefónicas, las navegaciones que se realiza a través del celular, todas estas maneras son usadas por los cyber-delincuentes para poder ingresar a la base de datos del usuario y cometer su fin.

B. Tipos de Programas Maliciosos

A esto debemos apreciar que algunos programas maliciosos como son:

El virus

Son unos de los programas que traen un perjuicio al sistema informático para lo cual antes de iniciar vamos a definir que es un virus, según Costas (2006): “Los virus con programas maliciosos creados para manipular el normal funcionamiento de los sistemas,

sin el consentimiento ni conocimiento del usuario" (p. 124) este virus ingresa al sistema operativo del usuario manteniéndolo en error para que así desconozca que su sistema está infectado.

Este virus ataca de la misma manera que lo hace un virus dentro del organismo humano; lo que hace este virus es ingresar al sistema operativo del usuario para que, este sistema no funcione de manera correcta, presentando problemas en su funcionamiento y creando una copia falsa del archivo original, algunos virus pueden destruir, alterar o modificar parcialmente o totalmente un archivo, haciendo imposible su recuperación, pero hay otros que simplemente copian el archivo sin obtener mayor peligro, a estos se les puede aplicar un antivirus, mejorando el sistema y volviéndola segura.

Troyanos:

Mientras que Troyanos, según Sánchez (2016) señala que es un:

> "Método consistente en la inclusión de instrucciones dentro del programa de uso habitual de una rutina para que realice un conjunto de funciones, desde luego no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto. Puede tratarse en determinados casos de la ejecución de cálculos erróneos, por ejemplo: aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir documentos reales, emitir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador. Al igual que la conducta anterior, se trata de una manipulación fraudulenta de

los sistemas o programas informáticos generalmente practicados con fines económicos.” (p. 43)

Los troyanos lleva el mismo que el caballo de Troya que simula ser un programa sano para que así el usuario pueda utilizarlo y cuando este lo ejecuta le da acceso al tercero que pueda manipular el sistema informático, es por ello que este programa muchas veces pasa inadvertido ya que confunde al usuario simulando que es un programa seguro, sin embargo es un mecanismo muy usado por el cyber-delincuente para poder ingresar a la base de datos del usuario sin que este pueda reconocerlo u optar por alguna medida de protección.

Entre sus principales funciones es eliminar los archivos, alterar y copiar la información que tiene el usuario.

Gusanos:

Mientras que los gusanos a diferencia de los demás programas, este presenta difícil configuración, pero una vez que se encuentra configurado su distribución es más fácil ya que además este se multiplica por sí solo, ya no necesita la intervención del tercero.

Keylogger:

Uno de los programas más usados por los cyber-delincuentes es el programa keylogger ya que este programa es comúnmente usado para clonar tarjetas o el robo del dinero a través de esta ya que su principal función es la de registrar la digitalización del teclado, por ejemplo, si un ciberdelincuente infecta un sistema con este programa para que posteriormente grabe las pulsaciones de la tecla, donde el usuario a digitalizado su contraseña, el ciberdelincuente ya posee y tiene registrado la contraseña del usuario, y

con este sustraer todo el dinero que este posee en su tarjeta, o solicitar un crédito. Es decir que este programa graba las contraseñas del usuario.

Trojan-GameThief:

Por ultimo tenemos al programa malicioso Trojan-GameThief quien a través de patrones de juegos ingresa al sistema informático; así como lo señala Sánchez (2016) "Software que roba información de la cuenta de usuario en los juegos en línea." (p.47). En este software se presenta como lo menciona el autor a través de los juegos en línea, que de manera inconsciente el usuario accede a este virus; este puede robar la cuenta del juego o ingresar a la base de datos del usuario, pero esto se manera de manera inconsciente que el usuario no pueda conocer que es un programa malicioso.

C. Prevención de los Programas Maliciosos

Es decir que cada uno de los programas maliciosos son ingresados a través de programas que confunde al usuario suponiendo que es un programa o página seguros, sin embargo, estos ingresan al sistema informático y se mantienen ahí de manera oculta, sin ser captado de manera rápida al cyber-delincuente.

Sin embargo existe varios mecanismos para proteger al usuario de que los agentes puedan introducir algún programa malicioso, como son por ejemplo: evitar realizar descargas de documentos de sitios web de dudosa procedencia, evitar realizar ingresar a páginas que no son seguras, realizar de manera constante la actualización de los dispositivos esto hace que el programa de seguridad sea más adecuada ya que presenta cambio y nuevas metodológicas de protección del sistema, así mismo es recomendable crear siempre una copia de seguridad, también podemos instalar en nuestros dispositivos programas que protegen de cualquier programa malicioso.

Antimalware:

Uno de los programas más usados es el antimalware que es un programa que busca proteger que ningún software malicioso o conocido como malware ingrese al sistema operativo del usuario; así mismo señala (SoftwareLab.org, 2020):

> "El antimalware (anti-malware) es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI. Los términos antivirus y antimalware se utilizan a menudo como sinónimos ya que los virus informáticos son un tipo específico de malware. Por lo tanto, el antivirus y el anti-malware son lo mismo." (párr.2).

Este programa presenta tipos los cuales dependiendo de su uso tiene diferentes aplicaciones, una de ellas es el software antimalware autónomo, según (SoftwareLab.org, 2020) señala:

> "El software antimalware autónomo es una herramienta especializada, diseñada para detectar y eliminar ciertos virus. Se le conoce comúnmente como software antimalware portable porque se puede instalar también en un USB y los administradores los pueden usar para realizar escáneres de emergencia de un sistema infectado. Sin embargo, la mayoría de los programas portables no están diseñados para proporcionar una protección en tiempo real y descargar nuevas definiciones diariamente, que es la razón por la no pueden sustituir los paquetes de seguridad en internet que incluyen una gran variedad de elementos adicionales." (párr.4)

Este antivirus aparenta ser practico debido a su fácil instalación, pero este presenta carencias al momento de poder realizar actualizaciones, ya que en un sistema operativo es indispensable realizar de manera constante las actualizaciones.

Este mismo antivirus cuenta con paquetes de software de seguridad, a lo que según (SoftwareLab.org, 2020) señala:

> "Los paquetes de software de seguridad son más que programas antimalware. Además de ser capaces de detectar y eliminar virus, también están equipados para luchar contra todos los demás softwares maliciosos y proporcionar protección absoluta en todo momento para su ordenador y archivos. La mayoría de estos paquetes de programas incluyen antispyware, cortafuegos (firewall) y componentes de control parental. Algunos también incluyen una función adicional como gestión de contraseñas, VPN (red virtual privada) e incluso un programa antimalware autónomo incorporado en el paquete." (párr.5)

Este programa es de mayor gama, ya que no solo protege el antimalware sino de otros posibles programas maliciosas que pueden atacar al sistema informático, es decir que este programa puede evitar que el cyber-delincuente pueda ingresar al sistema informático del usuario.

Mientras que el software antimalware en la nube, según (SoftwareLab.org, 2020) señala:

> "El software antimalware en la nube es un nuevo tipo de tecnología antimalware que analiza sus archivos en la nube en lugar de en el ordenador, con el fin de liberar sus recursos computacionales y permitir

> una respuesta más rápida. Estos programas se componen normalmente de dos partes; el cliente que está instalado en su ordenador y realiza escáneres periódicos de virus y malware, sin ocupar demasiada memoria y el servicio web que procesa los datos recogidos por el cliente y lo inspecciona en busca de coincidencia con virus y malware de su base de datos." (párr.6)

Este nuevo programa se adecua a las nuevas necesidades de los usuarios, ya que la nueva manera de poder guardar la información del usuario es en la nube, pero este también es susceptible de que un programa malicioso pueda acceder, este programa protege desde la nube los archivos y hace más seguro el uso de este procesador de datos.

TERCERA DIMENSIÓN: Dirección IP

A. Concepto

Para conocer que es una dirección IP es necesario partir de una definición a lo que según Sánchez (2016) señala que:

> "Es un número de cuatro a doce dígitos que identifica a una computadora específica conectada a internet. Los dígitos se organizan en cuatro grupos de números (que pueden ir de 0 a 255) separados por períodos (por ejemplo 1.160.10.230) dependiendo de cómo un ISP (Internet Service Provider: Proveedor de Servicios de Internet) asigna su dirección IP, usted puede tener una misma dirección todo el tiempo o una diferente cada vez que se conecta. Los servidores de Internet tienen el mismo tipo de direcciones, por ejemplo, si colocamos http://216.58.219.110 en nuestro buscador podemos acceder a www.google.com" (p. 37)

Es decir que el IP es como un reconocimiento dactilar de cada persona, no existe dos personas con las mismas huellas; es por ello que esto nos sirve para poder localizar a los ciberdelincuentes, ya que ellos necesitan en primer lugar ingresar al internet para crear un programa malicioso, y el simple hecho de estar conectado a internet hace que este usuario tenga un numero de IP único con el fin de relacionarse con otros, es decir que el IP es necesario para poder comunicarse con otros dispositivos.

B. Tipos de IP

Dirección IP Pública

Esta dirección IP al ser Pública va a varias tanto en su seguridad como en su instalación, pero para conocer que es una dirección IP publica, daremos una definición a lo que según Gavín y Otros (2012) señala:

> "Una dirección IP publica es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente un ordenador) dentro de una red, en este caso el numero identifica tu punto de enlace con internet. Suelen darse dos casos de IP Publica:
>
> Si tienes varios ordenadores conectados en red y a su vez a un router la IP Publica la que tiene el router sea de cable o adsl e independiente de los ordenadores que tengas conectados.
>
> Si por el contrario solo tienes un equipo conectado mediante un modem de cable o adsl, la IP Publica es la que tendrá el ordenador." (párr.3)

Este IP pública hace que cada servidor tenga un IP único para que el usuario pueda navegar en el internet, es decir que este en un reconocimiento que realizada el proveedor para que el usuario pueda navegar con otros dispositivos, a esto debemos de mencionar que cada usuario tiene un IP diferente a los demás por más que se comparta de un mismo

router este va a variar, pueden ser similares, pero jamás pueden ser iguales, no pueden presentar el mismo código.

Ahora este IP ya no es usado como servidor público, sino que se ha sustituido por el servidor de dominio debido a que la búsqueda de servidores a través de los números era difícil de recordar por parte de los usuarios y dificultaba la búsqueda; es por ello que se usó los servidores de dominio. Por ejemplo, si querías buscar información a través de un servidor tenías que colocar el IP imaginemos que este era 187.13.763.232, es difícil de recordar todos estos números, ahora usando los servidores de dominio solo puedes ingresar a través del nombre *Wikipedia.com,* esto es más fácil de recordar y conocerse en el mercado tecnológico.

Estas IP público puedes ser dinámicas o las fijas, en las fijas como el mismo nombre lo señala, este no va a presentar cambio alguno ya que esta es estática; su aplicación es manual y en determinados casos se requiere de un pago adicional para su ejecución.

Este es comúnmente usado y fácil de atacar por parte de los ciberdelincuentes, ya que es estática los ciberdelincuentes se toman su tiempo para poder analizarlo y así quebrantas este IP, es por ello, que si bien es cierto es más fácil de usar ya que es más fácil realizar las descargas y se ayuda de la velocidad con la que esta se realiza; pero es más vulnerable de ser atacados.

Mientras que en el IP dinámico van a ser aquella que constantemente cambia el código de IP, es decir que esta cambia cada vez que el usuario ingresa a internet, esta configuración no es necesaria que el usuario lo realice de manera manual ya que es de manera automática.

Este IP al estar en constante cambio hace imposible que los ciberdelincuentes accedan al IP, haciéndolo más segura y confiable la navegación; pero este presenta problemas en la navegación de internet porque la descarga es más lenta y la navegación por internet es susceptible que pierda conexión.

Dirección IP Privada

Así mismo la dirección IP privada, es un diferente al IP público si bien es cierto no en es tanto en la enumeración, pero si en sus funciones y/o tipos, pero antes de analizar las diferencias debemos de partir de conocer que es una dirección IP privada a lo que según Tapia y Otros (2012) señala:

> "Algunos rangos de direcciones IP han sido reservados para la operación de redes privadas que usan el protocolo IP. Cualquier organización puede usar estas direcciones IP en sus redes privadas sin la necesidad de solicitarlo a algún Registro de Internet. La principal condición establecida para el uso de direcciones IP privadas es que los dispositivos que usen estas direcciones IP no necesiten ser alcanzados desde Internet." (párr.8)

Este IP no es accesible a través del internet, esta podría ser la única diferencia que hay entre una IP pública y privada ya que la finalidad de esta es que existe un operador que divide más señales IP fijas, pero estas IP no son iguales al IP privado, cada dispositivo maneja un similar Ip pero con diferentes códigos. por ejemplo, el IP privado puede ser un router que distribuye internet a los demás dispositivos, el router principal presenta un código IP este al estar compartiendo el mismo acceso con otros tiende a ser similar, pero los otros dispositivos cambiaran uno a dos dígitos en la parte final del código de IP fijo.

Esto no quiere decir que el router principal es igual que el de los otros dispositivos o que presentan el mismo código, más estos se diferencian ya que presentan dígitos diferentes, jamás se repiten el mismo código y este no es detectado por internet.

Ahora este tipo de dirección Ip privada es utilizada por su uso en tres rangos los cuales varían dependiendo de su uso y la seguridad que este va a dar al usuario. Empezaremos hablando del Rango clase A, la cual según Pacheco (2016) señala que:

> "Esta clase es para las redes muy grandes, tales como las de una gran compañía internacional. Del IP con un primer octeto a partir de 0 al 127 son parte de esta clase. Los otros tres octetos son usados para identificar cada anfitrión. Esto significa que hay 126 redes de la clase A con 16,777,214 (2^24 -2) posibles anfitriones para un total de 2,147,483,648 (2^31) direcciones únicas del IP. Las redes de la clase A totalizan la mitad de las direcciones disponibles totales del IP." (párr.3)

Estas son bien utilizadas por empresas multinacionales o de amplia gama, el primer bloque sirve para poder reconocer que tipo de red se está empleando mientras que los otros tres bloques sirven para identificar desde que dispositivo se está realizando la búsqueda.

Por otro lado, los de Rango clase B, según Pacheco (2016) señala:

> "La clase B se utiliza para las redes de tamaño mediano. Un buen ejemplo es un campus grande de la universidad. Las direcciones del IP con un primer octeto a partir del 128 al 191 son parte de esta clase. Las direcciones de la clase B también incluyen el segundo octeto como parte del identificador neto. Utilizan a los otros dos octetos para identificar cada

> anfitrión (host). Esto significa que hay 16,384 (2^14) redes de la clase B con 65,534 (2^16 -2) anfitriones posibles cada uno para un total de 1,073,741,824 (2^30) direcciones únicas del IP. Las redes de la clase B totalizan un cuarto de las direcciones disponibles totales del IP y tienen un primer bit con valor de 1 y un segundo bit con valor de 0 en el primer octeto" (párr.4)

Tomaremos el ejemplo de las universidades, estas presentan un menor digito que el de rango A, ya que ahí trabajamos con tres bloques mientras que aquí trabajamos con 2 bloques, es la misma que el rango de clase A solo disminuye 1 digito al bloque.

Por ultimo uno de los rangos más utilizados es el Rango clase C, a lo que según Pacheco (2016) señala:

> "Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a medianos de tamaño. Las direcciones del IP con un primer octeto a partir del 192 al 223 son parte de esta clase. Las direcciones de la clase C también incluyen a segundos y terceros octetos como parte del identificador neto. Utilizan al último octeto para identificar cada anfitrión. Esto significa que hay 2,097,152 (2^21) redes de la clase C con 256 (2^8 -2) anfitriones posibles cada uno para un total de 536,870,912 (2^29) direcciones únicas del IP. Las redes de la clase C totalizan un octavo de las direcciones disponibles totales del IP. Las redes de la clase C tienen un primer bit con valor de 1, segundo bit con valor de 1 y de un tercer bit con valor de 0 en el primer octeto." (párr.5)

Este rango es el que comúnmente usamos en nuestros hogares a través del router, pero este a pesar de que podría ser un repetidor genera una diferente dirección IP, la cual jamás podrían ser iguales.

VARIABLE DEPENDIENTE: Delitos Informáticos:

A. Concepto

Para abarcar que son los delitos informáticos, señalaremos la definición que Ochoa (2016) señala: "Es toda conducta Típica, Antijurídica y culpable valiéndose de un medio informático, que lesiona un bien Jurídico autónomo" (p. 38) es decir que estos delitos son reprochados por la sociedad y que va en contra las buenas conductas, que el sujeto activo para la realización de su delito necesita realizar a través de un medio tecnológico, por otro lado, según Zarich (2005) señala:

> "Como aquellas conductas disvaliosas socialmente y reprochables desde el punto de vista penal que, concertadas mediante instrumentos y sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tutelados por la ley, en un momento dado" (p. 134)

Estos delitos se van a cometer mediante el empleo de cualquier red informático en vista de que la utilidad de una red informática ha tenido un gran impacto para varias áreas de nuestra sociedad como son en salud, educación, economía, sistema de seguridad y otros, al ser este parte de nuestra sociedad, ha estado en constante avance tecnológico, la delincuencia también ha ido mejorando conforme nuestra sociedad avanza es por eso que a estos delincuentes se les conoce como cibedelincuentes que atacan un sistema informático, sea para robar una identidad, sustraer información privilegiada y/o dañar un sistema operativo todo esto teniendo como eje principal del crimen la obtención de un bien patrimonial (económico).

Afectando el bien jurídico tutelado, así como lo señala Zarich (2005) “El bien jurídico tutelado para este tipo de delitos puede ser cualquiera de los protegidos por el derecho penal, pero entre ellos podemos destacar uno: la propiedad privada.” (p. 134), si bien es cierto el eje principal de los ciberdelincuentes es la adquisición de un patrimonio, pero al querer alcanzar este objetivo se vulneran varios derechos hacia el usuario como son el derecho a la intimidad, a la propiedad privada y otros, atacando de muchas formas al usuario.

Para nuestra realidad social los delitos Informáticos son amplio teniendo como base el Convenio de Budapest, al cual solo se ha adecuado este convenio a nuestra realidad social, la cual no se ve en vista de que el uso de los sistemas informáticos se ha vuelto necesario para cualquier actividad que se realiza.

Pero nuestra legislación no se ha preocupado en poder prevenir y de alguna disminuir los índices que se cometen a través de un sistema informático; en lo cual surge la importancia no solo de poder prevenir el delito o sancionar, sino en el hecho de modificar los articulados que genera vacíos legales al momento de su aplicación a los casos; como es el caso del Fraude Informático el cual no se puede determinar en qué momento se puede determinar que delitos son de resultado y que delitos son de mero hecho.

B. Tipicidad Objetiva

Sujeto Activo:

Así mismo la tipicidad objetiva que se tiene como sujeto activo según Peña (2008) señala que:

> “La descripción en análisis hace inferir que no se requiere cualidad especial alguna para ser considerado autor, basta con que se cuente con ciertos conocimientos propios de la informática para poder realizar la conducta prohibida. Resulta admisible apreciar una autoría mediata, cuando el hombre de atrás se aprovecha de la buena fe del hombre del adelante, del instrumento quien, sin dolo, desconociendo la naturaleza de los actos que está cometiendo, ingresa de forma indebida a una red, o a una base de datos.” (p.482)

Debemos de mencionar que el autor del delito necesariamente debe de ser una persona que tenga conocimiento de informática para así poder manipular los programas que este necesita para cometer su ilícito, por ejemplo, la creación de un programa malicioso y que este tenga los conocimientos de poder infectar el dispositivo.

Ahora también debemos de hablar de una autoría mediata ya que para cometer este delito se emplea la buena fe del usuario para que el hombre de atrás se aproveche de este actuar para poder su ilícito.

En la mayor parte de los delitos informáticos contra el patrimonio el atacante usa la buena fe o el desconocimiento para así cometer su ilícito, incidiéndolo a error. Para que el atacante ingrese a la base de datos del usuario es indispensable que este le otorgue de manera inconsciente o en error para que el atacante ingrese.

Sujeto Pasivo

Mientras que como sujeto pasivo según Peña (2008) señala que:

> “Puede también ser cualquier persona, tanto la persona natural como una persona jurídica, de derecho público o de derecho privado; más si éste se aprovecha el cargo para acceder a la base de datos, se daría la conducta que se encuentra glosada en el artículo 207ª del C.P.” (p.482)

El sujeto pasivo puede ser cualquier persona que maneja un sistema informático, es decir que para que se concurra este delito y que la persona sea víctima de esto es necesario que esta persona se encuentre en el ciberespacio o que maneje cualquier dispositivo informático, en razón de que, si una persona no maneja ningún dispositivo informático, la posibilidad de ser atacado por un ciberdelincuentes es casi nula a excepción de la clonación de tarjetas.

C. Crimen Organizado en Delitos Informáticos

Este delito debido a la era tecnológica en la que vivimos, se ha optado por un crimen organizado en delitos informáticos, para lo que mencionaremos lo que Anarte citado por Hurtado (2016) expresa: “En ese proceso expansivo es que la criminología ha venido reconociendo la utilización cada vez mayor por parte de las organizaciones criminales de la tecnología informática como instrumento de realización de sus actividades delictivas” (p.204)

Conforme las necesidades avanzan las nuevas maneras de poder satisfacer estas necesidades se incrementan a través de los medios tecnológicos, ya que ahora vivimos en una era tecnológica, cada servicio y bien lo podemos conseguir a través de la tecnología, es por ello que esta manera ha sido aprovechada por los ciberdelincuentes.

En razón de que estos delincuentes han mejorado su modus operandi utilizando ahora los medios tecnológicos para obtener su ilícito, haciendo que cualquier persona conocerá de sistemas informáticos pueda cometer estos ilícitos.

A este hecho surge que el ciberdelincuente ya no actué solo, sino que este necesité de más personas conocedoras de informática para poder entre todo este grupo atacar un mercado informático.

D. Tipos de Delitos Informáticos

El espionaje Informático

Estos delitos informáticos debido al uso de la tecnología se pueden presentar de diversas formas una de ellas es el espionaje Informático, a lo que según Herrera (2014) señala que:

> "Estos delitos se refieren principalmente a la obtención (por parte de competidores) del resultado de direcciones de clientes, investigaciones, etc. Son realizados con el ingreso de programas copiadores o por otros métodos (un terminal informático genera una radiación magnética esta puede ser captada y registrada sin mayor complicación hasta cerca de un kilómetro del lugar de la instalación)." (p.102)

Estos delitos son usados con mayor frecuencia para personas que desean conocer los secretos comerciales de otra empresa; por ejemplo, la empresa big cola quiera conocer los ingredientes de la empresa coca-cola conocida a nivel mundial, haciendo que la empresa big cola ingrese a la base de datos de esta empresa para que así este genere el mismo producto y a menor costo, generando un perjuicio económico a la empresa coca-cola.

Por eso decimos que muchas veces este delito sirve para robar información privilegiada del usuario para así poder obtener ganancias económicas, pero este no altera ningún tipo de información o lo manipula, sino que su único fin es conocer los movimientos que este realiza y la información que maneja.

El sabotaje informático

Por otro lado, tenemos al sabotaje informático que según Herrera (2014) señala que:

> "Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema (ejemplo: un programa temporizado que destruye el programa principal o una rutinador cáncer que distorsiona el funcionamiento de aquel mediante instrucciones que se auto reproducen." (p.102)

El sabotaje informático esta direccionado al cambio total o parcial que el infiltrado realiza con la información que tiene el usuario en su sistema informático, este no siempre será con un fin económico de manera directa, sino para poder destruir la competencia empresarial y con este hecho aumentar sus ventas.

E. Consecuencias de los Delitos Informáticos

Si no se opta por ningún mecanismo seguro que proteja al usuario al navegar en el ciberespacio este acarrearía varias consecuencias a lo que según Ius et Praxis (2018) señala que:

> "En lo que atañe a las víctimas de delitos informáticos, es posible distinguir entre consecuencias inmediatas y (más o menos) mediatas de la cibercriminalidad. En ese orden de ideas, los delitos de sabotaje, espionaje y fraude informático tienen una incidencia en diversos intereses de titularidad de la víctima, que se verán afectados según el comportamiento delictivo que se cometa. Tratándose de víctimas que son personas

> naturales, dichos intereses se identificarán, por lo general, con su intimidad o privacidad, o bien con su patrimonio. En el caso de víctimas que son empresas, dichos delitos afectarán, fundamentalmente, intereses patrimoniales. En fin, cuando los delitos informáticos incidan en el funcionamiento del aparato público, se afectarán los diversos ámbitos de actuación en los que interviene el Estado, con la consiguiente afectación de la ciudadanía que (directa o indirectamente) se beneficia de la actividad estatal. Además, tratándose de comportamientos que se cometen a través de internet o del uso de redes computacionales, los delitos informáticos pueden tener consecuencias sobre la funcionalidad de los sistemas informáticos, o sea, sobre aquel conjunto de condiciones que posibilitan que dichos sistemas realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo." (párr.35)

Entre las principales consecuencias que recaería en diversos factores, ya que estos cyber-delincuentes atacan a diversos usuarios, sean personas naturales o personas jurídicas, que se encuentran inmersas en el ciberespacio.

Las afectaciones en las que incurre el atacante se dividen en dos: en la afectación de bienes jurídicos como la privacidad, el patrimonio, entre otros; y otro con menos afectación como la simple introducción de un virus que genera el proceso lento en el procesamiento de datos.

Las empresas que manejan un sistema informático con la finalidad de obtener un rentabilidad económica a través de los medios tecnológicos, son los que están expuestos a sufrir ataques informáticos, como son el sabotaje y espionaje que generan un perjuicio económico a la empresa y prestigio; ya que los atacantes en el sabotaje alterar la

información que maneja dicha empresa, perjudicando a los clientes y a las otras empresas tercerizadoras que ya no van a optar por laborar con una empresa que no sabe proteger sus datos informáticos.

En las personas naturales son vulnerables de que los atacantes busquen la clonación de sus tarjetas, robo de identidad con fines lucrativos, chantaje o amenaza con información privilegiada que maneja el atacante, entre otros.

Estos atacantes su fin no solo es patrimonial también atacan la privacidad y dignidad de los usuarios al observar cada uno de la información que maneja el usuario.

Por todo lo anteriormente señalado es recomendable que el usuario conozca las medidas de seguridad para que así este no sufra ataques por parte del cyber-delincuente y proteja toda la información personal que este maneja, por ejemplo, instalar un antivirus, antimalware, la simple modificación de contraseñas de todos los aplicativos de manera constante, encriptar la información que se maneja.

F. Bien jurídico tutelado

En cada ilícito penal debe de haber un bien jurídico tutelado, a lo que según Gutiérrez citado por Villavicencio (2014) señala que:

> "El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera. Respecto de la información debe ser entendido como el contenido de las bases y/o banco

> 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 del valor económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado" (p. 288).

El bien jurídico tutelado en estos delitos, son diversos en razón de que el cyber-delincuente ataca de diversas maneras y con diferentes intenciones, en las que tenemos como principal delito contra el patrimonio **e**n los delitos contra el patrimonio encontramos, el sabotaje informático, el espionaje informático, el fraude informático, entre otros delitos que cuya finalidad delictiva es la obtención de una ganancia económica a través del engaño que se le induce al usuario.

Para obtener este ilícito debemos de mencionar que la creación de los programas maliciosos con la simple creación y la venta de este ya se estaría consumando su ilícito y que no es necesario llegar al resultado del delito, en razón de que es de mero hecho.

Así mismo en los delitos contra la intimidad, debemos de poner énfasis de que antes de que el atacante ingrese a la base de datos del usuario para obtener un beneficio económico, lo primero que se ataca es la intimidad y la privacidad que maneja el usuario y que el cyber-delincuente utiliza esta información para obtener su beneficio. Por ejemplo, si el atacante quiere robar la información de una empresa al romper la base de seguridad que este maneja, los datos del usuario están a completa disposición del atacante.

Mientras que en la libertad sexual encontramos la pornografía que se puede realizar a través de este medio o incitar a una persona a este tipo de actos, estos delitos ya no son suficiente que se realice a través de la computadora o Tablet, sino que el modus operandi se ha expandido, así como son a través de los mensajes de texto y/o llamadas telefónicas, tal como lo señala la ley 30171 en la que se encuentra abarcado que aquel que

envía a un menor o a cualquier persona mensajes de texto fotos con relevancia pornografía o que a través de llamada incita a la misma son delitos que atenta contra la libertad sexual.

Este delito se relaciona con más bienes jurídicos tutelados, ya que para que el cuándo el cyber-delincuente ataca el dispositivo móvil que maneja el usuario, este en primer lugar debe de atacar la privacidad que este tiene en el celular, es decir que el primer bien jurídico tutelado es la privacidad que el usuario tiene, este se vulnera a través de la simple visualización de los datos del dispositivo, así mismo este podría encontrar fotos comprometedoras o que atente contra la dignidad del usuario, la simple visualización de estas fotos atenta contra su privacidad pero si este se beneficia a través del chantaje al usuario o la distribución de estas fotos con fines lucrativos se vulneran más derechos del usuario.

PRIMERA DIMENSIÓN: Estafa Informática:

Antes de partir por conocer que es la estafa informática debemos de hablar de que es la estafa, a lo que, para Peña, citado por Pérez y Ramírez (2008), señala que:

> "Se trata fundamentalmente del uso del engaño, del abuso de confianza o de procedimientos semejantes que impliquen la elaboración de una determinada maquinación del sujeto activo en contra el patrimonio de otro; en otras palabras, el fraude que emplea el autor, a partir de un sinfín de modalidades, para hacerse de un patrimonio de forma ilícita." (p. 317)

Partiendo de lo citado podemos decir que la estafa es cualquier engaño que realiza el sujeto activo contra el sujeto pasivo para poder obtener un beneficio patrimonial para sí mismo o para un tercero; pero que, este sujeto activo va a generar cualquier medio para inducir a error al sujeto pasivo, en lo que podríamos agregar que de alguna manera engañar al usuario a poder ingresar a un link que ha sido creado con la intención de

sustraer una información privilegiada o que este pueda modificar y/o transformar esta información que tiene el usuario.

En esta definición hubo diversas aportaciones de la cual vamos a poner énfasis en dos direcciones la cual nos habla de la Estafa y la Estafa Informática, el primero según el Código Penal en su artículo 196 nos señala a la Estafa como: "El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, (…)", mientras que la Estafa Informática según Arroyo y Nieto (2006) “La equiparación al engaño de la influencia en el resultado de un sistema de procesamiento de dato (…)” (p. 32).

Podemos decir que estos dos ámbitos tienen dos cosas en común el primero que ambos tienen una final lucrativa y la otra que se recurre al engaño para poder este delito, pero en realidad ambos a ser lo mismo en vista de lo mencionado, solo va a varias el modus operandi y el iter criminis en vista de que, la estafa informática va a tener aporte de la tecnología, pero su naturaleza criminal no ha variado, por ende, estamos hablando del mismo delito, solo con diversas modalidades de cumplir el ilícito.

Es decir que es el mismo delito pero que la estafa informática va a tener apoyo de las redes informáticas para poder consumar su delito.

Para lo cual vamos a definir la estafa informática y cuáles son los elementos típicos para que se configure una estafa informática, lo cual (PORTALEY, 2012) nos señala que:

> “La estafa informática es un fenómeno delictivo que en los últimos años está tomando mayor magnitud y relevancia en el ámbito de la criminalidad informática, siendo éste la base principal del delito informático sobre el

> que gira la ciberdelincuencia. (…). Los elementos típicos que integran el delito de estafa informática son: La manipulación informática y artificio semejante, Transferencia patrimonial no consentida por el titular del mismo, ánimo de lucro, y perjuicio en tercero." (párr. 3)

Para entender mejor lo mencionado por el autor debemos de explicar cada uno de los elementos que se mencionó a lo que referido:

La manipulación informática y artificio semejante

Nos referimos de que este ilícito es necesario que se cometa a través de un medio informático a diferencia de la estafa dicha como tal, en la cual cualquier persona que tenga bastos conocimiento en informática podrá crear, fabricar o alterar un sistema informático ingresando a través de un ordenador, para cometer este ilícito debemos de saber que no estamos ante cualquier delincuente ya que este delincuente necesita tener primero conocimiento avanzados sobre un sistema informático, para poder crear software maliciosos que ingresan a los sistemas tratando de destruir o introducir un virus que genera un perjuicio al usuario.

Otro factor es tener contacto directo con la persona natural o jurídica a quien desea cometer su ilícito, en este caso de manera indirecta se mantiene en contacto con el usuario.

La transferencia patrimonial no consentida por el titular del mismo

Se dará después de que el ciberdelincuente accede a la base de datos y tenga el dominio de toda la información privilegiada que el usuario pudiera tener este ciberdelincuenta hará la simulación de la entrega de un bien económico hacia su persona figurando que el usuario de buena fe le ha realizado una transferencia dineraria, este actuar es un poco difícil de poder encontrar su responsabilidad, ya que, no solo genera un

perjuicio dinerario a la víctima sino a las financieras, ya que se figura una licitud de una transferencia dineraria, el retiro o préstamo dinerario, lo cual induce a error a las entidades financieras las cuales procederán a realizar el proceso correspondiente para no perjudicarse.

En conclusión, podemos decir que es aquella transferencia de un bien económico no consentido por el titular.

Ánimo de lucro

Para estos delitos es importante el ánimo de lucro a lo que según Enciclopedia Jurídica (2020) señala que:

> "Un sector del pensamiento jurídico entiende el ánimo de lucro con laxitud, identificándolo con el propósito de obtener cualquier beneficio de índole material o espiritual, mientras que otro sector doctrinal, más estricto entiende que tal ventaja patrimonial debe consistir en la apropiación de la cosa ajena. La jurisprudencia y la doctrina mayoritaria lo entienden en sentido amplio, como animus lucri faciendi gratia (…)" (párr. 3)

Todo el iter criminis que realizan los cyber-delincuentes es con la finalidad de generar un bien económico para sí mismo o para un tercero.

Es decir que el móvil con la que realiza el cyber-delincuente es la obtención de una ganancia económica, a ello debemos mencionar que el simple hecho de crear un programa de espionaje sin ejecutarlo también estaría consumado el delito de estafa informática, aunque para la estafa informática no es necesario la utilización de programas maliciosos sino inducir a error al usuario a través del medio tecnológico.

Perjuicio en tercero

Por ultimo tenemos el elemento de generar un perjuicio a un tercero, manteniéndolo en error o en engañar al usuario para poder ingresar a su operador y

manipular los datos privilegiados que este puede acceder, esto se tiene que dar a través de cualquier medio tecnológico ya que caso contrario solo podría ser considerado como una estafa.

SEGUNDA DIMENSIÓN: Derecho a la Intimidad Informática

El derecho a la intimidad es un derecho fundamental que toda persona sujeta a derecho ejerce, este derecho se encuentra protegido en la Constitución Política del Perú en el artículo 2 inciso 7 menciona que: "Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y la imagen propia (…)" (p. 10); así mismo en el inciso 7 artículo 2 de la Constitución Política del Perú señala que: "El secreto y a la inviolabilidad de sus comunicaciones y documentos privados(…)" (p.10) es decir que toda persona tiene el derecho a su intimidad, respetando su honor, en la que tampoco se puede agraviar este derecho mediante la violación a través de las comunicaciones, pero cuando hablamos de derecho a la intimidad informática nos referimos a la protección de este derecho en el ciberespacio, es decir que se protege este derecho a través de cualquier medio tecnológico de telecomunicación, para lo cual es necesario dar una definición del derecho a la Intimidad a los que Rebollo citado por Ruiz (2005) señala que:

> "a) Es un derecho universal porque pertenece a todos los hombres; es innato, inherente a la persona, corresponde a su titular por el solo hecho de ser persona, y acompaña a todo hombre desde su nacimiento hasta incluso después de su fallecimiento; b) es individual porque se reconoce a favor de casa persona individualmente considerada; protege al sujeto en lo que es (con su entorno físico, psíquico y moral) o en lo que puede ser. Se configura para establecer un ámbito en el que el individuo es soberano; c) es un derecho inviolable, que no puede ser negado por los otros; es ejercitable erga omnes, frente a las personas o instituciones. Eso no quiere

> decir que sea un derecho ilimitado, ya que, en determinadas circunstancias, podría ceder ante otro interés más relevante; d) decimos que el derecho a la intimidad es inalienable porque no está sujeto a prestación o renuncia, no puede extinguirse por voluntad abdicativa de su titular, ni se puede renunciar a él de forma total; en este sentido es también extramatrimonial porque no se puede comerciar con él; e) por último, se trata de un derecho imprescriptible, pues al ser inherente a la persona , no cabe posibilidad de que el derecho se extinga" (p. 262)

En las redes sociales lo que se protege es la privacidad que tienen los usuarios, a lo cual tenemos que mencionar la diferencia que hay entre la intimidad y la privacidad, a lo que Herrán (2002) señala:

> "De las posibles objeciones que pueden plantearse a las manifestaciones contenidas en este texto, destacar dos: por un lado, si como se afirma por el legislador la "privacidad" constituye un conjunto más amplio y global de aspectos de la persona, ningún obstáculo puede impedir considerar incluido en el mismo aquellos aspecto más interiores y próximos a la persona; por otro lado, no puede afirmarse sin pecar de simplicidad que la intimidad ya está suficientemente protegida por el ordenamiento jurídico, mientras que la privacidad puede verse agredida por la utilización de medios informáticos. Así, también la esfera más íntima y personal del individuo es susceptible de agresión informática, aunque nos es frecuente y, en consecuencia, debe ampararse por mínima que sean las injerencias, precisamente porque en él se reconoce el baluarte principal de la dignidad y personalidad humana, el derecho al respeto de su esfera íntima." (p. 43)

Si bien es cierto el derecho a la intimidad de alguna manera se puede proteger con los softwares de seguridad informática que podemos adquirirlo de manera gratis o poder comprar uno de los softwares, entre las cuales tenemos: antispyware, firewall, antimalware y otros, para así evitar que cualquier persona pueda ingresar al ordenador de las personas que poseen un sistema informático.

Pero estos solo van a proteger el software lógico, es decir que van a proteger información privilegia o personal, evitando que pueda ingresar un virus a tu laptop, computadora o Tablet, mediante anuncios que te informan que dichas paginas a las cuales accedes tienen de alguna manera un virus malicioso.

Al tener instalado estos softwares no podría quebrantarse de ninguna manera esta seguridad y así evitar que puedan ingresar a nuestra base de datos, pero estos no te protegen de que cualquier persona a través de las redes sociales puedan ingresar a tus cuentas a través de spams, las cuales cualquier persona con bastos conocimiento en red lo pueden crear o aplicar; es por ello que surge la interrogante de ¿Cómo proteger mi información no solo en mi operador sino en mis redes sociales y si el Estado de alguna manera controla el adecuado funcionamiento de las redes sociales?.

Ante esta interrogante podemos decir que en si el Estado no supervisa el adecuado funcionamiento de las redes sociales ya que eso, es responsabilidad del creador de dicha aplicación, las cuales al momento de crear una cuenta en las redes sociales en el aplicativo, el usuario otorga permiso y este se sujeta a las políticas que tiene esta aplicación, pero en realidad se otorga el permiso de que tengan acceso a tu información, lógicamente no se podría usar para fines ilícito pero sí que te direccionan a otras aplicaciones que podrían interesarte, vulnerando de esta manera tu derecho a la intimidad y protección de los datos personales, en vista de que esta aplicación a vendido tus datos

como usuario para que puedas acceder a otros aplicativos los cuales no has solicitado información. No solo de esta manera se puede vulnerar nuestro derecho a la privacidad.

Si bien es cierto algunas aplicaciones te dan la opción de proteger tus datos personales en la aplicación, estos datos en la mayor parte del tiempo están a facultad del usuario proteger sus datos personales o mantenerlos de manera pública, donde cualquier persona pueda acceder a estos datos, es por ello que estos posibles delitos de Estafa o Fraude Informático recaen en responsabilidad del usuario ya que en realidad es decisión del usuario proteger o no estos datos personales las cuales se pueden sustraer, pero no solo por el simple hecho de mantener en público tus datos personales pueden sustraer un bien ilícito, ya que eso sería una de las fases del *iter criminis* por lo que su fin no es la sustracción de tus datos personales sino el fin ilícito que se puede llegar a conseguir con este como son la clonación de datos personales, vender tus datos personales para poder obtener un fin económico con este dato personal.

Este ilícito de vender un dato personal acarrea otro conflicto aun mayor de poder mediar responsabilidad penal al autor del delito ya que, al vender tus datos personales los cyber-delincuentes pueden crear varias cuentas falsas con una dirección bloqueada o difícil de rastrear, con la finalidad de inducir a error a otras personas que optan por confiar en la página web creada con los datos sustraídos, y sufrir de algún Fraude o Estafa Informática. Todo este actuar en las redes sociales no está sancionado legalmente, si bien es cierto va en contra de las buenas conductas del aplicativo la cual te sanciona, pero se deja de lado la integridad de la persona, la cual pudo a ver sufrido alguna extorsión por que el cyber-delincuente posee una información privilegiada.

En todos los delitos que podría acarrear se deja de lado el hecho de que los cyber-delincuentes, lo primero que han quebrantado contra las víctimas fue su derecho a la

intimidad y privacidad, en la cual han accedido no solo a los datos personales sino al acceso de fotos, videos, documentos, conversaciones y otros con la finalidad de cometer su ilícito, pero no solo pueden conocer esta información privilegiada, sino que lo pueden usar en contra de la víctima, la cual puede generar otros delitos como el chantaje o extorsión, incluso pueden dañar la dignidad que una persona tiene con el solo hecho de mal utilizar estos datos informáticos, generando un perjuicio moral a la víctima.

La única manera de proteger nuestros datos informáticos recae en nuestra responsabilidad ya que en realidad por más que el ciberdelincuente tenga un virus malicioso es indispensable que el usuario le dé la luz verde de poder acceder a la base de datos ya que somos los usuarios que de manera inconsciente le damos las facilidades de que a través de un software malicioso ingrese a nuestra base de datos y pueda sustraer, modificar o alterar información privilegiada. Por ejemplo, el cyber-delincuente puede crear una página de lo que más nos interesa para así captar nuestra atención, para posteriormente indicarnos que debemos de dar un clic a su página para más información, pero de manera inconsciente al dar ese clic ya estamos permitiendo que el cyber-delincuente pueda introducir este software malicioso, es por eso que el primer factor que tenemos que tener en cuenta es saber manejar adecuadamente los sistemas informáticos.

Podríamos decir que cometer un ilícito a través de una red social es más fácil en razón que, no se tiene un control de si, efectivamente las personas crean sus cuentas en estas redes con sus datos reales ya que en estas redes sociales puedes crear un usuario con nombre ficticios y estos no están supervisados por las autoridades ya que solo regula con las conducta que señala el creador del aplicativo, dejando a libertad a los cyber-delincuente de crear cuentas falsas o clonar cuentas de los usuarios acarreando diversos ilícitos.

TERCERA DIMENSIÓN: Fraude Informático

A. Concepto

El fraude informático lo vamos a encontrar en la ley 30171 en su artículo 8º en donde nos manifiesta lo siguiente:

> "El que deliberadamente e ilegalmente procura para sí o para otro un provecho ilícito en perjuicio de un 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 pena privativa (…)" (párr. 8).

Este artículo guarda relación con el convenio de Budapest en su artículo 8 en la que señala que:

> "(…) a) La introducción, alteración, borrado o supresión de datos informáticos; b) Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona" (p. 6)

Ha este convenido el Perú se ha adherido con Resolución Legislativa Nº 30913 el 13 de febrero del 2019, pero en dicho convenio no se ha unido el articulo 8 en la que refiere sobre el fraude informático por ello, nos deja solo la ley 30171 en la se presenta vacíos de interpretación, así como lo señala Villavicencio (2014) menciona que:

> "(…)un beneficio para sí o para otro en perjuicio de tercero; y por la forma como esta estructura (apropósito de la mala redacción que genera mucha confusión al momento de interpretar la figura, y las conductas inadecuadas como "diseñar, introducir, alterar, borrar y suprimir" que no encajan en el delito de fraude informático; estas conductas son propios del delito de daño) se clasifica como un delito de resultado porque no basta cumplir con el tipo penal para que se consuma 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." (p. 297).

A lo que podemos decir que al tipificar la ley no ha tenido en consideración en que momento podríamos hablar de una tentativa y en qué momento se dará la consumación del delito, además de que las conductas de "diseñar, introducir, alterar, borrar y suprimir" son hechos de resultados es decir que es indispensable que se realice este hecho caso contrario no estaríamos hablando de un delito y es el principal mecanismo para poder consumar el delito o poder llegar a la finalidad de obtener una ganancia económica por ende este hecho no se estaría configurando en un hecho de resultado.

Mientras que según Gutiérrez (1991) Señala que el fraude informático es:

> "(…) El fenómeno de mayor magnitud y trascendencia en el ámbito de la criminalidad mediante computadoras (…)" (p. 87). Al respecto Villavicencio (2014) señala que "Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, el internet, etcétera; sin embargo, esta forma de criminalidad no solo son

> instrumentos que facilitan, pero no determinan la comisión de estos delitos (…)" (p. 286).

De lo citado podemos partir de dos interpretaciones sobre el Fraude Informático: El primero, interpretarlo como aquel ilícito que es cometido mediante el uso de la tecnología que facilita la consumación de la misma o es una modalidad de cometer el ilícito, por ende podemos decir que este delito ya se encuentra tipificado en el Código Penal pero que ciertos delitos van a tener un apoyo de la tecnología o que se va a realizar por este medio pero teniendo como resultado el primer delito que se quería consumar; estos casos se dan con mayor frecuencia en delitos contra el patrimonio como el hurto, el robo o la estafa en vista de que la sustracción de un patrimonio es el principal objetivo criminal pero que, para poder consumar este delito en determinados casos se va a tener que necesitar el apoyo tecnológico pero que en realidad su objetivo es la sustracción del bien mas no la apropiación de un sistema operativo.

Mientras que la segunda manera es cometer el ilícito dentro de un sistema informático o alterar las mismas, es decir que estos delitos deben de estar basadas desde su origen al ilícito criminal dentro de estos sistemas como lo es la introducción de un software de espionaje, aplicativos que destruyan total o parcialmente un sistema operativo, generalmente para realizar este delito usan un sistema operativo de software libre Kaly Linux que contiene herramientas que si bien son de mucha utilidad positiva en manos equivocadas son para realizar actos delincuenciales entre esas herramientas tenemos las siguientes: Wireshark, Zenmap, Oswap ZAP, Armitage, Suite aircrack-ng, etc.

Ahora según Sánchez (2016) señala:

> "En este caso las acciones típicas buscan conseguir un beneficio para sí o para otro en perjuicio de tercero, se clasifican como un delito de resultado, requiere el cumplir con el tipo penal y seguida de un resultado que consiste en causar un perjuicio a un tercero, sino el delito quedará en grado de tentativa". (p. 76)

Por lo cual, de este artículo debemos de saber que delitos necesariamente deben de ser de mero hecho y cuales son de resultado ya que no todos los delitos que señala el artículo 8 de la ley 30171 son delitos de resultado, en razón de que algunos con la simple creación de un software es decir de hecho han conseguido su propósito, demostrando así que no se necesita acabar el delito, sino que depende de la utilidad que esta le da para que se configure como delito.

B. El fraude informático y el hurto

Para explicar porque hablamos del hurto y el fraude informático debemos de dar una definición de cada uno de ellos, por lo que según Gutiérrez (1991) Señala que el fraude informático es: "(…) El fenómeno de mayor magnitud y trascendencia en el ámbito de la criminalidad mediante computadoras (…)" (p. 87), es decir que el fraude informático es aquel daño que se realiza a través de un sistema informático, mientras que el hurto es según Westreicher (2020): "El hurto es la apropiación de propiedad ajena sin consentimiento, pero sin tener que recurrir al uso de la fuerza o a la amenaza de violencia." (párr.1), a lo mencionado no podemos encontrar ningún vínculo o nexo entre sí, ya que ambos son diferentes delitos y el ámbito de aplicación de la criminalidad es diferente. A este punto Mayer y Oliver (2020) señala que:

> “En ese sentido, en materia de criminalidad informática, si es que se alude al hurto, por lo general no es para referir la apropiación de especies muebles ajenas sin la voluntad del dueño y con ánimo de lucro (artículo 432 del Código Penal), sino para dar cuenta de la usurpación de nombre (artículo 214 del Código Penal) o de la suplantación de identidad.” (p.165)

En este sentido podemos ver de qué, hay delitos de los cuales se puede relacionar, no estrictamente como delitos contra el patrimonio sino la apropiación de datos personales, como es el nombre del usuario, copia de las informaciones, secretos comerciales, entre otros.

En este panorama podemos decir que el hurto es la mera apropiación de una información que de manera que el usuario no se dé cuenta de la sustracción de esta información, es decir que el usuario jamás se entera que el atacante ha sustraído alguna información, ya que tampoco este implica la violencia con la que ingresa a la base de datos o con la que debe de sustraer dicha información.

Sobre la fuerza física Etcheberry citado por Mayer y Oliver (2020) señala que:

> “En específico, se sostiene que en los delitos de apropiación por medios materiales se requiere el empleo de energía física para concretar la apropiación” (p.166) a esto también debemos de mencionar sobre los delitos de apropiación de objetos inmateriales Aguilar citado por Mayer y Oliver (2020): “mientras que en los delitos de apropiación por medios inmateriales lo que hay es el uso de mecanismos preferentemente intelectuales” (p. 166)

En referencia a la imposición de la fuerza física que se emplea es menester mencionar que en la apropiación de bienes materiales es indispensable el uso de la fuerza,

mientras que, en la apropiación de bienes inmateriales, no es necesario y no se podría presenciar, pero esta fuerza no es de manera física contra el usuario sino la fuerza con la que se emplea es un ataque contra la seguridad o el sistema informático de cada dispositivo que maneja el usuario.

Esta fuerza está destinada a la que de manera el ciberdelincuente rompe las medidas de seguridad, en este caso no es necesario la cooperación del usuario, sino que de manera violenta el ciberdelincuente ataca el sistema informático.

En la relación que el atacante realiza con la imposición de la violencia al sistema informático podemos estar hablando del robo, en razón de que se emplea a través de la fuerza no física sino de una violencia contra la seguridad informática que maneja el usuario

1.2. Marco conceptual

Agravio material. - El que recae sobre la integridad física o el patrimonio de una persona, como consecuencia de un acto ilícito, civil o penal, realizado por otra persona, que queda obligada a la reparación del daño causado.

Bien inmaterial. - El que no cae generalmente bajo la apreciación de los sentidos; así, los derechos establecidos sobre los objetos materiales. Representa lo contrario de bien corporal (v.).

Buena fe. - La buena fe impone el deber de lealtad recíproca en las negociaciones. Es la lealtad en el tratar, el proceder honrado y leal; el guardar la fidelidad a la palabra dada y no defraudar la confianza ni abusar de ella.

Criminalidad. - Calidad o circunstancia que hace que una acción sea criminosa.

Datos informáticos. - Se entenderá toda la representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluido los programas diseñados para que un sistema informático ejecute una función.

Intimidad. - Podría considerarse a la intimidad como la antítesis de lo público: por tanto, todo aquello relativo al hogar, la familia, la religión, la salud, la sexualidad y los asuntos legales y económicos personales de un individuo. Pero, el individuo es miembro de la sociedad y como tal no puede pretender disfrutar de una intimidad total. La formulación "el derecho a que uno le dejen en paz" resulta demasiado simplista.

Software. - Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

3.3.Marco legal o formal

Constitución Política del Perú

La presente investigación con respecto a la dimensión del derecho a la intimidad guarda relación con el artículo 2 inciso 7 y 10 de la Constitución Política del Perú.

En la que, se consideró que este derecho está protegido dentro de la ley de leyes de la Constitución Política, la misma que se estudió dentro de la investigación que se realizó.

Convenio de Budapest

En la presente investigación con respecto a la dimensión del Fraude Informático guarda relación con el artículo 8 del Convenio sobre la Ciberdelincuencia en Budapest.

En la que se consideró que, en el convenio de Budapest, nos ha delimitado de buena manera el fraude informático la cual no se realizó en nuestra legislación

Ley 30171 sobre los delitos informáticos

En la presente investigación con respecto a la dimensión del Fraude Informático guarda relación con el artículo 8 de la ley 30171 sobre los delitos informáticos.

En la que, se consideró que está conducta está regulada en la mencionada ley, la misma que se estudió dentro de la investigación que se realizó.

Código Penal Peruano

La presente investigación con respecto a la dimensión de estafa informática guarda relación con el artículo 196 del Código Penal Peruano.

En la que, se consideró que este artículo está estrechamente vinculado con el delito de estafa tipificado en el Código Penal Peruano, la misma que se estudió dentro de la investigación que se realizó.

CAPITULO IV

MÉTODOLOGÍA DE LA INVESTIGACIÓN

4.1. Métodos de investigación

Métodos generales

El método que se empleó en la presente investigación fue el método Deductivo-inductivo, ya que se va a partir del aspecto general de los delitos informáticos para llegar a términos más delimitados; a ello daremos una definición de cada uno de estos métodos:

Ander (1992) señala que el método deductivo: “Este tipo de investigación se basa en el estudio de la realidad y la búsqueda de verificación o falsedad de unas premisas básicas a comprobar. A partir de la ley general se considera que ocurrirá en una situación particular.” (párr.15) mientras que el método inductivo según Ander: “(…) se basa en la obtención de conclusiones a partir de la observación de hechos. La observación y análisis permiten extraer conclusiones más o menos verdaderas, pero no permite establecer generalizaciones o predicciones.” (párr.16)

El método deductivo se utilizó en el extremo que, lo Delitos informáticos es un tema amplio de la cual se ha partido analizando mediante la observación ya que para ser considerado delitos informáticos debemos de determinar que delitos afectan al patrimonio y a la intimidad del usuario, es por ello que se desgloso cada delito y cuáles son los acciones que esta comprende para ser calificado como delito informático para así no incurrir en un error de conceptualización ni de interpretación legal; así mismo se utilizó el método inductivo debido a que la inseguridad informática es cada vez mayor por parte de los usuarios es por ello que con mediante esta variable se pueda encontrar mecanismos preventivos contra los Delitos Informáticos.

Método especifico

El método que se empleó en la presente investigación fue el método explicativo debido a que se van a explicar las causas que desencadeno el problema de investigación, a ello mencionamos lo que dice Caballero citado por Montero y De la Cruz (2016):

"Es aquella orientación que, además de considerar la respuesta al ¿Cómo?, se centra en responder a la pregunta ¿Cuáles son las causas?; lo que implica plantear una Hipótesis explicativa; y, un diseño explicativo" (p. 114)

Este método si bien es cierto partió de una realidad social que en ciertos casos mediante la inseguridad informática que presenta el usuario se han desencadenado diversas causas que pone vulnerable al usuario y que en determinados delitos informáticos aún no se da una solución legal que sea favorable para el sujeto pasivo por eso los Delitos Informáticos nos ayudó a identificar cuáles son las causas que desencadena este ilícito para que así se encuentren las posibles soluciones que se pueden dar para prevenir y controlar estos delitos.

Métodos particulares

El método que se empleó en la presente investigación fue el método sistemático, debido a que; a lo que según Ramos citado por Montero y De la Cruz (2016) señala que:

"Consiste en determinar qué quiere decir una norma, atribuyéndole los principios o conceptos que están descritos con mayor claridad en otras normas, pero que no están claramente expresados en el texto normativo que se quiere interpretar" (p. 115)

Se utilizó este método debido a que en los delitos informáticos tipificado en la Ley 30171, nos basaremos en el artículo 8ª, muestra ambigüedad al momento de interpretarla, ya que, no explica en que, momento nos referimos a un delito de mero hecho y que delito son de resultados, así mismo en los delitos informáticos no se determina que delitos se configura una tentativa y cuando hablamos de una consumación del delito; así mismo se transcribe el mismo tipo legal consignado en el código penal en su artículo 196 tipificado como Estafa, es por ello que al momento de interpretarla induce a error al legislador, en razón de que al momento de tipificar esta Ley se acogió al convenio de BUDAPEST donde cada Estado podía adecuar este convenio a la legislación que considere adecuado para cada Estado, pero nuestro Estado lo une dos artículos, como es el Fraude Informático y la Estafa Informática; dando como resultado la ambigüedad de la menciona ley y en lo referido al derecho a la intimidad, lo dejan de lado en razón de que solo analizan el aspecto de la libertad sexual.

4.2. Tipos de investigación

El tipo de investigación que se empleó en la presente investigación, según su profundad fue el explicativo debido a que se han descubierto las razones por la que la inseguridad informática influye en los delitos informáticos, a ello mencionamos que según Montero y De la Cruz (2016) señala que: "Consiste en explicar un problema con la

finalidad de descubrir las causas, factores y como estos están afectando la concurrencia de ora variable" (p. 122)

Se utilizó el mencionado tipo de investigación, debido a la inseguridad informática que se presenta, se han configurado los delitos informáticos con mayor influencia, pero en la mayor parte que genera esta inseguridad informática, son los mismos usuarios que de manera inconsciente o inducidos en error por parte del ciberdelincuente, colaborar con la consumación de los delitos informáticos en los delitos de resultado.

4.3.Niveles de investigación

El nivel que se utilizó en la presente investigación fue el nivel explicativo, en razón de que se ha explicado las causales que ha desencadenado para que la inseguridad informática tenga repercusiones en los delitos informáticos; de este nivel nos basamos a lo mencionado por:

> Según Montero y De la Cruz (2016) señala que: "Lo que se pretende en este nivel de investigación es aclarar, definir, interpretar el de como una variable independiente afecto, incidió, influyo en la variable dependiente, es decir la variable dependiente ya ocurrió, o está ocurriendo, por lo tanto, los datos empíricos permitirán la comparación de la hipótesis planteada" (p. 131)

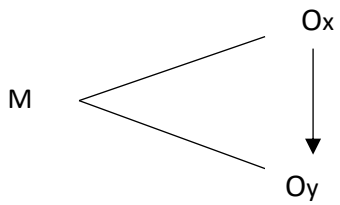
Se utilizó este nivel debido a que, se explicó, las razones por las cuales se quebrante la Inseguridad Informática del Usuario que afecta de manera considerativa en los Delitos Informáticos ya que los usuarios no tienen un adecuado uso de sus datos informáticos o estos se encuentran a la libre disposición de los ciberdelincuentes, la cual facilita a estos a cometer el ilícito.

4.4. Diseño de la investigación

El diseño que se utilizó en la presenta investigación fue el diseño no experimental porque en toda la investigación ninguna variable de estudio ha sufrido cambios o alteración para poder llegar a una conclusión; a ello según Montero y De la Cruz (2016) señala que: "Consiste en realizar el estudio de la variable o variables de investigación sin la necesidad de manipular o condicionar para el efecto de la variable" (p.137)

Se utilizó este diseño en razón de que la variable dependiente e independiente en el transcurso de la investigación no sufrió cambios o se realizó experimentos; por otro lado, como variable independiente tenemos a la Inseguridad Informática del y como variable dependiente a los Delitos Informático, estas se analizaron tal como se presenta en nuestra realidad sin sufrir cambio alguno.

Así mismo como tipo de diseño no experimental transeccional o transversal se empleó el diseño explicativo, ya que se determinó la influencia que tiene la inseguridad informática con los delitos informáticos; para lo cual según Montero y De la Cruz (2016) señala que: "Este tipo de diseño permite hacer un estudio sobre la relación de causa-efecto existe una y otra variable, a fin de determinar la incidencia e influencia de la variable independiente sobre la variable dependiente" (p.140)



M: Muestra de estudio.

Ox: Inseguridad Informática

Oy: Delitos Informáticos.

Se utilizó este diseño ya que nos permitió determinar la influencia que la inseguridad Informática tiene frente a los Delitos Informáticos.

4.5. Población y muestra

4.5.1. Población

En la presente investigación la población que se ha tomado fue en la Fiscalía Corporativa de Huancayo, a lo que según Montero y De la Cruz (2016) señala que la muestra:

> "Es el conjunto de elementos que tienen características comunes y que integra el objeto de estudio, susceptible de observación o mediación" (p.143)

Por lo cual, en la presente investigación debido a su clasificación, la población fue finita ya que se contó con 72 fiscales correspondientes a la Fiscalía Provincial Penal Corporativa de Huancayo, en la que se ha analizado la influencia en que recae la inseguridad informática con los delitos informáticos.

4.5.2. Muestra

La muestra que se utilizó en la presente investigación fue el muestreo no probabilístico por conveniencia a lo que se señala que según Creswell citado por Vicente y Figueroa (2011):

Lo define como un procedimiento de muestreo cuantitativo en el que el investigador selecciona a los participantes, ya que están dispuestos y están disponibles para ser estudiados" (párr. 1)

Teniendo como muestra: 6 fiscales quienes equivalen a 1 fiscal por cada una de dependencias de la Fiscalía Provincial Penal Corporativa de Huancayo.

.6. Técnicas e instrumentos de recolección de datos

.6.1. Técnicas de Recolección de datos

Según Montero y De la Cruz (2016) señala que: "Las técnicas vienen a ser el conjunto de procedimientos o recursos que se usan a fin de viabilizar y operativizar los métodos y lograr el objetivo propuesto en la investigación científica, mediante la recopilación de datos o informaciones" (p. 155)

ENCUESTA

Según García citado por Montero y De la Cruz (2016) señala que: "Una encuesta sirve para recopilar datos, como conocimientos, ideas y opiniones de grupos; aspectos que analizan con el propósito de determinar rasgos de la persona, proponer o establecer relaciones entre las características de los sujetos, lugares y situaciones o hechos" (p.162)

En la presente investigación se utilizó los 6 fiscales de la Fiscalía Provincial Penal Corporativa de Huancayo, sobre los delitos informáticos con el propósito de determinar la influencia de la inseguridad informática en los delitos informáticos, así mismo si la tipificación de Fraude Informático contemplado en el artículo 8 de la ley 30171 esta formulado de forma clara y precisa.

.6.2. Instrumentos de Recolección de Datos

CUESTIONARIO

Según por Montero y De la Cruz (2016) señala que: "Es una técnica que consiste en un conjunto de preguntas escritas con el cual se obtiene información por escrito de las opiniones de los sujetos de la muestra de estudio, como respuesta a las preguntas planteadas (…)" (p. 173).

En la presente investigación se utilizará el cuestionario para los fiscales de la Fiscalía Provincial Penal Corporativa de Huancayo, con el propósito de conocer la

influencia de la inseguridad informática en los delitos informáticos, así mismo si en los casos que los usuarios han sufrido un fraude informático han sido vulnerados sus derechos a la intimidad y por último para ver si los usuarios de manera inconsciente facilitaron de alguna manera la consumación del delito.

4.7. Técnicas de procesamiento y análisis de datos

En la técnica de procesamiento de datos, la presente investigación utilizará el programa SPSS versión 25 para poder procesar los datos obtenidos del cuestionario realizado, luego se realizará las tablas de distribución de frecuencia y los gráficos estadísticos, prosiguiendo se realizará el análisis e interpretación conforme a las preguntas realizadas en la ficha de observación el cual se obtuvo de la Fiscalía Provincial Penal Corporativa de Huancayo, para así poder respaldar nuestra posición planteada en nuestra hipótesis.

4.8. Aspectos éticos de la Investigación

- En la presente investigación, los datos obtenidos no han sido alterados.
- En la aplicación de la encuesta realizada a los fiscales provenientes de la Fiscalía Provincial Penal Corporativa De Huancayo, se les ha comunicado sobre el consentimiento informado, así mismo se puede observar en los anexos.

CAPITULO V

RESULTADOS

4.1. Presentación de Resultados

A continuación, presentare los resultados obtenidos de la encuesta realizada en la Fiscalía Provincial Penal Corporativa de Huancayo

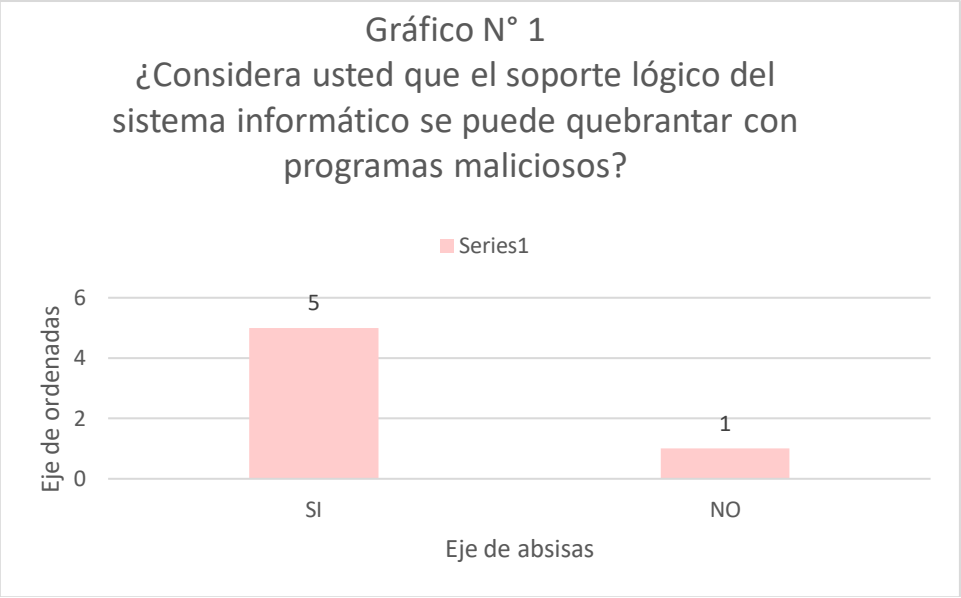
1. **¿Considera usted que el soporte lógico del sistema informático se puede quebrantar con programas maliciosos?**

TABLA N° 1

¿Considera usted que el soporte lógico del sistema informático se puede quebrantar con programas maliciosos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7
	SI	5	83,3	83,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que el soporte lógico del sistema informático si se quebranta con programas maliciosos y el 16,7% considera que el soporte lógico del sistema informático no se quebranta con programas maliciosos.

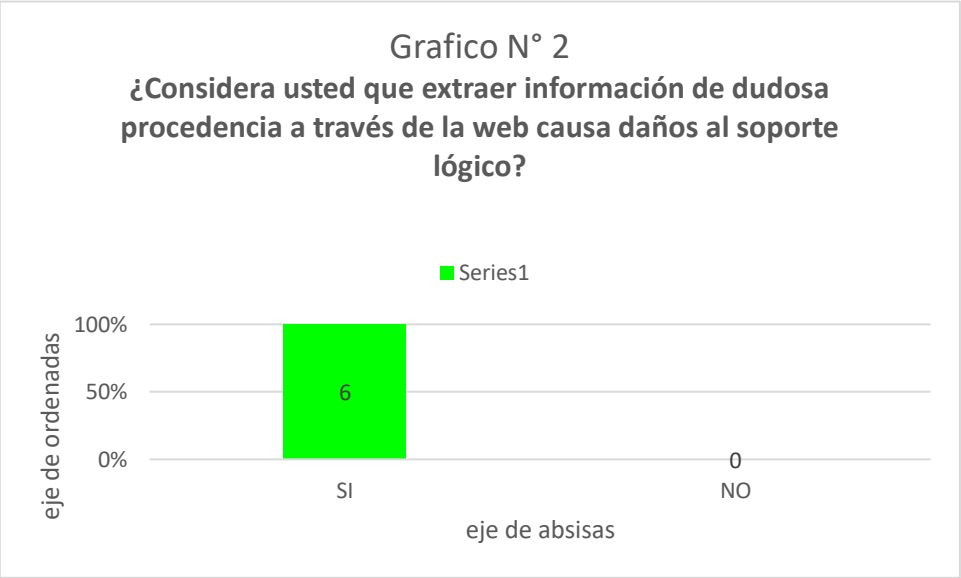
2. **¿Considera usted que extraer información de dudosa procedencia a través de la web causa daños al soporte lógico?**

TABLA N° 2

¿Considera usted que extraer información de dudosa procedencia a través de la web causa daños al soporte lógico?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	6	100,0	100,0	100,0

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que extraer información de dudosa procedencia a través de la web causa daños al soporte lógico y el 0% considera que extraer información de dudosa procedencia a través de la web no causa daños al soporte lógico.

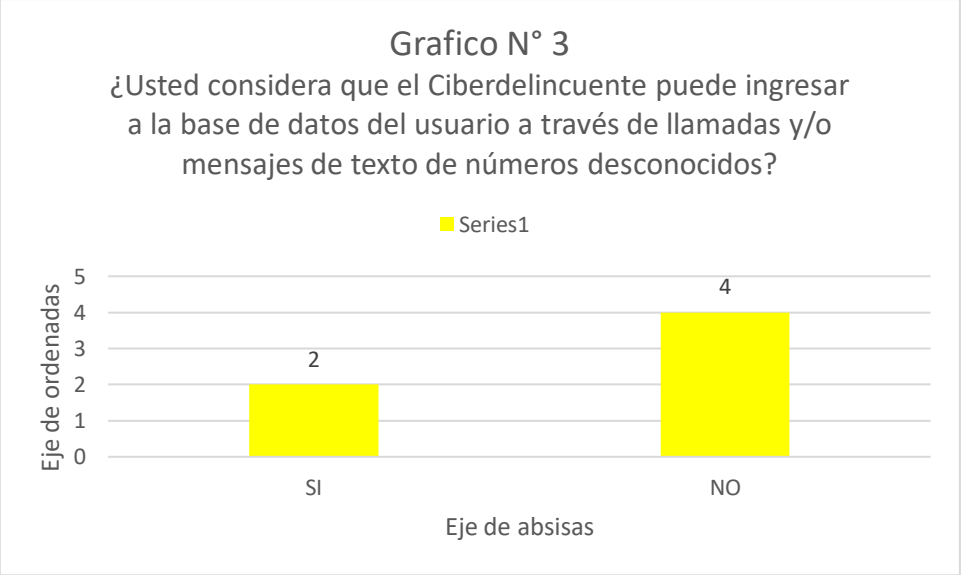
3. **¿Usted considera que el Ciberdelincuente puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos?**

TABLA N° 3

¿Usted considera que el Ciberdelincuente puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	4	66,7	66,7	66,7
	SI	2	33,3	33,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 33,3% considera que el Ciberdelincuente si puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos, mientras que el 66,7% considera que el Ciberdelincuente no puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos.

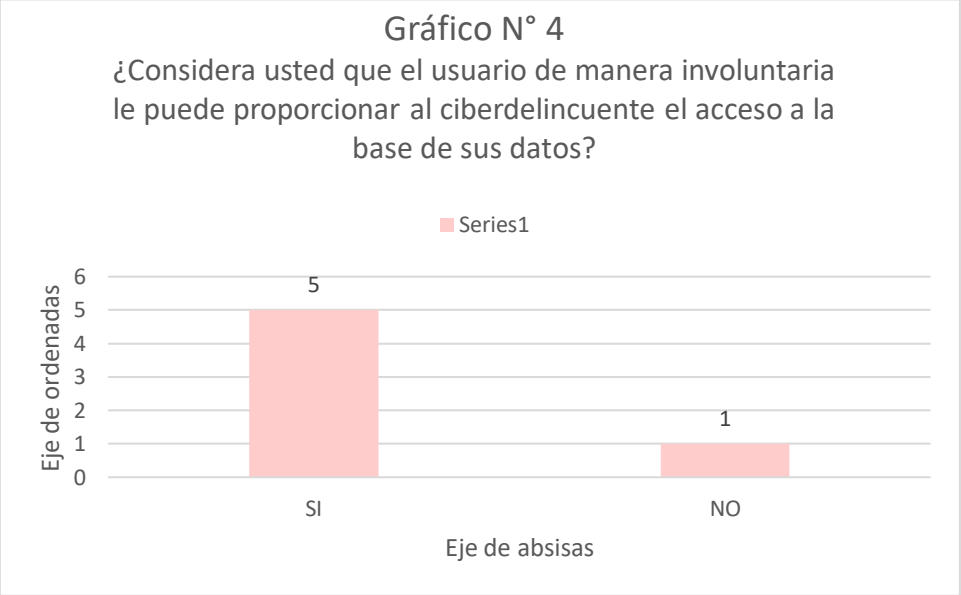
4. ¿Considera usted que el usuario de manera involuntaria le puede proporcionar al ciberdelincuente el acceso a la base de sus datos?

TABLA N° 4

¿Considera usted que el usuario de manera involuntaria le puede proporcionar al ciberdelincuente el acceso a la base de sus datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7
	SI	5	83,3	83,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que el usuario de manera involuntaria si puede proporcionar al ciberdelincuente el acceso a la base de sus datos, mientras que el 16,7% considera que el usuario de manera involuntaria no puede proporcionar al ciberdelincuente el acceso a la base de sus datos.

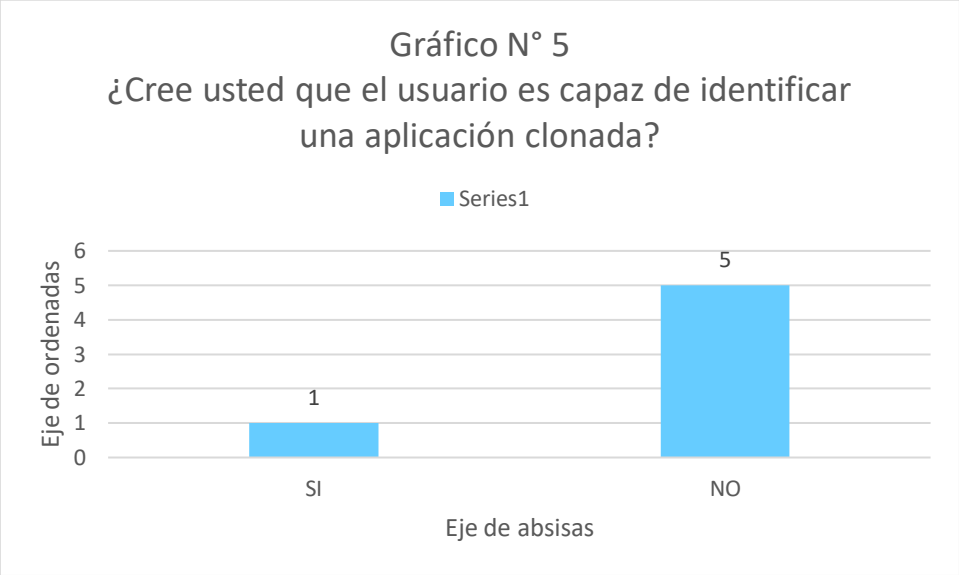
5. ¿Cree usted que el usuario es capaz de identificar una aplicación clonada?

TABLA N° 5

¿Cree usted que el usuario es capaz de identificar una aplicación clonada?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	83,3	83,3	83,3
	SI	1	16,7	16,7	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 16,7% considera que el usuario si es capaz de identificar una aplicación clonada, mientras que el 83,3% considera que el usuario no es capaz de identificar una aplicación clonada.

6. **¿Considera usted que él envió de mensajes en cadena puede permitir al ciberdelincuente el acceso a la base de datos?**

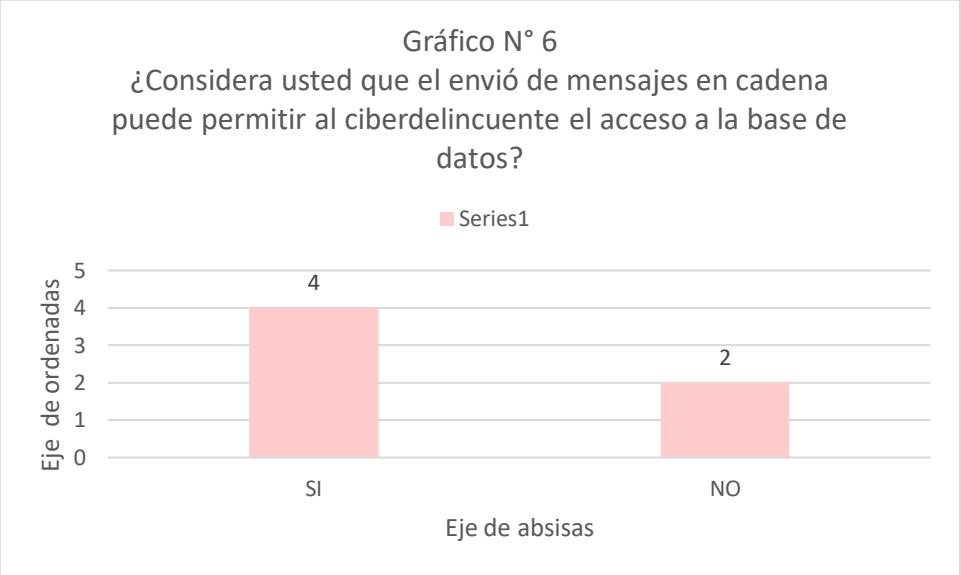
TABLA N° 6

¿Considera usted que el envió de mensajes en cadena puede permitir al ciberdelincuente el acceso a la base de datos?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado

Válido	NO	2	33,3	33,3	33,3
	SI	4	66,7	66,7	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2021
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2021
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 66,7% considera que él envió de mensajes en cadena si permite al ciberdelincuente el acceso a la base de datos, mientras que el 33,3% considera que él envió de mensajes en cadena no puede permitir al ciberdelincuente el acceso a la base de datos

7. **¿Cree usted que el programa Malverstising diseña anuncios maliciosos para robar información?**

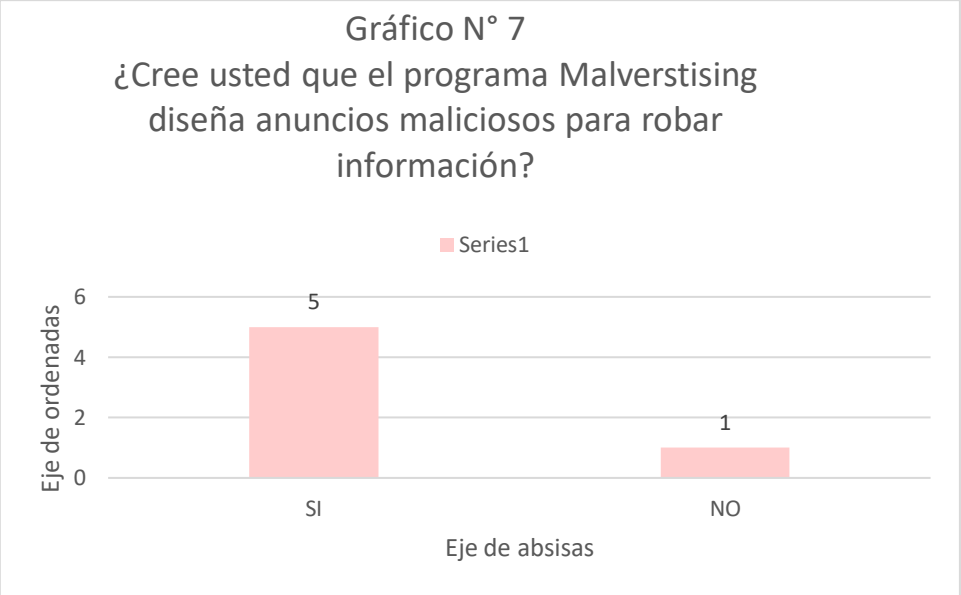
TABLA N° 7

¿Cree usted que el programa Malverstising diseña anuncios maliciosos para robar información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7

	SI	5	83,3	83,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que el programa Malverstising si diseña anuncios maliciosos para robar información, mientras que el 16,7% considera que el programa Malverstising no diseña anuncios maliciosos para robar información.

8. ¿Considera usted que el IP oculto puede encubrir al ciberdelincuente?

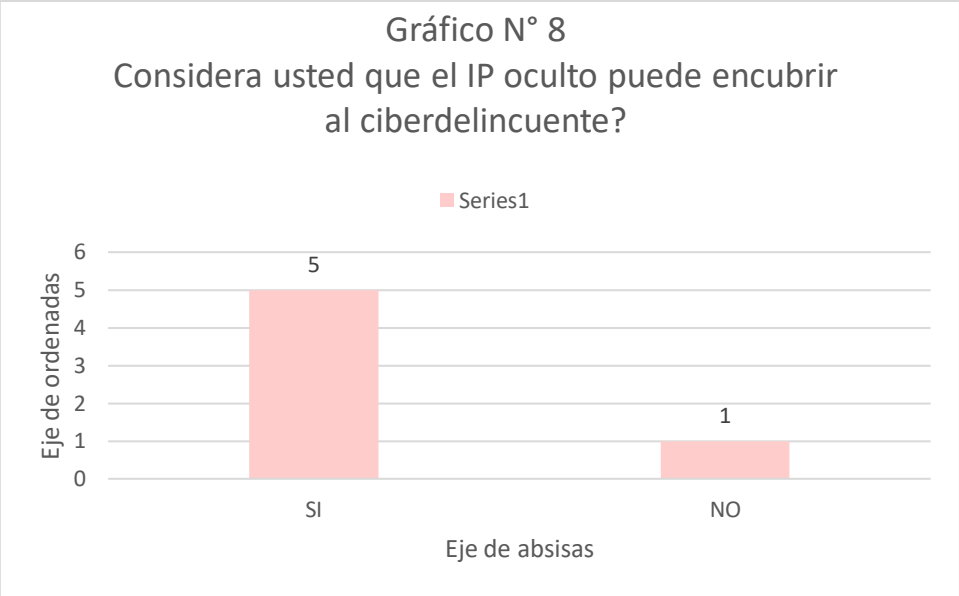
TABLA N° 8

¿Considera usted que el IP oculto puede encubrir al ciberdelincuente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7
	SI	5	83,3	83,3	100,0

	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que el IP oculto si puede encubrir al ciberdelincuente, mientras que el 16,7% considera que el IP oculto no puede encubrir al ciberdelincuente.

9. **¿Considera usted que debería de existir normas legales que regulen la compra y venta online?**

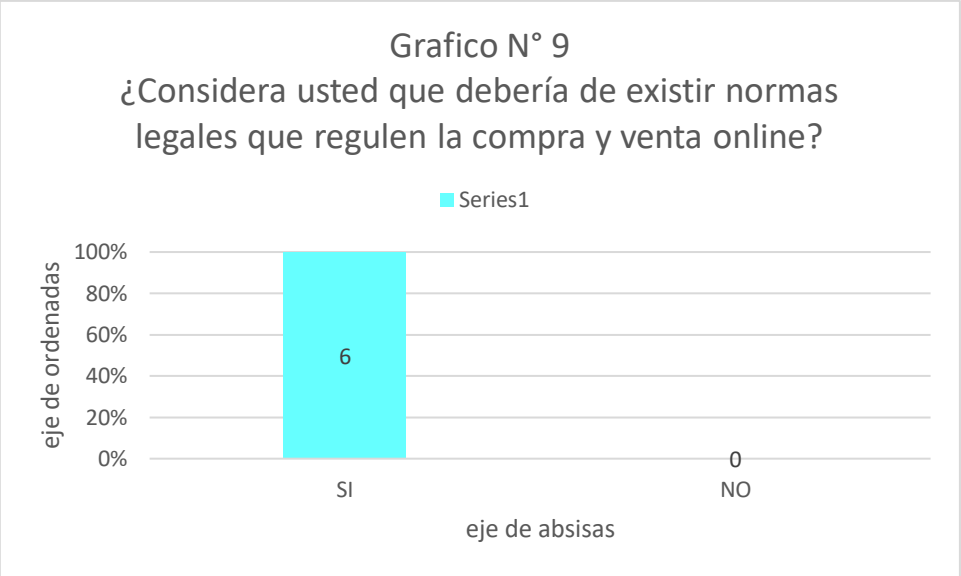
TABLA N° 9

¿Considera usted que debería de existir normas legales que regulen la compra y venta online?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	6	100,0	100,0	100,0

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019

ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

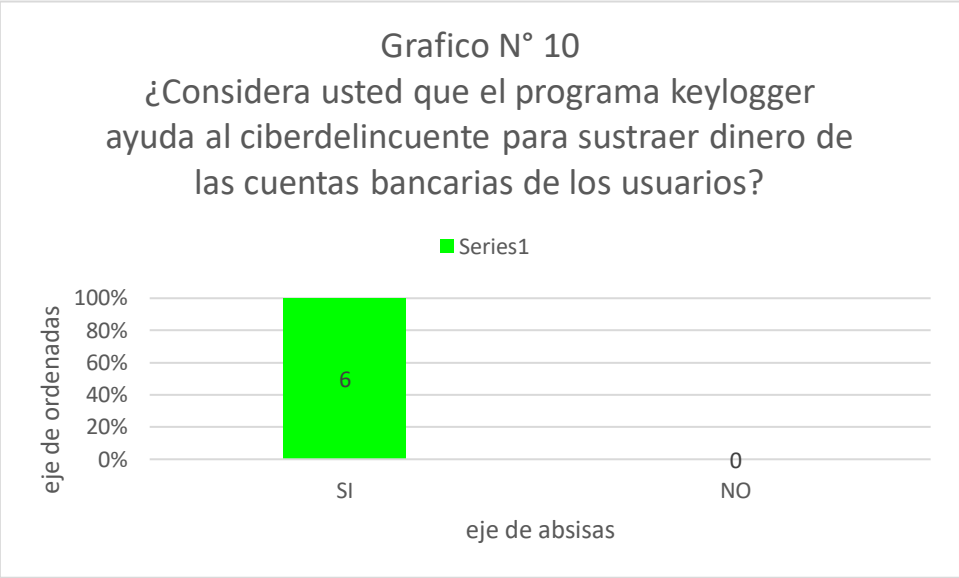
INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que si debería de existir normas legales que regulen la compra y venta online y el 0% considera que no debería de existir normas legales que regulen la compra y venta online.

10. ¿Considera usted que el programa keylogger ayuda al ciberdelincuente para sustraer dinero de las cuentas bancarias de los usuarios?

TABLA N° 10

Válido	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	6	100	100	100
NO	0	0	0	100
TOTAL	6	100	100	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

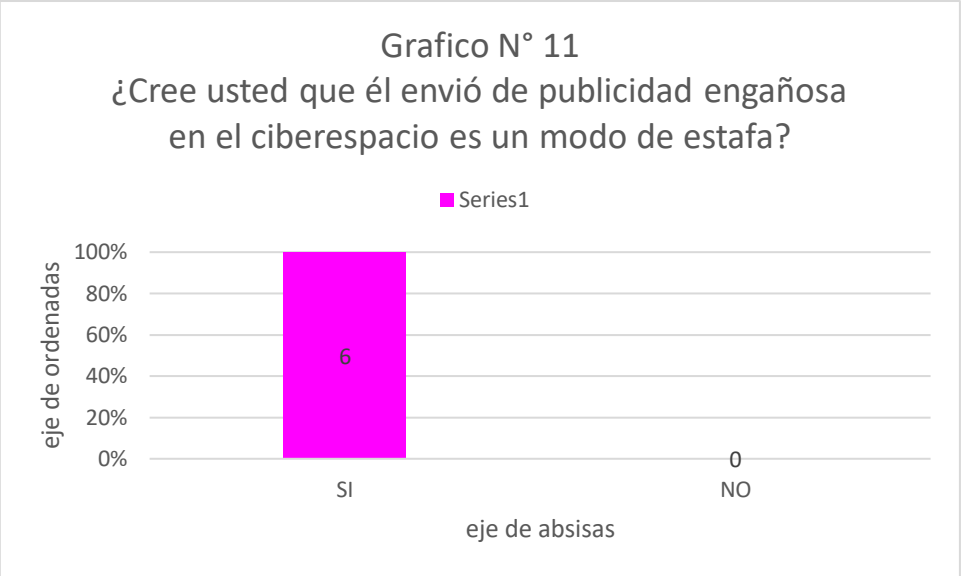
INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que el programa keylogger si ayuda al ciberdelincuente para sustraer dinero de las cuentas bancarias de los usuarios y el 0% considera que el programa keylogger no ayuda al ciberdelincuente para sustraer dinero de las cuentas bancarias de los usuarios.

11. ¿Cree usted que él envió de publicidad engañosa en el ciberespacio es un modo de estafa?

TABLA N° 11

Válido	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	6	100	100	100
NO	0	0	0	100
TOTAL	6	100	100	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

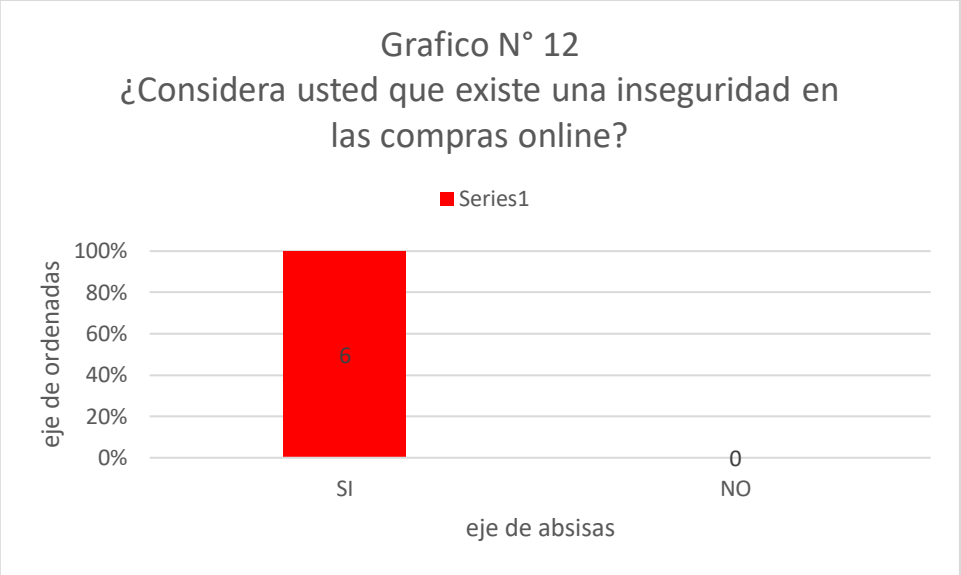
INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que él envió de publicidad engañosa en el ciberespacio si es un modo de estafa y el 0% considera que él envió de publicidad engañosa en el ciberespacio no es un modo de estafa.

12. ¿Considera usted que existe una inseguridad en las compras online?

TABLA N° 12

Válido	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	6	100	100	100
NO	0	0	0	100
TOTAL	6	100	100	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

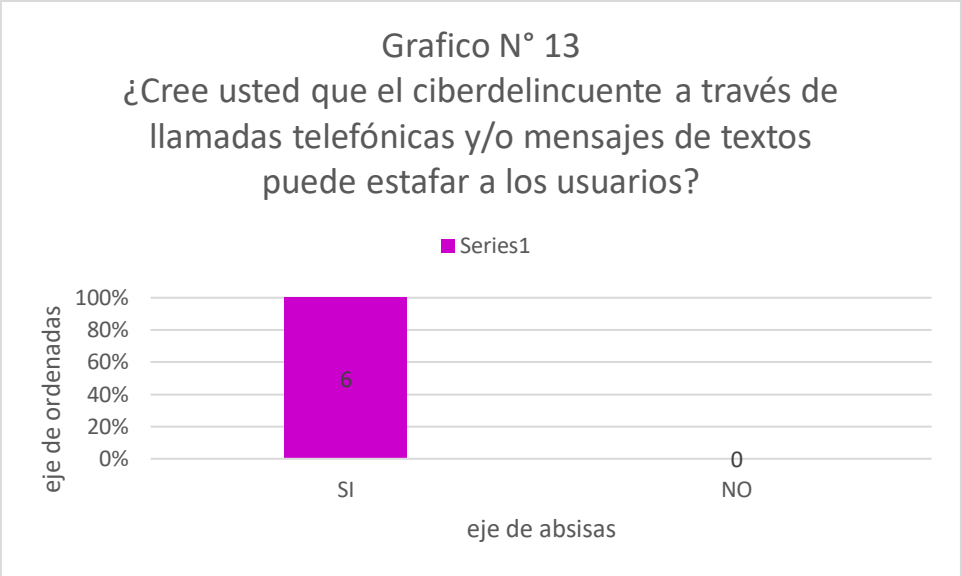
INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que si existe una inseguridad en las compras online y el 0% considera que no existe una inseguridad en las compras online.

13. ¿Cree usted que el ciberdelincuente a través de llamadas telefónicas y/o mensajes de textos puede estafar a los usuarios?

TABLA N° 13

Válido	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	6	100	100	100
NO	0	0	0	100
TOTAL	6	100	100	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta realizada a los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 100% considera que el ciberdelincuente a través de llamadas telefónicas y/o mensajes de textos si puede estafar a los usuarios y el 0% considera que el ciberdelincuente a través de llamadas telefónicas y/o mensajes de textos no puede estafar a los usuarios.

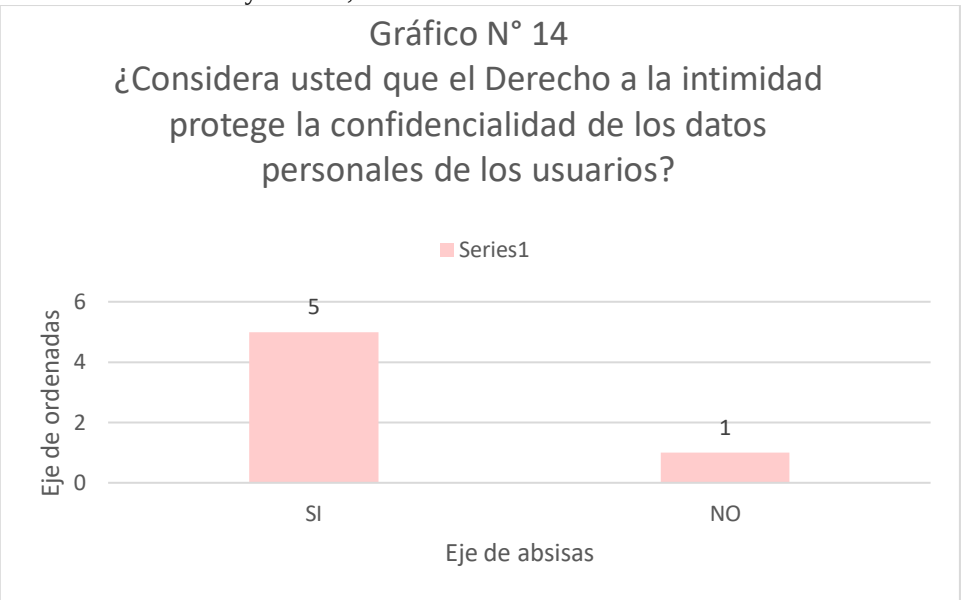
14. ¿Considera usted que el Derecho a la intimidad protege la confidencialidad de los datos personales de los usuarios?

TABLA N° 14

¿Considera usted que el Derecho a la intimidad protege la confidencialidad de los datos personales de los usuarios?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7
	SI	5	83,3	83,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que el Derecho a la intimidad si protege la confidencialidad de los datos personales de los usuarios, mientras que el 16,7% considera que el Derecho a la intimidad no protege la confidencialidad de los datos personales de los usuarios.

15. ¿Considera usted que nuestras normas legales protegen a los usuarios en el ciberespacio?

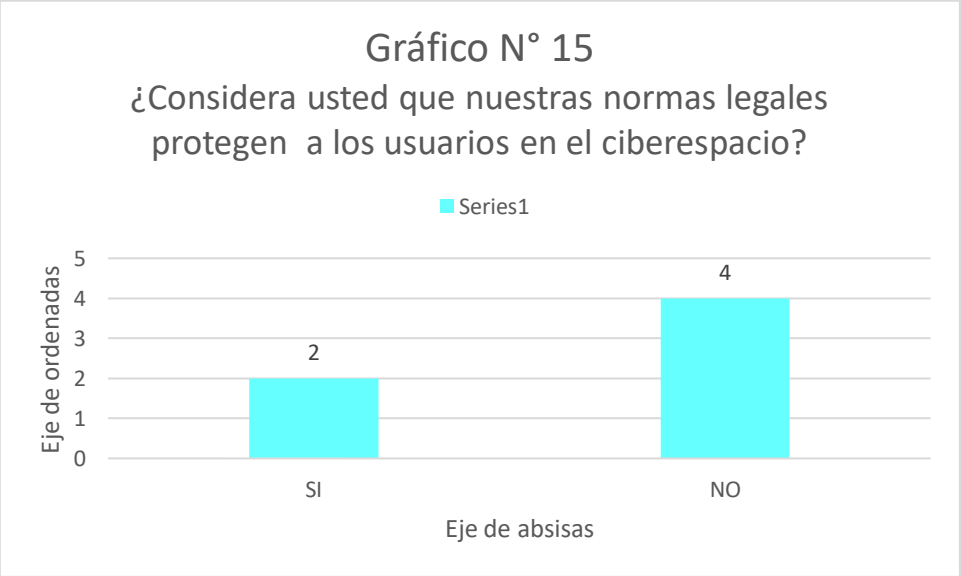
TABLA N° 15

¿Considera usted que nuestras normas legales protegen a los usuarios en el ciberespacio?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	4	66,7	66,7	66,7
	SI	2	33,3	33,3	100,0

	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 33,3% considera que nuestras normas legales si protegen a los usuarios en el ciberespacio, mientras que el 66,7% considera que nuestras normas legales no protegen a los usuarios en el ciberespacio.

16. ¿Considera usted que debería de existir una entidad que supervise y controle el uso de las redes sociales?

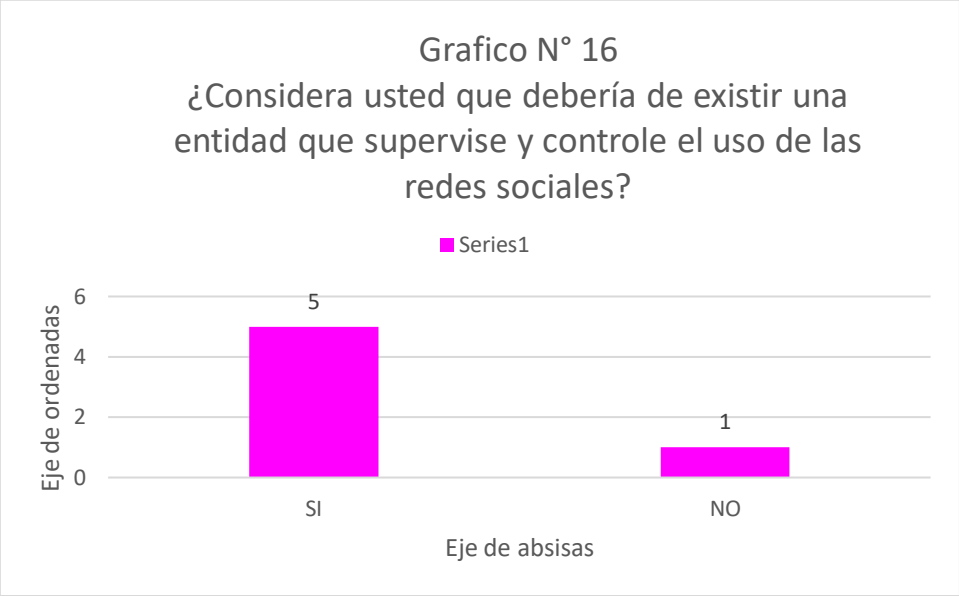
TABLA N° 16

¿Considera usted que debería de existir una entidad que supervise y controle el uso de las redes sociales?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	16,7	16,7	16,7

	SI	5	83,3	83,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 83,3% considera que si debería de existir una entidad que supervise y controle el uso de las redes sociales, mientras que el 16,7% considera que no debería de existir una entidad que supervise y controle el uso de las redes sociales.

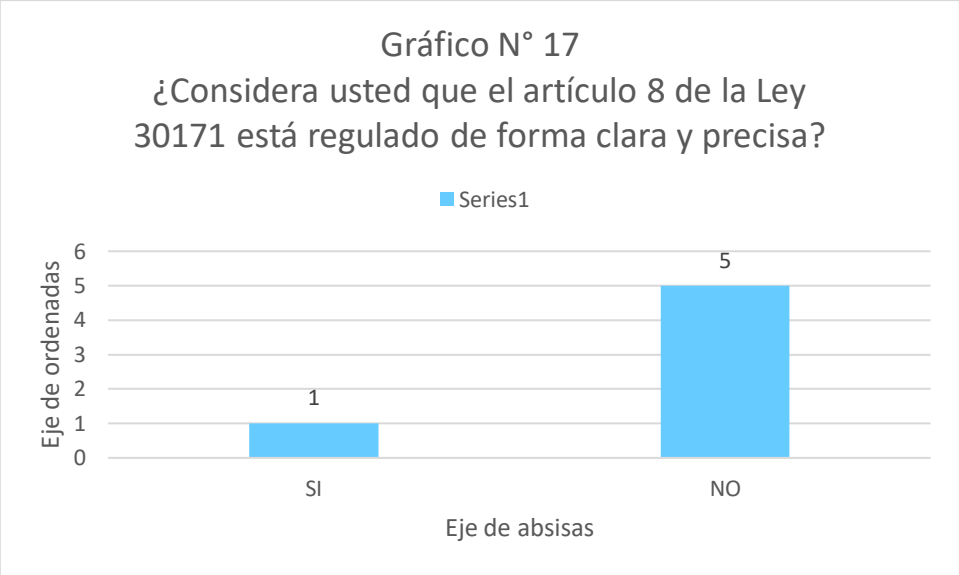
17. ¿Considera usted que el artículo 8 de la Ley 30171 está regulado de forma clara y precisa?

TABLA N° 17

¿Considera usted que el artículo 8 de la Ley 30171 está regulado de forma clara y precisa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	83,3	83,3	83,3
	SI	1	16,7	16,7	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2021
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 16,7% considera que el artículo 8 de la Ley 30171 si está regulado de forma clara y precisa mientras que, el 83,3% considera que el artículo 8 de la Ley 30171 no está regulado de forma clara y precisa.

18. ¿Considera usted que el Fraude Informático es un delito de mera actividad?

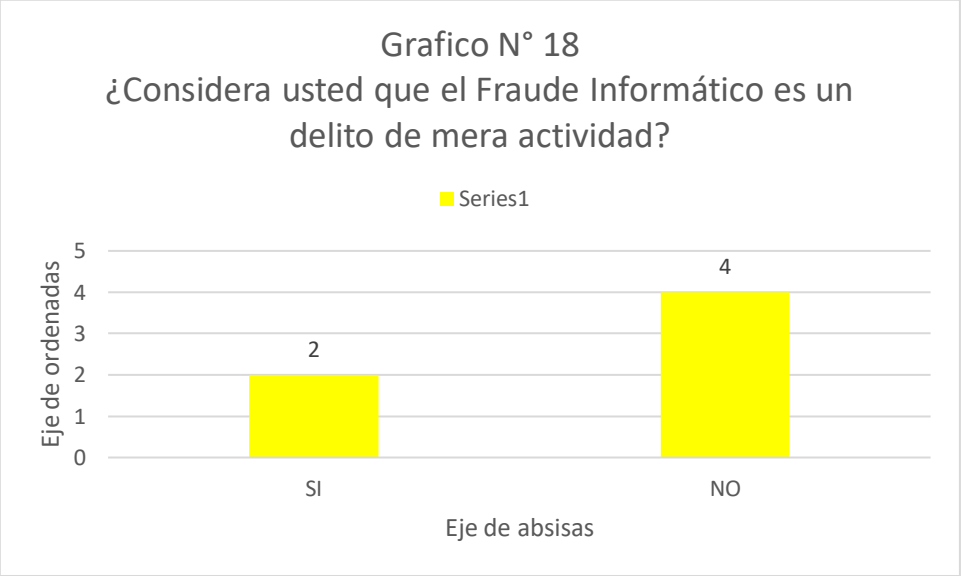
TABLA N° 18

¿Considera usted que el Fraude Informático es un delito de mera actividad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	4	66,7	66,7	66,7

	SI	2	33,3	33,3	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2021
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 33,3% considera que el Fraude Informático si es un delito de mera actividad, mientras que el 66,7% considera que Fraude Informático no es un delito de mera actividad.

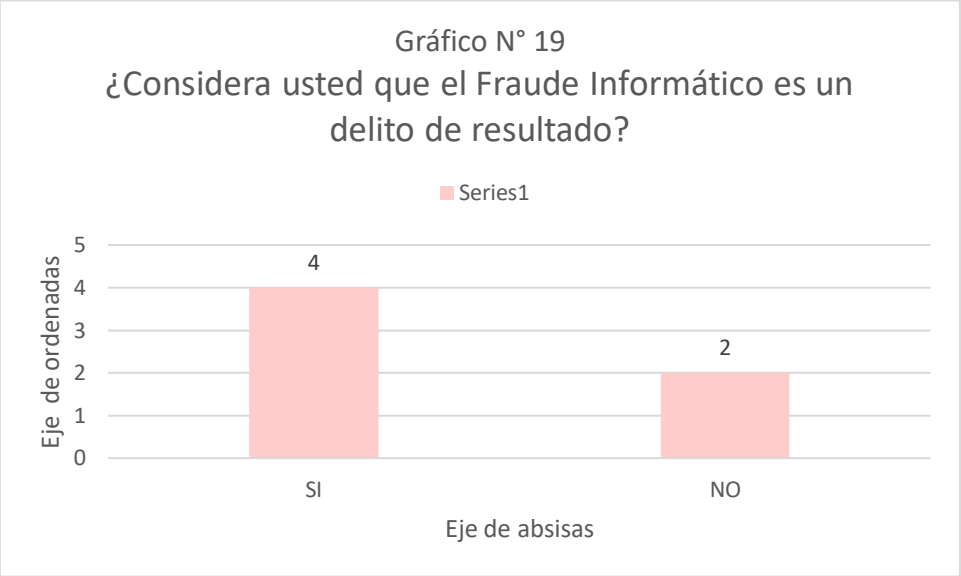
19. ¿Considera usted que el Fraude Informático es un delito de resultado?

TABLA N° 19

¿Considera usted que el Fraude Informático es un delito de resultado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	2	33,3	33,3	33,3
	SI	4	66,7	66,7	100,0
	Total	6	100,0	100,0	

FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.



FUENTE: Encuesta aplicada a los fiscales de las seis fiscalías de la Fiscalía Provincial Penal Corporativa de Huancayo-2019
ELABORADO: Alanya Rivera, M.I.

INTERPRETACION: De la encuesta recogida de los 6 fiscales correspondientes a cada una de las fiscalías Penales de la ciudad de Huancayo, se aprecia que el 66,7% considera que el Fraude Informático si es un delito de resultado mientras que, el 33,3% considera que el Fraude Informático no es un delito de resultado.

4.2. ESTADISTICA INFERENCIAL

4.2.1. Contrastación de Hipótesis General

Formulamos las hipótesis estadísticas:

Ha: La inseguridad informática influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

H0: La inseguridad informática NO influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

Tabla cruzada INSEGURIDAD INFORMATICA*DELITOS INFORMATICOS

			DELITOS INFORMATICOS			
			7	8	9	Total
INSEGURIDAD INFORMATICA	4	Recuento	0	1	1	2
		Recuento esperado	,3	1,0	,7	2,0
		% del total	0,0%	16,7%	16,7%	33,3%
	5	Recuento	0	0	1	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	0,0%	16,7%	16,7%
	6	Recuento	0	1	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	16,7%	0,0%	16,7%
	7	Recuento	1	1	0	2
		Recuento esperado	,3	1,0	,7	2,0
		% del total	16,7%	16,7%	0,0%	33,3%
Total		Recuento	1	3	2	6
		Recuento esperado	1,0	3,0	2,0	6,0
		% del total	16,7%	50,0%	33,3%	100,0%

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	5,500[a]	6	,481
Razón de verosimilitud	6,592	6	,360
Asociación lineal por lineal	2,276	1	,131
N de casos válidos	6		

a. 12 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,17.

Medidas simétricas

		Valor	Significación aproximada
Nominal por Nominal	Coeficiente de contingencia	,692	,481
N de casos válidos		6	

Donde se obtiene los siguientes datos:
P valor: 0,481

Chi cuadrado: 692
1) Si p valor (Sig.) < 0.050(5%) existe correlación = se rechaza Ho y se acepta Ha.

2) Si p valor (Sig.) > 0.050 (5%) no existe correlación = Se rechaza Ha y se acepta Ho.

CONCLUSIÓN: Como el nivel de significancia es mayor que 0,05 (0,000 <0,05) se rechaza la hipótesis alternativa y aceptamos la hipótesis nula, por lo cual podemos concluir que la inseguridad informática NO influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

4.2.2. Contrastación de Hipótesis Especifica 1

Ha: La inseguridad informática influye significativamente en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019

H0: La inseguridad informática NO influye significativamente en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019

Tabla cruzada SISTEMA INFORMATICO*DELITOS INFORMATICOS

			DELITOS INFORMATICOS			
			7	8	9	Total
SISTEMA INFORMATICO	SI	Recuento	0	1	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	16,7%	0,0%	16,7%
	2	Recuento	1	2	2	5
		Recuento esperado	,8	2,5	1,7	5,0
		% del total	16,7%	33,3%	33,3%	83,3%
Total		Recuento	1	3	2	6
		Recuento esperado	1,0	3,0	2,0	6,0
		% del total	16,7%	50,0%	33,3%	100,0%

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	1,200[a]	2	,549
Razón de verosimilitud	1,588	2	,452
Asociación lineal por lineal	,059	1	,808
N de casos válidos	6		

a. 6 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,17.

Medidas simétricas

		Valor	Significación aproximada
Nominal por Nominal	Coeficiente de contingencia	,408	,549
N de casos válidos		6	

Donde se obtiene los siguientes datos:

P valor: 0,549

Chi cuadrado: 1,200

1) Si p valor (Sig.) < 0.050(5%) existe correlación = se rechaza Ho y se acepta Ha.

2) Si p valor (Sig.) > 0.050 (5%) no existe correlación = Se rechaza Ha y se acepta Ho.

CONCLUSIÓN: Como el nivel de significancia es mayor que 0,05 (0,000 <0,05) se rechaza la hipótesis alternativa y aceptamos la hipótesis nula, por lo cual podemos concluir que la inseguridad informática NO influye significativamente en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019

4.2.3. Contrastación de Hipótesis Especifica 2

H1: La inseguridad informática influye significativamente en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

H0: La inseguridad informática NO influye significativamente en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

Tabla cruzada PROGRAMAS MALICIOSOS*DELITOS INFORMATICOS

			DELITOS INFORMATICOS			
			7	8	9	Total
PROGRAMAS MALICIOSOS	SI	Recuento	0	1	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	16,7%	0,0%	16,7%
	2	Recuento	0	0	2	2
		Recuento esperado	,3	1,0	,7	2,0
		% del total	0,0%	0,0%	33,3%	33,3%
	3	Recuento	0	1	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	16,7%	0,0%	16,7%
	4	Recuento	1	0	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	16,7%	0,0%	0,0%	16,7%
	5	Recuento	0	1	0	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	16,7%	0,0%	16,7%
Total		Recuento	1	3	2	6
		Recuento esperado	1,0	3,0	2,0	6,0

	% del total	16,7%	50,0%	33,3%	100,0%

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	12,000[a]	8	,151
Razón de verosimilitud	12,137	8	,145
Asociación lineal por lineal	1,308	1	,253
N de casos válidos	6		

a. 15 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,17.

Medidas simétricas

		Valor	Significación aproximada
Nominal por Nominal	Coeficiente de contingencia	,816	,151
N de casos válidos		6	

Donde se obtiene los siguientes datos:

P valor: 0,151

Chi cuadrado: 12,000

1) Si p valor (Sig.) < 0.050(5%) existe correlación = se rechaza Ho y se acepta Ha.

2) Si p valor (Sig.) > 0.050 (5%) no existe correlación = Se rechaza Ha y se acepta Ho.

CONCLUSIÓN: Como el nivel de significancia es mayor que 0,05 (0,000 <0,05) se rechaza la hipótesis alternativa y aceptamos la hipótesis nula, por lo cual podemos concluir que la inseguridad informática NO influye significativamente en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

4.2.4. Contrastación de Hipótesis Especifica 3

Ha: La inseguridad informática influye significativamente en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019.

H0: La inseguridad informática influye significativamente en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019.

Tabla cruzada DIRECCION IP*DELITOS INFORMATICOS

			DELITOS INFORMATICOS			
			7	8	9	Total
DIRECCION IP	NO	Recuento	0	0	1	1
		Recuento esperado	,2	,5	,3	1,0
		% del total	0,0%	0,0%	16,7%	16,7%
	SI	Recuento	1	3	1	5
		Recuento esperado	,8	2,5	1,7	5,0
		% del total	16,7%	50,0%	16,7%	83,3%
Total		Recuento	1	3	2	6
		Recuento esperado	1,0	3,0	2,0	6,0
		% del total	16,7%	50,0%	33,3%	100,0%

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	2,400[a]	2	,301
Razón de verosimilitud	2,634	2	,268
Asociación lineal por lineal	1,471	1	,225
N de casos válidos	6		

a. 6 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,17.

Medidas simétricas

		Valor	Significación aproximada
Nominal por Nominal	Coeficiente de contingencia	,535	,301
N de casos válidos		6	

Donde se obtiene los siguientes datos:

P valor: 0,301

Chi cuadrado: 2,400

1) Si p valor (Sig.) < 0.050(5%) existe correlación = se rechaza Ho y se acepta Ha.

2) Si p valor (Sig.) > 0.050 (5%) no existe correlación = Se rechaza Ha y se acepta Ho.

CONCLUSIÓN: Como el nivel de significancia es mayor que 0,05 (0,000 <0,05) se rechaza la hipótesis alternativa y aceptamos la hipótesis nula, por lo cual podemos concluir que la inseguridad informática influye significativamente en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019.

CAPÍTULO VI

ANALISIS Y DISCUSIÓN DE RESULTADOS

En este capítulo vamos a discutir sobre los resultados obtenidos a través de los cuadros generales y gráficos obtenidos, así como la prueba de chi-cuadrado; por lo cual después de realizar la prueba de chi - cuadrado se demostró que nuestras hipótesis son nulas, sin embargo, en el desarrollo de la presente investigación hemos demostrado que la informática influye en los delitos informáticos, por ende, lo demostraremos en la discusión de los resultados obtenidos:

5.1. Discusión del resultado del objetivo general

El objetivo general de la investigación es: Determinar la influencia de la inseguridad informática en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

En este sentido debemos de mencionar que conforme la sociedad avanza, nuestras normas y necesidades van conforme a estos nuevos avances, es por ello que debido al

cambio y a la utilidad de los medios tecnológicos es necesario generar nuevas medidas de seguridad.

Actualmente el modus operandi del delincuente ya no necesita de generar una violencia física, sino que ahora el ciberdelincuente a través de programas maliciosos puede sustraer dinero, realizar prestamos, difundir información personal de un usuario o de una empresa, clonar tarjetas, dejar inseguro la base de datos de bancos, etc. Al ser un nuevo modus operandi del delincuente es necesario adecuar nuestras normas legales para poder contrarrestar este tipo de delitos.

Para poder respaldar nuestra postura que los delitos informáticos esta en estrecha relación con el sistema informático, debemos de señalar lo que menciona Zarich (2005):

> "Como aquellas conductas disvaliosas socialmente y reprochables desde el punto de vista penal que, concertadas mediante instrumentos y sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tutelados por la ley, en un momento dado" (p. 134)

Por ello a modo de conclusión podemos decir que el sistema informático (inseguridad informática) tiene esta estrecha relación con los delitos informáticos ya que la existencia de programas maliciosos que atacan el sistema de seguridad de los usuarios para poder obtener su fin ilícito, sin embrago cabe mencionar que este ataque puede ser de dos maneras, la primera cuando el ciberdelincuente a través de programas maliciosos y aprovechándose del desconocimientos de medidas de seguridad por parte del usuario ataca al sistema informática para poder cometer su ilícito y la segunda cuando utiliza los programas maliciosos y destruye las medidas de seguridad que tuviera el usuario para poder comerter si fin ilícito.

5.2. Discusión del resultado del primer objetivo especifico

El primer objetivo específico que se planteó en la investigación es: Determinar la influencia de la inseguridad informática en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

En este sentido mencionaremos lo mencionado por Gutiérrez (1991) sobre el fraude informáticos: "(…) El fenómeno de mayor magnitud y trascendencia en el ámbito de la criminalidad mediante computadoras (…)" (p. 87). Al respecto Villavicencio (2014) señala que "Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, el internet, etcétera (…)" (p. 286).

En este aspecto del delito de fraude informático debemos de mencionar que es aquel ilícito cometido mediante el uso de la tecnología que facilita la consumación de la misma o es una modalidad de cometer el ilícito, por ende podemos decir que este delito ya se encuentra tipificado en el Código Penal pero que ciertos delitos van a tener un apoyo de la tecnología o que se va a realizar por este medio pero teniendo como resultado el primer delito que se quería consumar; estos casos se dan con mayor frecuencia en delitos contra el patrimonio como el hurto, el robo o la estafa en vista de que la sustracción de un patrimonio es el principal objetivo criminal pero que, para poder consumar este delito en determinados casos se va a tener que necesitar el apoyo tecnológico pero que en realidad su objetivo es la sustracción del bien mas no la apropiación de un sistema operativo.

A modo de conclusión podemos decir que la inseguridad informática tiene relación con el fraude informático, ya que para la consumación del delito se da de dos maneras, la primera que se puede usar un programa maliciosos que pueda quebrantar y/o alterar el sistema informático del usuario para que así pueda acceder a la base de datos,

mientras que el otro solo queda en tentativa ya que con la creación de un programa malicioso y la venta de esta termina su fin ilícito, sin embargo este hecho quedaría en una tentativa y no en la consumación del delito de fraude informático.

5.3. Discusión del resultado del segundo objetivo especifico

El segundo objetivo específico que se planteó en la investigación es: Determinar la influencia de la inseguridad informática en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019.

Si bien es cierto nuestro sistema legal no contempla la estafa informática como tal sino solo se tipifica como estafa, sin embargo existe este tipo de estafa informática pero es usado como herramienta para poder consumar el primer delito que se pretende logra, que en este caso es la apropiación de un bien ajeno, sin embargo a esto debemos de mencionar lo que (PORTALEY, 2012) nos señala :

> "La estafa informática es un fenómeno delictivo que en los últimos años está tomando mayor magnitud y relevancia en el ámbito de la criminalidad informática, siendo éste la base principal del delito informático sobre el que gira la ciberdelincuencia. (…). Los elementos típicos que integran el delito de estafa informática son: La manipulación informática y artificio semejante, Transferencia patrimonial no consentida por el titular del mismo, ánimo de lucro, y perjuicio en tercero." (párr. 3)

En este punto estamos de acuerdo con la hipótesis nula ya que en realidad la estafa informática no es ajeno a la estafa tipificada en el artículo 196 del Código Penal, ya que la modalidad es la misma solo que en este caso se acoge a los medios tecnológicos para poder cometer su ilícito criminal.

Por ende, podemos concluir que la estafa informática no es otra cosa que la estafa propiamente dicha que tiene aportación de la tecnología para poder consumar el delito, por ejemplo, las compras y ventas online, no cambian la figura de mantener en engaño al usuario, sino que este hecho se hace a través de medios tecnológicos.

5.4. Discusión del resultado del tercer objetivo especifico

El tercer objetivo específico que se planteó en la investigación es: Determinar la influencia de la inseguridad informática en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019

En este apartado podemos señalar lo mencionado por Rebollo citado por Ruiz (2005) señala que:

> "a) Es un derecho universal porque pertenece a todos los hombres; es innato, inherente a la persona, corresponde a su titular por el solo hecho de ser persona, y acompaña a todo hombre desde su nacimiento hasta incluso después de su fallecimiento; b) es individual porque se reconoce a favor de casa persona individualmente considerada; protege al sujeto en lo que es (con su entorno físico, psíquico y moral) o en lo que puede ser. Se configura para establecer un ámbito en el que el individuo es soberano; c) es un derecho inviolable, que no puede ser negado por los otros; es ejercitable erga omnes, frente a las personas o instituciones. Eso no quiere decir que sea un derecho ilimitado, ya que, en determinadas circunstancias, podría ceder ante otro interés más relevante; d) decimos que el derecho a la intimidad es inalienable porque no está sujeto a prestación o renuncia, no puede extinguirse por voluntad abdicativa de su titular, ni se puede renunciar a él de forma total; en este sentido es también extramatrimonial

> porque no se puede comerciar con él; e) por último, se trata de un derecho imprescriptible, pues al ser inherente a la persona , no cabe posibilidad de que el derecho se extinga" (p. 262)

Para poder consumar los delitos informáticos, en primer lugar, es necesario acceder a la base de datos, en donde el ciberdelincuente con el primer derecho que viola es el derecho a la intimidad ya que al quebrantar la seguridad del sistema informático puede tener acceso a toda la base de datos.

Estos hechos se pueden observar con mayor frecuencia en los casos en los que se quebranta la seguridad informática de una base de datos de un banco, quedando a disposición cada uno de los datos personales de sus clientes.

Por ello a modo de conclusión podemos decir que en los delitos informáticos debido a la poca seguridad informática o la inseguridad informática que presenta, los usuarios son susceptibles de ser violados en su derecho a la intimidad, ahora esta vulneración no solo se basa a la poca seguridad la inseguridad, sino que también está ligada a no conocer los términos y condiciones de las aplicaciones que se suelen usar.

CONCLUSIONES

1. Se concluye que nuestra hipótesis general y especificas a través de la prueba de chi cuadrado ha generado una hipótesis nula, sin embargo, cabe mencionar que nuestras normas legales no están de acuerdo al avance tecnológico, lo cual genera cierta inseguridad jurídica, ya que no es posible controlar estos hechos punibles a través de nuestra normal legal, que no son concordantes con nuestra realidad social.

2. Se logró demostrar que en los delitos informáticos es indispensable que el usuario genere el acceso al ciberdelincuente a la base de datos de este, ya que si el usuario de manera involuntaria no otorga el acceso es casi imposible que el ciberdelincuente pueda acceder a la base de datos.

3. En nuestra legislación el artículo 8 de la ley 30096 modificado por la 30171, no se evalúa de manera clara y precisa el delito por su consecuencia de la acción, ya que en dicho artículo se encuentra delitos de mera actividad como de resultado, lo que imposibilita al fiscal realizar una adecuada imputación del delito.

4. Se concluyó que en nuestra legislación no existe una adecuada protección al derecho a la intimidad del usuario en el ciberespacio, ya que cualquier persona puede suplantar la identidad de un usuario.

RECOMENDACIONES

1. Se recomienda una orientación y/o capacitación a la población para tener un adecuado uso de las redes sociales y conocer las medidas de seguridad para que cada usuario se pueda proteger en el ciberespacio.
2. Se recomienda seguir adelante con la investigación, cambiando la metodología de la investigación para así poder generar un mejor aporte social y jurídico.
3. Se recomienda generar un proyecto de ley que pueda regular de manera clara y precisa el artículo 8 de la ley 30096 modificado por la ley 30171.
4. Se recomienda generar un proyecto de ley en la que exista una entidad fiscalizadora y supervisora de las redes sociales en cuanto a la protección de la intimidad de las personas como en la evasión de impuestos a través de la venta y compra online.
5. Se recomienda generar un agravante en el artículo 196-A, que establezca como agravante aquella estafa que se realice a través de un medio tecnológico.

REFERENCIAS BIBLIOGRAFICAS

Ander-Egg, (17 de octubre del 2017). *Tipos y Niveles de Investigación*. Recuperado de la página: http://devnside.blogspot.com/2017/10/tipos-y-niveles-de-investigacion.html

Arreola, A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* (1ª Ed.). México.

Arroyo L. y Nieto A. *Fraude y Corrupción en el Derecho penal Económico Europeo. Eurodelitos de corrupción y fraude.* (2006). (1 Edición). Editorial Universidad de Castilla. Recuperado de: https://books.google.com.pe/

Bermúdez y Bailón (2015); *Análisis en seguridad informática y seg011uridad de la información basado en la norma ISO/IEC 27001-sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros.* [Tesis de Pregrado]; presentado para optar el Título Profesional de Ingeniero en Sistemas, Universidad Politécnica Salesiana Sede Guayaquil - Ecuador.

Cano J. (2004): *Inseguridad informática: Un concepto dual en seguridad informática:* Revista de Asociación Colombiana de Ingenieros de Sistemas- ACIS, 1(6): Recuperado de: https://acis.org.co/portal/content/articulos

Chauca (2014); *El principio de proporcionalidad en la prevención de los delitos informáticos*. [Tesis de Pregrado]; presentado para optar el Título Profesional de Abogado, Universidad Regional Autónoma de los Andes, Ibarra-Ecuador.

Código Penal [CP]. Decreto Legislativo Nº 635. Mayo 2016. Lima, Perú.

Constitución Política del Perú [Const.] Art. 2, 29 de diciembre de 1993.

Convenio sobre la Ciberdelincuencia. Budapest. artículos del 1 al 8. 23 de noviembre del 2001. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Costas, J. (2006). *Seguridad Informática.* (1ª Ed.) Editorial RA-MA.

Diccionario jurídico de Derecho. (2020). *Enciclopedia Jurídica*. Recuperado de: http://www.enciclopedia-juridica.com/temas.htm

ECURED (2020). Obtenido de: https://www.ecured.cu/Sistema_inform%C3%A1tico#Tipos_de_sistemas_inform.C3.A1ticos

Experto, E. d. (31 de 03 de 2018). *VIU-Universidad Internacional Valencia.* Obtenido de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Gómez (2014): *Enciclopedia de la Seguridad Informatica* (2 Edición); Edición RA-MA; Madrid-España; Recuperado en: https://books.google.com.pe/books?id=Bq8DwAAQBAJ&pg=PT56&dq=A+la+hora+de+analizar+las+posibles+consecuencias+de+la+ausencia+o+de+unas+deficientes+medidas+de+seguridad+inform

GSITIC. (19 de ENERO de 2018). *Apuntes Gestión de Sistemas de Información (GSI)*. Obtenido de https://gsitic.wordpress.com/2018/01/19/bii13-seguridad-fisica-y-logica-de-un-sistema-de-informacion-riesgos-amenazas-y-vulnerabilidades-medidas-de-proteccion-y-aseguramiento-auditoria-de-seguridad-fisica/#:~:text=Seguridad%20F%C3%ADsica%20y%20Seguridad%

Gutiérrez L. (1991). *Fraude Informático y Estafa (Amplitud del tipo de estafa en el Derecho Español ante las defraudaciones por medios informáticos).* (1º Edición). Madrid, España: Editorial. Ministerio de Justicia, Secretaria General Técnica. Recuperado de: https://books.google.com.pe/books?id=V57-

Snqh94sC&pg=PA272&dq=fraude+informatico&hl=es&sa=X&ved=2ahUKEw#v=onepage&q=fraude%20informatico&f=false

Herrán A. (2002). *El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales.* (1º Edición). Madrid-España: Editorial DYKINSON. Recuperado de: https://books.google.com.pe/books?id=CCVT48egc5MC&pg=PA43&lpg=PA43&dq=herran:+%22De+las+posibles+objeciones+que+pueden+plantearse+a+las+manifestaciones+contenidas+en+este+texto,+destacar+dos:+por+un+lado,+si+como+se+afirma+por+el+legislador+la+%

Herrera R. (2014): *Breve análisis y algunas observaciones al delito informático:* Revista de Investigación Jurídica de Estudiantes, 1(1), 99-114.

Infosegur. (10 de Noviembre de 2013). Obtenido de https://infosegur.wordpress.com/tag/integridad/#:~:text=Otra%20de%20las%20definiciones%20de,y%20aquella%20informaci%C3%B3n%20que%20procesan%2C

León (2018); *Bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención de los Delitos Informáticos de la Ley 30096*. [Tesis de Grado]; presentado para optar el Título Profesional de Abogado, Universidad Señor de Sipán, Chiclayo-Perú.

Ley 30171 de 10 de marzo, *Ley que modifica la ley 30096, ley de delitos informáticos*. (El Peruano – Normas legales, número 518568 de 2014)

Mayer L. (2018): *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*: Revista Ius et Praxis, 24(1).

Mayer L. Oliver G. (2020): *El Delito de Fraude Informático: Concepto y Delimitación*: Revista Chilena de Derecho y Tecnología, *9*(01), 151-184.

Montero I. y De la Cruz M. (2016), *Metodología de la Investigación Científica. (*1º Edicion*)* El Tambo, Perú. Editorial Grupo Crecentro S.A.C.

Ochoa F. (2016). *Ratio Iuris: La razón del derecho.* (1ª Edi.). Chorrillos-Perú

Oficina de Administración de los Tribunales Academia Judicial Puertoriqueña (2015): *Glosario de Términos y de conceptos Jurídicos o Relativos del Poder judicial* (1ª Ed.)

Ossorio, M. (2012): *Diccionario de Ciencias Juridicas Politica y Sociales.* (1ª Edición Electrónica)

Pacheco A. (05 de abril del 2016). *Rangos y clases de IP*. Redes de Comunicación en la UDI. https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip

Pardo (2018); *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*. [Tesis de Posgrado]; presentado para optar el Título Profesional de Maestro en Derecho Penal y Procesal Penal, Universidad César Vallejo, Lima-Perú.

Peña Cabrera (2008). *Derecho Penal Parte Especial.* (2ª Tomo). Lima-Perú: Editorial Moreno S.A.

Pichihua, S. (enero de 2020). *Agencia Peruana de Noticias ANDINA*. Obtenido de https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

PORTALEY. (17 de Diciembre de 2012). *Abogados Portaley penal, civil e Internet.* Obtenido de Guía de Abogados: https://portaley.com/2012/12/introduccion-a-la-estafa-informatica-2/#:~:text=A%20pesar%20de%20las%20diferencias,da%C3%B1o%20patrimonial%20cuantificable%20mediante%20un

Prácticas.COM, G. (03 de Mayo de 2017). Obtenido de http://www.guiaspracticas.com/recuperacion-de-datos/inseguridad-informatica

Prakmatic. (2017). Obtenido de http://www.prakmatic.com/uncategorized/principales-amenazas-de-un-sistema-informatico/#:~:text=Los%20tres%20elementos%20m%C3%A1s%20vulnerables,programa%20descargado%20de%20forma%20gratuita.

Real Academia Española. (2001). *Diccionario de la lengua española* (22.ª ed.). Consultado en https://www.rae.es/

Rivero (2017); *Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017*. [Tesis de Pregrado]; presentado para optar el Título Profesional de Abogado, Universidad César Vallejo, Lima-Perú.

Romero (2017); *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016* [Tesis de Pregrado]. presentado para optar el Título Profesional de abogada, Universidad de Huánuco - Perú.

Romero y Otros (2018): *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*" (1 Edición). Recuperado de: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Ruiz F. (2005). *Discernimiento vocacional y derecho a la intimidad en el candidato al presbiterado diocesano.* (1º Edición). Roma-Italia: Editrice Pontificia Universita Gregoriana. Recuperado de: https://books.google.com.pe/books?id=BvO-9Nv70_oC&pg=PA262&dq=a)+Es+un+derecho+universal+porque+pertenece

Sánchez J. (2016): *Delitos informáticos:* Revista de Academia de la Magistratura, 1(98).

Saraviia, T. (2020): *Causas de la Inseguridad Informática*. SCRIBD. Obtenido de https://es.scribd.com/doc/145302919/Causas-de-La-Inseguridad-Informatica

SoftwareLab.org. (2020). Obtenido de https://softwarelab.org/es/que-es-antimalware

Tapia, A., Gavín, J., y Mayea, R. (2012). *Dirección IP*. https://sites.google.com/site/direccionamientosipredes/home/direccionamiento-ip

Villar, A. (2006). *Introducción a la Informática y al uso y manejo de aplicaciones comerciales. Estrategias para Implementar las Aplicaciones Informáticas en la Gestión empresarial.* (1ª Ed.). España.

Villavicencio F. (2014): *Delitos Informáticos – Cybercrimes*: Revista Ius Et Veritas, 49(29), 284-304

Zarich F. (2005). *Derecho Informático.* (1º Edición). Argentina: Editorial Librería Juris. Recuperado de: https://books.google.com.pe/books?id=BMWwzOqjmEkC&pg=PA97&dq=delitos+informaticos+Seg%C3%BAn+Zarich&hl=es&sa=X&ved=2ahUKEwi_vdW.

Zúñiga L. Mendoza F. Reyna L. *Ley Contra el Crimen Organizado (Ley N.ª 30077) Aspectos sustantivos, procesales y de ejecución penal.* (2016). Lima-Perú: Instituto Pacifico S.A.C.

ANEXOS

ANEXO N° 01

MATRIZ DE CONSISTENCIA

TÍTULO: INSEGURIDAD INFORMATICA Y DELITOS INFORMATICOS DEL USUARIO EN LA FISCALÍA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO 2019

PROBLEMA	OBJETIVOS	MARCO TEÓRICO	HIPOTESIS Y VARIABLE:	VARIABLE Y DIMENSIONES	METODOLOGÍA
General: ¿De qué manera la inseguridad informática influye en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019? **Específicos** - ¿De qué manera la inseguridad informática influye en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019? - ¿De qué manera la inseguridad informática influye en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019? - ¿De qué manera la inseguridad informática influye en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019?	**General:** Determinar la influencia de la inseguridad informática en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019 **Específicos:** - Determinar la influencia de la inseguridad informática en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019. - Determinar la influencia de la inseguridad informática en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019 - Determinar la influencia de la inseguridad informática en el Derecho a la Intimidad del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019	**Antecedentes:** **A nivel Internacional:** a) Bach Kelly Gabriela Bermúdez Molina y Edber Rafael Bailón Sánchez (2015). "Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros". B) El Bach. Chauca Acero Gabriela Cristina (2014). "El Principio de Proporcionalidad en la Prevención de los Delitos Informáticos". **A Nivel Nacional:** a) El Bach. Yorli Adrian León Ochoa (2018): "Bloqueo del IP Dinámico Dentro del Comercio Electrónico como Medida de Prevención de los Delitos Informáticos de la Ley 30096" b) El Bach. Alejo Pardo Vargas (2018): "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018" c) El Bach. Leyla Keith Rivero Passuni (2017): "Delitos Informaticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017" c) El Bach. Meylin Del Pilar Romero Ocampo (2017): "Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016" **2. MARCO TEORICO REFERENCIAL:** La Dirección IP El Sistema Informático El Fraude Informático La Estafa Informática Programas de Espionaje	**Hipótesis General.** La inseguridad informática influye significativamente en los delitos informáticos del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019 **Hipótesis específicas.** 1. La inseguridad informática influye significativamente en el Fraude Informático del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019. 2. La inseguridad informática influye significativamente en la Estafa Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo en el año 2019. 3. La inseguridad informática influye significativamente en el Derecho a la Intimidad Informática del usuario en la Fiscalía Provincial Penal Corporativa de Huancayo 2019.	**VARIABLES:** **Variable X**: La Inseguridad Informática **Variable Y**: Los Delitos Informáticos **DIMESSIONES:** **Variable X**: La Inseguridad Informática - Sistema Informático - Programas Maliciosos - Dirección IP **Variable Y**: Los Delitos Informáticos - Estafa Informática - Derecho a la Intimidad Informática - Fraude Informático	**Tipo:** Explicativo. **Nivel:** Explicativo. **Diseño de investigación** No experimental  Donde: M = Muestra Ox = Observación de la V.I. Oy = Observación de la V.D. **POBLACIÓN Y MUESTRA** **Población**: La Fiscalía Provincial Penal Corporativa de Huancayo **MUESTRA**: No Probabilística por conveniencia, conformado por las 6 Fiscales de la Fiscalía Provincial Penal Corporativa de Huancayo **TÉCNICAS - INSTRUMENTOS DE OBSERVACION** TECNICA: Encuesta INSTRUMENTO: Cuestionario **TÉCNICAS ESTADÍSTICAS DE ANALISIS DE DATOS** programa SPSS versión 25

ANEXO N° 02

OPERALIZACIN DE VARIABLES

VARIABLES	DEFINICION	DIMENSIONES	INDICADORES
Inseguridad Informática (VARIABLE INDEPENDIENTE)	(Expertos, 2018): "El proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente." (párr.1)	Sistema Informático	Protege el soporte lógico en todo momento
		Programas maliciosos	Altera el funcionamiento del equipo el programa troyano
			Diseña anuncios maliciosos para robar información el hardware
		Dirección IP	Facilita el ocultamiento del IP
Delitos Informático (VARIABLE DEPENDIENTE)	Según Villavicencio (2014): "Aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que la Tecnología de la Información y Comunicación (TIC) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos (…)"(p.286)	Estafa Informática	Clona las tarjetas de crédito
			Envió de Publicidad engañosa
		Derechos a la intimidad informática	Protege la confidencialidad de los datos personales
		Fraude Informático	Se evalúa el delito por su consecuencia de la acción

ANEXO N° 03

MATRIZ DE OPERACIONALIZACION DEL INSTRUMENTO DE INVESTIGACIÓN

VARIABLE	NOMBRE DE VARIABLE	DIMENSIONES	INDICADORES	ITEM	VALORACIÓN	INSTRUMENTO
VARIABLE INDEPENDIENTE	Inseguridad Informática	Sistema Informático	Protege el soporte lógico en todo momento	• ¿Considera usted que el soporte lógico del sistema informático se puede quebrantar con programas maliciosos? • ¿Considera usted que extraer información de dudosa procedencia a través de la web causa daños al soporte lógico? •	1: SI 2: NO	CUESTIONARIO
		Programas maliciosos	Altera el funcionamiento del equipo el programa troyano	• ¿Usted considera que el Ciberdelincuente puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos? • ¿Considera usted que el usuario de manera involuntaria le puede proporcionar al ciberdelincuente el acceso a la base de sus datos?		
			Diseña anuncios maliciosos para robar información el hardware	• ¿Cree usted que el usuario es capaz de identificar una aplicación clonada? • ¿Considera usted que el envió de mensajes en cadena puede permitir al ciberdelincuente el acceso a la base de datos? • ¿Cree usted que el programa Malverstising diseña anuncios maliciosos para robar información?		
		Dirección IP	Facilita el ocultamiento del IP	• ¿Considera usted que el IP oculto puede encubrir al ciberdelincuente?		
		Estafa Informática	Clona las tarjetas de crédito	• ¿Considera usted que debería de existir normas legales que regulen la compra y venta online?		

VARIABLE DEPENDIENTE	Delitos Informático			• ¿Considera usted que el programa keylogger ayuda al ciberdelincuente para sustraer dinero de las cuentas bancarias de los usuarios?		
			Envió de Publicidad engañosa	• ¿Cree usted que él envió de publicidad engañosa en el ciberespacio es un modo de estafa? • ¿Considera usted que existe una inseguridad en las compras online? • ¿Cree usted que el ciberdelincuente a través de llamadas telefónicas y/o mensajes de textos puede estafar a los usuarios?		
		Derechos a la intimidad informática	Protege la confidencialidad de los datos personales	• ¿Considera usted que el Derecho a la intimidad protege la confidencialidad de los datos personales de los usuarios? • ¿Considera usted que nuestras normas legales protegen a los usuarios en el ciberespacio? • ¿Considera usted que debería de existir una entidad que supervise y controle el uso de las redes sociales?		
		Fraude Informático	Se evalúa el delito por su consecuencia de la acción	• ¿Considera usted que el artículo 8 de la Ley 30171 está regulado de forma clara y precisa? • ¿Considera usted que el Fraude Informático es un delito de mera actividad? • ¿Considera usted que el Fraude Informático es un delito de resultado?		

ANEXO N° 04

CÓDIGO: | | | |

FECHA : | | | |

CUESTIONARIO DE ENCUESTA

ESTIMADO MAESTRO(A): EL PRESENTE CUESTIONARIO ES PARTE DE UNA INVESTIGACIÓN QUE TIENE POR FINALIDAD LA OBTENCIÓN DE INFORMACIÓN ACERCA DE LA OPINIÓN QUE USTED TIENE DE "**SOBRE LA INSEGURIDAD INFORMATICA Y LOS DELITOS INFORMATICOS**". LA CONFIDENCIALIDAD DE SUS RESPUESTAS SERÁ RESPETADA, NO ESCRIBA SU NOMBRE EN NINGÚN LUGAR DEL CUESTIONARIO.

DATOS GENERALES:

1. Edad_____ (años cumplidos)
2. Género : a) Femenino ( ) b) Masculino ( )
3. Condición laboral : a) Nombrado ( ) b) Contratado( ) c) Otro ( )

INSTRUCCIONES: Lee cada una de las frases y selecciona una de las dos alternativas, la que sea más apropiada a tu opinión, seleccionando un SI o NO que corresponde a la respuesta que escogiste según tu convicción. Marca con aspa el número, no existe respuestas buenas ni malas, asegúrate de responder a todas las opciones.

1. SI.
2. NO.

PARTE I: INSEGURIDAD INFORMATICA

ÍTEMS		1	2
SISTEMA INFORMATICO			
1	¿Considera usted que el soporte lógico del sistema informático se puede quebrantar con programas maliciosos?		
2	¿Considera usted que extraer información de dudosa procedencia a través de la web causa daños al soporte lógico?		
PROGRAMAS MALICIOSOS			
3	¿ Usted considera que el Ciberdelincuente puede ingresar a la base de datos del usuario a través de llamadas y/o mensajes de texto de números desconocidos?		
4	¿Considera usted que el usuario de manera involuntaria le puede proporcionar al ciberdelincuente el acceso a la base de sus datos?		

5	¿Cree usted que el usuario es capaz de identificar una aplicación clonada?		
6	¿Considera usted que el envió de mensajes en cadena puede permitir al ciberdelincuente el acceso a la base de datos?		
7	¿Cree usted que el programa Malverstising diseña anuncios maliciosos para robar información?		
DIRECCION IP			
8	¿Considera usted que el IP oculto puede encubrir al ciberdelincuente?		

PARTE II: DELITOS INFORMATICOS

Nº	**ÍTEMS**	**1**	**2**
1	¿Considera usted que debería de existir normas legales que regulen la compra y venta online?		
2	¿Considera usted que el programa keylogger ayuda al ciberdelincuente para sustraer dinero de las cuentas bancarias de los usuarios?		
3	¿Cree usted que él envió de publicidad engañosa en el ciberespacio es un modo de estafa?		
4	¿Considera usted que existe una inseguridad en las compras online?		
5	¿Cree usted que el ciberdelincuente a través de llamadas telefónicas y/o mensajes de textos puede estafar a los usuarios?		
DERECHO A LA INTIMIDAD			
6	¿Considera usted que el Derecho a la intimidad protege la confidencialidad de los datos personales de los usuarios?		
7	¿Considera usted que nuestras normas legales protegen a los usuarios en el ciberespacio?		

8	¿Considera usted que debería de existir una entidad que supervise y controle el uso de las redes sociales?		
FRAUDE INFORMATICO			
9	¿Considera usted que el artículo 8 de la Ley 30171 está regulado de forma clara y precisa?		
10	¿Considera usted que el Fraude Informático es un delito de mera actividad?		
11	¿Considera usted que el Fraude Informático es un delito de resultado?		

ANEXO N° 05

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

Decenio de la Igualdad de oportunidades para mujeres y hombres
Año del Bicentenario del Perú: 200 años de Independencia
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES DEL DISTRITO FISCAL DE JUNIN

PROVEÍDO N° 257-2021
Huancayo, ocho de noviembre
Del año dos mil veintiuno.

Firma Digital
Firmado digitalmente por PARIONA ALIAGA Francisco Javier FAU 20131370301 hard
Presidente De La Junta De Fiscales Superiores Del Df Ju
Motivo: Soy el autor del documento

DADO CUENTA: La solicitud de fecha 08 de noviembre de 2021 **(Exp.7194)**, presentada por la ciudadana María Isabel Alanya Rivera, Bachiller en Derecho de la Universidad Peruana "Los Andes", mediante el cual solicita a esta Presidencia, autorización para la aplicación de instrumentos de investigación (Encuesta dirigida a Fiscales de las Fiscalías Provincial Penal Corporativa de Huancayo), a fin de obtener información relacionado al proyecto de Tesis denominado *"Inseguridad Informática y los delitos informáticos del usuario en la fiscalía provincial penal corporativa de Huancayo 2019"*. En atención a lo requerido, el Ministerio Público no puede estar ajeno a las investigaciones que realizan los estudiantes y/o profesionales, por el contrario, es necesario incentivar la investigación; en consecuencia, estando a su contenido, este Despacho Superior, **AUTORIZA** a la recurrente recabar la información relacionado al Proyecto de Tesis en mención, debiendo coordinar con los entrevistados (fiscales), respetando los protocolos de bioseguridad establecidos por vuestra institución. **NOTIFÍQUESE** y **ARCHÍVESE** donde corresponde.

DR. FRANCISCO JAVIER PARIONA ALIAGA
PRESIDENTE DE LA JUNTA DE FISCALES
SUPERIORES DEL DISTRITO FISCAL DE JUNÍN

ANEXO N° 06

CONSENTIMIENTO INFORMADO

El propósito de este protocolo es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador se quedará con una copia firmada de este documento, mientras usted poseerá otra copia también firmada.

La presente investigación se titula "INSEGURIDAD INFORMATICA Y LOS DELITOS INFORMATICOS DEL USUARIO EN LA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO 2019". Esta tesis es dirigida por María Isabel Alanya Rivera, bachiller de la facultad de Derecho y Ciencias Políticas. El propósito de la investigación es determinar la influencia de la inseguridad informática en los delitos informáticos.

Para ello, se le solicita participar en una encuesta que le tomará 20 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna consulta sobre la investigación, puede formularla cuando lo estime conveniente.

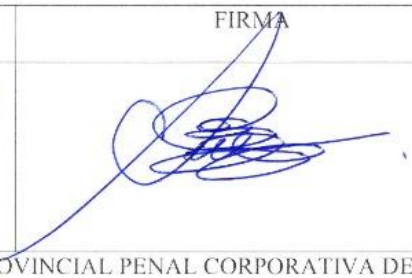
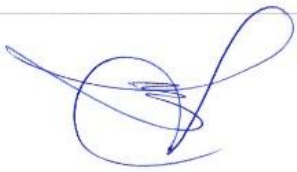
Su identidad será tratada de manera anónima, es decir, los datos obtenidos del encuestado serán utilizados con fines academicos. Asimismo, su información será analizada de manera conjunta con la respuesta de sus compañeros y servirá para la elaboración de la presente tesis.

Nombre: María Isabel Alanya Rivera

Fecha: 18 de noviembre de 2021.

Correo electrónico: mariaisabelalanyarivera@gmail.com

Firma del participante:

PRIMERA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
MARIO GROVER ORELLANA CASTILLO		20724463
SEGUNDA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
Zeidi Lozano Rodriguez		20106527
TERCERA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
Mario Lizo Olayanca		09026730
CUARTA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
CARLOS JORGE CAMPUZANO CARBAJAL		43612397

QUINTA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
Christian Gutierrez Zambrano.		70071901
SEXTA FISCALIA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO		
ENCUESTADO (Nombre y Apellido)	FIRMA	DNI
Janett Karine Santana Orihuela.		20038554

Firma del investigador:

Compromiso de Autoría

Yo, María Isabel Alanya Rivera, identificada con DNI Nª 76321232, con código estudiantil de pregrado H00305C, correo personal: mariaisabelalanyarivera@gmail.com y con numero de celular 968585731, domicilio en el Jr. Lino Mz "L" Lt. 02, distrito y provincia de Huancayo, me comprometo a asumir las consecuencias administrativas y/o penales que hubiera lugar si elaboración de mi tesis titulada "INSEGURIDAD INFORMATICA Y DELITOS INFORMATICOS DEL USUARIO FISCALÍA PROVINCIAL PENAL CORPORATIVA DE HUANCAYO 2019", se haya considerado datos falsos, falsificación, plagio, auto plagio, etc, y declaro bajo juramento que mi trabajo de investigación es de mi autoría y los datos presentados son reales y he respetado las normas internacionales de citas y referencias de las fuentes consultadas.

_____

María Isabel Alanya Rivera
DNI. 76321232