Pontificia Universidad Católica del Ecuador

Sede Ibarra

ESCUELA DE JURISPRUDENCIA

TRABAJO DE TITULACIÓN

TEMA:

DELITOS INFORMÁTICOS Y LA VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE INTEGRIDAD E INTIMIDAD

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO

LÍNEA DE INVESTIGACIÓN:

Derecho, Participación, Gobernanza, Regímenes Políticos e Institucionalidad.

AUTOR: JUAN LUCERO BURBANO

ASESOR: MSc. HUGO NAVARRO VILLACÍS

IBARRA, FEBRERO – 2023

Ibarra, 28 de febrero del 2023

MSc. Hugo Navarro Villacís

ASESOR

CERTIFICA:

Haber revisado el presente informe final de investigación, el mismo que se ajusta a las normas vigentes en la Escuela de Jurisprudencia, de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI); en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f:) .....

MSc. Hugo Navarro Villacís

C.C: 1002976924

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El Jurado examinador, aprueba el presente informe de investigación en nombre de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI).

(f): .....

MSc. Hugo Navarro Villacís

C.C: 1002976924

(f): .....

MSc. Kevin Jaramillo Vásquez

C.C: 1003485065

(f): .....

PhD. Hugo Santacruz Cruz

C.C: 1002826392

ACTA DE CESIÓN DE DERECHOS

Yo, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones, a título gratuito u oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia".

Ibarra, 28 de febrero del 2023

(f): .....

Juan Leandro Lucero Burbano

C.C: 1724519267

AUTORÍA

Yo, Juan Leandro Lucero Burbano, portador de la cédula de ciudadanía No 1724519267, declaro que la presente investigación es de total responsabilidad del y eximo expresamente a la Pontificia Universidad Católica del Ecuador Sede Ibarra de posibles reclamos o acciones legales.

(f): .....

Juan Leandro Lucero Burbano

C.C: 1724519267

DECLARACIÓN Y AUTORIZACIÓN

Yo: Juan Leandro Lucero Burbano, con C.C: 1724519267, autor del trabajo de grado intitulado: "Delitos informáticos y la violación de los derechos constitucionales de integridad e intimidad", previo a la obtención del título profesional de "Abogado" en la Escuela de Jurisprudencia

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede- Ibarra, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través del Repositorio Digital de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ibarra, 28 de febrero del 2023

(f:) .....

Juan Leandro Lucero Burbano

C.C: 1724519267

DEDICATORIA

Dedico este trabajo de investigación a mis ascendentes en primer grado de consanguinidad, José y Carmen, quienes han sido mi apoyo incondicional y gracias a su amor, paciencia y esfuerzo me permitieron lograr una de mis más grandes metas.

A mis ascendentes en segundo grado de consanguinidad, Juan y Luz, quienes son el soporte fundamental de todo y quienes con su sabiduría y cariño han sido una guía fundamental de mi camino, muchas gracias por sus oraciones.

AGRADECIMIENTO

Primeramente, le agradezco a Dios por ser mi fortaleza, acogerme con su amor y brindarme parte de su infinita sabiduría.

A la Pontificia Universidad Católica del Ecuador Sede Ibarra, mi Alma Mater, donde se me permitió desarrollarme personal y profesionalmente.

A mis docentes, de manera especial al Mgs. Hugo Navarro Villacís, gracias por haberme brindado todos sus preciados conocimientos e impartir el valioso significado de la justicia.

Gracias por permitirme cumplir mi sueño profesional.

Índice

1. Resumen y palabras clave

Los delitos son acciones contrarias a lo establecido en la ley, por lo que al cometerse deben ser sancionadas penalmente. Estas conductas se presentan como acción u omisión que pueden ser realizadas por voluntad propia, por imprudencia o negligencia y violentan el bien jurídico protegido como lo es el derecho a la intimidad personal. Los delitos informáticos son estas acciones delictivas, pero que involucran un sistema informático, es decir, una computadora o un entorno digital como medio o fin de su comisión. En razón de esto, el objetivo general fue dar a conocer si el ordenamiento jurídico nacional es un instrumento eficaz para amparar el derecho a la intimidad personal frente al impacto de los delitos informáticos. Mientras que los objetivos específicos planteados fueron identificar la causa de esta problemática y la finalidad con la que se desarrollan estas actividades; describir los mecanismos por medio de los cuales se llevan a cabo los delitos informáticos y que tan eficaces pueden ser; y analizar el alcance que pueden tener y la repercusión que causan en la intimidad personal de la víctima. La metodología utilizada fue bajo un enfoque cualitativo en razón de la selección y análisis de la información obtenida. Mientras que el nivel de profundidad fue descriptivo debido a que toman a que se toma en cuenta la descripción de varios aspectos importantes de la temática planteada. Además de esto, se utilizó el método socio-jurídico, por lo que se analizó y estudio de manera minuciosa la realidad que gira en torno a la temática de delitos informáticos y el derecho a la intimidad, en complemento a este método, se utilizó el método analítico-sintético que permitió estudiar e identificar diferentes componentes en referencia al tema propuesto en el presente trabajo de titulación. El cual se apoyó en la técnica de revisión y análisis documental, puesto que se buscó, seleccionó y analizó información de diferentes estudios e investigaciones previas sobre delitos informáticos y derecho a la intimidad. Por lo que se determinó la importancia que tienen los delitos informáticos en cuanto a su relación con el derecho a la intimidad personal.

Palabras clave: Delitos informáticos, derecho a la intimidad, sistemas informáticos, computador.

2. Abstract

Crimes are actions contrary to the provisions of the law, so when they are committed they must be criminally punished. These conducts are presented as action or omission that can be carried out by own will, imprudence or negligence and violate the protected legal right such as the right to personal privacy. Computer crimes are these criminal actions, but that involve a computer system, that is, a computer or a digital environment as a means or end of its commission. Therefore, the general objective was to find out whether the national legal system is an effective instrument to protect the right to personal privacy in the face of the impact of computer crimes. The specific objectives were to identify the cause of this problem and the purpose for which these activities are developed; to describe the mechanisms through which computer crimes are carried out and how effective they can be; and to analyze the scope they can have and the impact they cause on the victim's personal privacy. The methodology used was under a qualitative approach due to the selection and analysis of the information obtained. While the level of depth was descriptive due to the fact that it takes into account the description of several important aspects of the subject raised. In addition to this, the socio-legal method was used, so it was analyzed and studied in detail the reality that revolves around the subject of computer crimes and the right to privacy, in addition to this method, the analytical-synthetic method was used to study and identify different components in reference to the topic proposed in this degree work. This was supported by the documentary review and analysis technique, since information from different studies and previous research on computer crimes and the right to privacy was searched, selected and analyzed. Thus, the importance of computer crimes in terms of their relationship with the right to personal privacy was determined.

Keywords: Computer crimes, right to privacy, computer systems, compu

3. Introducción

El presente trabajo de investigación titulado tendrá su enfoque en los sistemas informáticos modernos y las modalidades de delitos que se pueden cometer por estos medios. Es decir, de aquellos medios tecnológicos, los cuales son cada vez más eficientes y desarrollados, facilitando a las personas ejecutar un sinnúmero de actividades las cuales se desempeñan cotidianamente y con normalidad. Permitiendo además que se agilicen varias diligencias que anteriormente necesitaban procedimientos más complejos para desarrollarse.

Asimismo, este trabajo de investigación, se enfocará en el derecho constitucional a la intimidad personal y familiar. Derecho consagrado en el artículo 66 numeral 20 de la Constitución de la República del Ecuador, el cual será el principal derecho objeto de análisis del presente trabajo. Con la finalidad de cumplir con los objetivos planteados primeramente se debe manifestar la importancia que tiene este derecho, que forma parte de los derechos de libertad y como puede ser violentado por medios informáticos. Además, se debe tener presente que la intimidad personal está íntimamente ligada con ciertos delitos informáticos, los cuales pueden afectar considerablemente a las víctimas. El Código Orgánico Integral Penal brinda una visión más amplia sobre la importancia que tiene el derecho a la intimidad. Manifestando que es un principio procesal de alta importancia y necesario para que se respete el derecho al debido proceso penal.

En este sentido, en el artículo 5, numeral 10 del COIP se menciona lo siguiente:

> Intimidad: toda persona tiene derecho a su intimidad personal y familiar. No podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente, con arreglo a las formalidades y motivos previamente definidos, salvo los casos de excepción previstos en este Código. (Asamblea Nacional de Ecuador. 2014).

El derecho a la intimidad garantiza que las personas mantengan en privado su vida familiar y personal. Esto incluye tanto datos personales como información sobre sus actividades laborales, su residencia, domicilio y demás aspectos de la intimidad de una persona. La legislación ecuatoriana garantiza el respeto de los derechos consagrados en los diferentes cuerpos normativos y establece las reglas para actuar cuando sea necesario algún procedimiento.

Es notable todo el progreso que ha tenido la normativa vigente y los sistemas informáticos durante los últimos años, esto ha sido de beneficio para la sociedad en general, pero también ha

desatado nuevas modalidades de delitos en el área informática. Delitos que involucran a medios digitales son constantes conforme se actualizan las nuevas tecnologías. Todas las personas están propensas a ser víctimas de un atentado bajo esta modalidad, lo que podría afectar considerablemente los derechos del perjudicado, comprometiendo información y datos privados de gran importancia. Violentando notablemente el derecho a la intimidad personal de la víctima, pudiendo revelar secretos o información de carácter personal concernientes únicamente a esa persona. En virtud de lo que se ha expuesto se formuló la siguiente pregunta de investigación:

¿Es el ordenamiento jurídico nacional un instrumento eficaz para amparar el derecho a la intimidad frente a los delitos informáticos?

De ahí que en el mismo contexto se formule el Objetivo General de esta investigación: Dar a conocer si el ordenamiento jurídico nacional es un instrumento eficaz para amparar el derecho a la intimidad personal frente al impacto de los delitos informáticos. En este sentido, se han planteado los siguientes objetivos específicos: 1. Identificar la causa de esta problemática y la finalidad con la que se desarrollan estas actividades. 2. Describir los mecanismos por medio de los cuales se llevan a cabo los delitos informáticos y que tan eficaces pueden ser. 3. Analizar el alcance que pueden tener y la repercusión que causan en la intimidad personal de la víctima.

Actualmente, convivimos en una sociedad moderna y digitalizada, los medios electrónicos y sistemas informáticos son elementos fundamentales de la vida cotidiana. La tecnología está presente en todas casi todos los rincones existentes, desde lo más estándar como un ordenador con acceso a internet en los hogares de las personas, hasta sistemas más complejos que son utilizados por grandes corporaciones para el desarrollo de sus actividades como la inteligencia artificial. Demostrando el avance que ha tenido la ciencia en el área informática y la importancia que tiene actualmente. Esto brinda una idea básica del desarrollo que se espera en los próximos años. Un avance que seguramente será de gran ayuda para realizar un sinnúmero labores, siendo de gran beneficio para la sociedad en general. En cuanto a lo antes referido, Calvo (2014), manifiesta:

> Aún con todo, aunque una sociedad “no quiera cambiar”, así lo termina haciendo con el transcurso del tiempo, porque, con independencia del nivel de desarrollo económico, político o social, suelen existir presiones del entorno externo. Este conjunto de cambios ocasiona una evolución, la que a su vez impacta sobre el Derecho, el cual,

> consecuentemente, ha de variar; pues parece obvio que la evolución social se vea reflejada jurídicamente. (p. 9).

Que una sociedad avance es algo inminente, este desarrollo implica cambios inevitables, por lo tanto, el Derecho debe ajustarse a las necesidades de una sociedad cambiante. Las leyes deben garantizar el bien común y el control social, regulando las actividades sociales que a diario se transforman y desarrollan. Conforme al entorno o lo que pueda surgir y cambiar dentro de este, las personas adoptan nuevos hábitos, ya sea en favor o no de su desarrollo personal, por lo que estas conductas deben estar reguladas jurídicamente en caso de que sean un instrumento para alterar el orden social y la tranquilidad de los ciudadanos.

Desarrollo y actualización son elementos indispensables de la tecnología, es algo inminente y que se puede observar a diario. Estos avances son de utilidad para las personas y de provecho en general, desafortunadamente al vivir en una sociedad que no está exenta de delitos y conductas inapropiadas, cualquier herramienta puede ser utilizada para cometer atentados contra el colectivo social. La tecnología moderna no es la excepción, por lo que un sistema informático se ha convertido en una herramienta eficaz utilizada por delincuente informático para dañar a las personas y lesionar sus derechos. Los cibercriminales han aprovechado los recursos tecnológicos a su disposición para cometer ilícitos y obtener un beneficio personal sin importar el perjuicio que puedan causar en las víctimas.

La relevancia del presente proyecto de investigación se basa en los dominios académicos y líneas de investigación de la Pontificia Universidad Católica del Ecuador, aplicando especialmente la línea de investigación número 13, y la sub línea de investigación Fundamentos y principios del derecho en sus distintos ámbitos y aplicaciones en relación con el Plan Nacional Creación de Oportunidades, en su Eje Seguridad Integral, Objetivo 9 Garantizar la seguridad ciudadana, orden público y gestión de riesgos.

4. Estado del arte

La masificación, actualización y progreso de la tecnología, además de su fácil accesibilidad, tiene un impacto muy profundo en nuestra sociedad, porque demuestra la gran exposición en la que todos estamos inmersos frente a una era en la cual la tecnología predomina. Por lo tanto, el Derecho como sistema encargado de regular la conducta de las personas se debe ajustar a los escenarios que pueden surgir con base a esta temática. Adoptando una posición en la que regule de manera eficaz los efectos jurídicos que se produzcan de la informática y actividades realizadas por los cibercriminales, para que se puedan proteger efectivamente los derechos constitucionales de los ciudadanos.

4.1 El Ecuador como un Estado de derechos

Es fundamental mencionar que, en nuestro país, todas las instituciones, entidades y personas están sometidas a la ley, incluyendo al propio Estado ecuatoriano, por lo que el Ecuador es un Estado constitucional de derechos, tal y como se encuentra consagrado en el artículo 1 de la Constitución de la República del Ecuador (2008) "El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada". (art. 1)

Por medio de esto se manifiesta que tenemos un Estado garantista, en el que prevalece la Constitucion y cuya aplicación es directa y también obligatoria para todos de manera general, con la finadalid de tutelar y amparar correctamente los derechos de los ciudadanos. Es obligación del Estado promover, respetar y garantizar esos derechos, ya que por medio de estos se preserva la dignidad humana, la cual es fundamental para poder tener un correcto desaroolo social, el cual puede fundamentarse en la conducta que desarrollen las personas en torno al ambiente estatal que se encuentren.

En conformidad con lo antes mencionado, Ávila Santamaría (2008) menciona lo siguiente:

> La constitución determina el contenido de la ley, el acceso y el ejercicio de la autoridad y la estructura de poder. La constitución es material, orgánica y procedimental. Material porque tiene derechos que serán protegidos con particular importancia que, a su vez, serán el fin del Estado; orgánica porque determina los órganos que forman parte del Estado y que son los llamados a garantizar los derechos; procedimental porque se establecen mecanismos de participación que procuran que los debates públicos sean

> informados y reglados, tanto para la toma de decisiones como para la elaboración de normas jurídicas. (p. 22)

La Constitución de la República del Ecuador es la normativa que jerárquicamente se constituye como la máxima expresión legal del Estado Ecuatoriano, a esta norma suprema se somete toda legislación ecuatoriana. Por medio de la Constitución se regula el poder estatal, se reconoce la soberanía nacional, básicamente se regula el Estado. Todos los derechos consagrados en la Carta Magna deben ser respetados y protegidos, son de gran importancia porque simbolizan un buen vivir de los ciudadanos, es decir, tener una vida digna y que las personas vivan como seres humanos en pleno goce de sus derechos, pero cumpliendo también, sus obligaciones. De la misma manera, la Constitución es una herramienta que precisa los medios que son utilizados por la administración pública para que se determine una correcta función estatal a fin de garantizar los derechos y evitar que estos puedan ser violentados. Se establecen diferentes mecanismos de participación, ya sea para elaborar leyes, promover la participación ciudadana y tomar decisiones. La aplicación directa de la Constitución como norma suprema y su amplio campo de aplicación brinda la noción de lo bien formada que se encuentra, para evitar toda arbitrariedad contra los ciudadanos y representar el garantismo del Estado ecuatoriano.

Dentro del mismo contexto y siguiendo la concepcion del tema, Grijalva (2012) indica que:

> Esta universalización de la capacidad para reclamar derechos se corrobora también en una ampliación y desarrollo de las garantías constitucionales. Las garantías en sentido amplio son los medios de los que disponen los ciudadanos para hacer efectivos sus derechos constitucionales. La Constitución de 2008 amplia y fortalece estas garantías. (p. 29)

Conforme a lo antes expuesto, el autor resalta la amplia cantidad de garantías constitucionales con las que cuenta la Carta Magna. Estos medios son sumamente importantes, ya que de presentarse el caso de transgredirse un derecho constitucional, se pueda reparar a través de estos mecanismos que están a disposición de los ciudadanos. De esta manera se puede defender los derechos frente a otros individuos o grupos. De esta manera los ciudadanos tienen la certeza de que se pueden corregir los defectos que afectan al correcto funcionamiento estatal, pero a pesar de contar con esto, es dificl que una reparacion vuelvo a establecer en otimas condiciones a una victima de violacion de derechos.

4.2 Delitos informaticos como un comportamiento criminal

Los delitos son acciones que causan daño dentro de la sociedad porque van en contra de lo que establece la ley. Estos comportamientos criminales se encuentran tipificados y son sancionados, pero existen conductas criminales en las que una computadora está involucrada. Por lo que esta modalidad de delincuencia tiene la característica de usar estas herramientas para cometer el ilícito. De esta manera, y en conformidad a lo antes mencionado se puede establecer una decisión precisa de lo que realmente sígnica esto, algo que manifiesta a continuación, Acurio (2015) al establecer que:

> Delincuencia Informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera. (p. 48).

Se puede percibir que las actividades que se desarrollan con la intervención de un sistema informático o medio digital son habituales en la cotidianidad de una persona, ya sea por razones laborales o de entretenimiento personal. Por esta causa, las acciones ilícitas realizadas por los cibercriminales que quebrantan los derechos de las personas son algo a tener en cuenta, ya que se realizan por medios informáticos y son constantes. Estos delitos tienen un factor fundamental, el cual es que las tecnicas y funciones que se desempeñaron ya sea como medio, método o fin son las que involucran sistemas informáticos. En estos mismo terminos Fernández y Martínez (2020) exponen que:

> Los delitos informaticos son delitos convencionales que toman nueva vida con el uso de las Tecnologías de la Información y la Comunicación (no representan un tipo de criminalidad específica y tienen lugar en el ciberespacio), que se caracterizan por el uso de redes de transmisión de datos y por su relación con los sistemas informáticos, y, que pueden afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (p. 28)

Los delitos cibernéticos son una variación de los delitos tradicionales, es decir, son una transformación de los comportamientos delictivos ejecutados por criminales de manera regular. Al ser delitos que presentan la particularidad de que se cometen mediante el uso de sistemas informáticos, su zona de desarrollo es el espacio cibernético, por lo que poseen una amplia área de desarrollo de difícil rastreo. Naturalmente, al ser actos delictivos, pueden afectar objetos de

valor en el área jurídica como lo son los bienes jurídicos de las personas, ocasionando que se afecten negativamente los derechos.

La tegnología moderna e ha consolidado fuertemente, tanto que es fundamental para realizar un sin numero de actividades diarias. Por lo tanto es llamativo para los criminales que buscan lucrarse por medio de la utilizacion de medios informaticos. La tegnologia representa una herramienta creada para el beneficio de la sociedd en general, pero al no estar excentos de actos criminales, esta se potencializa como un arma utilizada por cibercriminales. En contexto a esto, Trujillo (2021) expresa que:

> Al constituirse la tecnología como una puerta a la comodidad y a la rentabilidad, es sumamente atractiva para la mente criminal. Y, por ende, también se ubica como un medio en el cual se ejerce una actuación delictiva, de tal forma que la acción cibercriminal se materializa en el mundo real. La ciberdelincuencia se potencializa, al apreciar que la mayor parte de las actividades humanas hoy se realizan a través de la web. (p 35)

La tecnología moderna constituye una herramienta fundamental para la sociedad, debido a que es de beneficio general por su amplio uso en diferentes áreas. Es un medio para adquirir beneficios mutuos al desarrollar actividades que en ocasiones no cualquier persona está capacitada para realizarlas. Esto ha generado ser llamativo para quienes buscan delinquir, y los medios informáticos son una herramienta adecuada para poder hacerlo. Quienes aplican sus conocimientos desarrollando actividades fuera de la ley causaran efectos nocivos en quienes sean sus víctimas, generando consecuencias negativas como en cualquier otro delito. Idea que Téllez (2009), amplia, manifestando lo siguiente:

> Las personas que cometen dichos delitos poseen ciertas características que no presentan el denominador común de los delincuentes. Esto es, los sujetos activos tienen habilidad para manejar los sistemas informáticos y en general por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible; o son hábiles en el uso de los sistemas informatizados. (p. 188).

Por consiguiente, a lo antes manifestado, la particularidad que tiene los delincuentes informáticos es un amplio conocimiento en el área de la informática, ya sea porque es su posición profesional o porque simplemente su conocimiento es amplio en estas ciencias. Una característica a tener en cuenta es que los delitos informáticos se realizan por medio de un

ordenador y se pueden efectuar desde casi cualquier lugar, logrando un alcance inmensurable, por lo que identificar al responsable y dar con su ubicación puede llegar a ser realmente complicado, dando como resultado que una investigacion pena para identificar al resonsable se turbe y llegue a sser archivada. En contexto a esta opinion, Barrio (2018) da a conocer lo siguiente:

> El Derecho penal y procesal penal clásico, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de delincuencia física, marginal e individual. Sin embargo, la aparición de la informática primero, de Internet después y ahora de las tecnologías disruptivas ha resquebrajado este paradigma, al tiempo que los distintos organismos encargados de su represión se han ido enfrentando a un cauce de ejecución criminal capaz de cuestionar muchos de los principios tradicionales de la investigación penal. (pp. 29-30)

La función de la norma jurídico penal es encaminar el comportamiento de las personas dentro de la sociedad, esto se lo hace prohibiendo determinados comportamientos de riesgo que alteren la tranquilidad del colectivo social. Esto ha sido consolidado teniendo en cuenta elementos como la conducta ante una determinada situación, dando como resultado el Derecho penal actual que ha sido construido con base a las conductas que surgían y debían ser observadas y posteriormente reguladas. El comienzo de la era de la informática origino nuevas conductas, las cuales debían ser observadas y de ser necesario restringidas, extendiendo así el área de ejecución de los delitos.

4.3 Seguridad informática como un mecanismo de protección

La existencia de los delitos que se cometen por medios informaticos es evidente, el desarrollo que tienen dentro de la sociedad ecuatoriana es visible dentro del sistema judicial. Pero asi mismo existen instrumento de proteccion para poder afrontar estos peligro informaticos. La ciberseguridad es una serie de medidas de protección que impiden la ejecucion de acciones y operaciones no autorizadas dentro de los sistemas informaticas. Son mecanismo preventivos que brindan seguridad ante cualquier eventualidad. Hernandéz, Arroyo y Gayoso (2020) dan a conocer una amplia definicion de lo antes expuesto.

> La ciberseguridad surge como mecanismo de control del ciberriesgo. De forma más precisa, podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada

> a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización. (p. 12)

Para poder afrontar la exposición a un riesgo se deben tomar medidas de prevención, esto no solamente se lo hace en el Derecho, sino también en el área informática, donde frente una fragilidad que puede ser aprovechada para cometer un delito que posteriormente afecte los derechos de las personas que sean víctimas, se toman medidas. Así como la Constitución de la República del Ecuador consagra derechos y garantías para amparar a las personas, en informática la manera de hacer frente a los ciberriesgos y resguardar los activos de las personas es por medio de la ciberseguridad. En ambos casos, la finalidad con la que de salvaguardar elementos importantes es para la protección de las personas. Ademas de esto, y en relacion con lo anteriormente establecido. Gómez (2011), brinda una conceptualización personal con la que define a la seguridad informática.

> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (p. 5).

Con base a esto se hace saber que la manipulación de un sistema informático con la finalidad de acceder a bases de datos u obtener información personal ajena es una intervención que entorpece y causa daños sobre la información y la persona que es víctima. Desarrollar esta actividad compromete la intimidad personal de la persona y lesiona sus derechos. La seguridad informática es el mecanismo que se emplea para poder sofrenar esta actividad y evitar que los delincuentes informáticos cumplan su finalidad, brindando una herramienta para evitar que se tenga como consecuencia un delito que violente los derechos de las personas que hacen uso frecuente de los medios informáticos.

Alcívar (2015), contribuye a todo lo expresado, manifestando la importancia del cibercrimen y el alcance casi ilimitado que puede tener, tal y como menciona a coninuación:

> La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de

> la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. (p. 63).

El alcance que se logra obtener al momento de cometer un ilícito con el uso de un medio informático queda evidenciado, lógicamente, porque su modalidad de desarrollo y alcance es mayor al que se obtiene cuando se cometen los delitos tradicionales. Sumando la constante evolución de la programación y de los sistemas informáticos, los delitos informáticos son más habituales y recientes. Se utilizan un sinnúmero de herramientas modernas para infringir la seguridad de un sistema y poder violentar su privacidad. Debido al espacio donde estos crimenes de desarrollan, su alcanse aumenta considerablemente, puesto que es espacio digital es amplio y dificl de controlar y rastrear. Beneficios que los crimales informáticos han aprovechado perfectamente. Tal y como Costas (2015) lo expone expresamente.

> Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espias, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. (p. 29)

La exposición que se tiene al momento de navegar en internet por medio de un ordenador es considerable. Dependiendo de las actividades que se desarrollen y de sí el dispositivo cuenta con los filtros de seguridad necesarios para brindar una protección, se puede estar brindando entrada libre a nuestro sistema. Creando una exposición que puede ser aprovechada para obtener datos e información, que posteriormente puede ser utilizada para cometer actividades ilícitas, que en muchos casos comprometen a personas que son inocentes. Lo que evidencia muchas veces la capacidad que tiene los ciberdelincuentes para actuar, pero asi mismo deja en evidencia la inatención de las personas hacia los instrumentos informáticos que utilizan, puesto que el descuido y la falta de protección de una computadora puede determinar si es blanco facil de los cibercriminales. Por lo que contar con un sistema de protección es una garantia de tener mejor seguridad, asi como Escrivá (2013) lo determina, indicando que:

> En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a estas herramientas, como las orientadas a explotar las debilidades del factor humano. Es el caso de la ingeniería social, que consiste en la obtención de información

> confidencial y/o sensible de un usuario mediante métodos que son propios de la condición humana. (p. 11)

La Constitución de la República del Ecuador garantiza el efectivo goce de los derechos que han sido establecidos. El Código Orgánico integral Penal regula el ejercicio punitivo y preventivo del estado Ecuatoriano. Estos son mecanismo por medio de los cuales se garantiza el ejercicio de derechos y responsabilidades. De igual manera, en informática se brindan herramientas de seguridad para conseguir la protección frente a las transgresiones que se puedan presentar. Estas transgresiones violentarían el sistema informático de un ordenador, por consecuente la información del usuario estaría expuesta y si es de utilidad para el ciberdelincuente sería robada para posteriormente ser mal utilizada, acción que causaría daño y violentaría el efectivo goce de derechos que tiene el ciudadano.

4.4 Información y datos personales

La información personal de los ciudadanos es súmansete importante, solo le concierne a su portador. Caso contrario, el derecho constitucional a la intimidad puede verse afectado cuando una persona ajena accede sin autorización a datos personales, los cuales, según Cuadros (2019), se conceptualizan como "Toda información que identifica directa o indirectamente a una persona natural, como por ejemplo nuestros nombres completos, el correo electrónico, número de cédula de ciudadanía, matrícula del carro, fotografías, entre otros" (p. 72). Por lo tanto se está quebrantando el bien jurídico protegido que representa esta información personal, la cual es cualquier dato que esté relacionado a una persona y que con base a esto se la pueda identificar y revelar aspectos íntimos e importantes de su vida personal. En cuestión, esto es de suma importancia, por lo que Castro (2019) manifiestan que:

> La constante incorporación de plataformas digitales a distintos aspectos de las actividades humanas supone una mayor recolección de información personal en tiempo real. Los datos recopilados, puede ser el medio para detectar hábitos de consumo, intereses, interacciones personales, emociones, sentimientos, estados de ánimo, intenciones futuras y hasta predicciones de las relaciones que surgirán entre los internautas. (p. 1).

Conforme se desarrollan y actualizan los sistemas digitales, surgen nuevos desafíos para poder intervenir y majenar correctamente la gran cantidad de información que será recolectada y todas las actividades que a esto concierne. La intervención humana es fundamental para que ciertos

sistemas cumplan su propósito y almacenen información en conformidad con nuestra actividad informática. Esto permite que sistemas de alto nivel e inteligencia artificial puedan anticipar nuestras necesidades en un futuro y nos brinden mejores resultados. Por lo que todo esto, tambien debe contar con el respaldo y protección necesaria para salvaguardar la intimidad de las personas y todo lo que se haya recolectadao referente a cualquier individuo. Por otra parte, Quispe (2019) brinda una visión novedosa en cuanto a los datos personales.

> Los datos personales son un tema que se enfoca desde un nuevo paradigma de la privacidad de la era digital y se encuentra en varios aspectos que se origina en la sociedad y que aún no son centro de explicación, que, en defensa, hay que indicar el alcance jurídico a partir del delito tipificado con los contratos de las redes sociales sobre la cláusula de confidencialidad y reserva. (p. 2).

La recopilación de datos personales que se da por medio de sistemas informáticos o plataformas digitales es inminente. Para ser beneficiarios de herramientas y funciones que brindan aplicaciones o programas es necesario acceder a desvelar nuestra privacidad hasta un cierto nivel. Por ejemplo, para utilizar una aplicación móvil de GPS con todos los beneficios que esta nos brinda, permitiéndonos encontrar una dirección específica, es necesario acceder a brindar nuestra ubicación para obtener resultados positivos. Por lo que de esta y de infinidad de formas se recopilan datos de carácter personal que en cualquier momento pueden ser violentados por una tercera persona con altos niveles de conocimiento que acceda a sistemas de bases de datos con la finalidad de cometer un ilícito y beneficiarse. Explicación que se complementa con lo que Baca (2016) mnifiesta, al afirmar que:

> Los riesgos a que está expuesta la información, se conocen como fisicos y lógicos, Los riesgos fisicos son el daño que puede sufrir el hardware y en general las instalaciones del centro o área de cómputo de la empresa (…) Por su parte, todos los riesgos lógicos conocidos han sido creados y siguen siendo creados por personas que tienen la intencion de dañar o robar información de los sistemas informáticos empresariales o de las computadoras personales de un hogar. (p. 15)

Tanto la información personal como la herramienta informática donde está se encuentra puede verse afectada en cualquier momento y por distintas razones. Con la característica de que el hardware, es decir, la parte tangible y física del ordenador, se puede estropear por un error humano sin intención o un accidente, lo que puede afectar al software, es decir, a la parte

intangible del ordenador como programas e información y datos valiosos. Sin embargo, un daño o una inconsistencia en el software puede representar indicador de que el daño fue hecho con alguna intención y por una tercera persona.

Gil (2022) manifiesta que: “En la actualidad, prácticamente todas nuestras acciones cotidianas generan datos que son recogidos y almacenados. La capacidad de recoger y almacenar datos para extraer valor de ellos hace que las fuentes de los datos se hayan diversificado enormemente”. (pág. 36) El historial de actividad y movimientos que una persona tiene al navegar por internet genera datos, ya sea para beneficio del usuario o para innovar en las actividades que se pueden realizar. Se utilizan herramientas como los algoritmos con la finalidad de ordenar el contenido y guardar las preferencias del usuario para mejorar el servicio que se presta. Todo esto es información importante, ya que por mínima que sea la actividad digital que tiene una persona, solamente con esto se llegaría a saber las preferencias de búsqueda y temas de interés del usuario.

4.5 Derecho a la intimidad personal

Toda persona tiene derecho a mantener asuntos como sus datos personales y cuestiones de su vida personal en privado, sin la obligación de compartir esto a menos que sea por su propia voluntad. Por lo tanto, esta información de carácter restringido solo le consierne al individuo, sin que este sea objeto de injerencias arbitrarias en su vida persona, familiar o en contra de su honra y reputación. Al respecto de esto, Nogueira (1998) manifiesta la importancia de la intimidad y porque es fundamental que esta sea preservado solamente a quien le corresponde.

> La intimidad es el ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana. El derecho a la intimidad es la facultad de la persona para evitar las injerencias de terceros en el ámbito de su privacidad, salvo la autorización de tal develamiento de la intimidad por el propio afectado. La intimidad de la persona es una zona intrínsecamente lícita, que merece respeto y protección a nivel constitucional. (p. 68).

Conforme manifiesta el autor, la intimidad es un valor intrínseco de las personas, un elemento intangible que opera conjuntamente con la dignidad, y al constituirse como un bien primordial del individuo, requiere de un reconocimiento vinculante que garantice su eficaz protección y que los hechos ejecutados por cada uno guarden su privacidad y el respeto de los demás en

cuanto a lo que le es ajeno a sí mismo. Con respecto a lo antes mencionado Rios y Villega (2021) indican el valor de tener presente la importancia de la intimidad,

> El derecho a la intimidad, es un tema que debería interesarle a toda la sociedad, puesto que las nuevas tecnologías que existen actualmente, son instrumentos que almacenan, planifican, regulan, controlan y transmiten todo tipo de información, que puede afectar a cualquier persona expuesta; debido a que existe gran facilidad en reproducción y publicación e información que están relacionados a los bienes jurídicos objeto de este estudio. (párr. 9)

Como manifiesta el autor, la importancia del derecho a la intimidad es algo que debería ser de interés social, aún más cuando la privacidad que las personas buscan mantener fuera del alcance de terceros puede ser expuesta y reproducida fácilmente un sinnúmero de veces por medio de las nuevas tecnologías. Teniendo un alcance tan grande que incluso puede ser pasado desapercibido por la víctima.

De acuerdo con Poquet (2018) "Toda persona tiene derecho para decidir por sí misma, de qué datos pueden disponer y en qué condiciones pueden ser revelados, en la medida en que forman parte de su intimidad" (p. 118).

La autora destaca la libertad de cada individuo para decidir conforme a su voluntad sobre sus datos e información y en que medida podrán estar disponibles y develarse. Por lo que la intimidad de cada persona depende ligeramente de sí misma, de acuerdo a la cantidad de información que se haya compartido y la constancia de su actividad digital. Por esta razón, los datos que pueden existir de una persona, no precisamente pueden ser íntimos y delicados.

En este mismo contexto, Rodríguez & Magdalena (2015) indican la importancia de conocer las consecuencias de la mala utilización de una herramienta digital:

> Se observa una falta de conciencia y sensibilización acerca de los problemas que puede llegar a ocasionar un mal uso de estas herramientas virtuales, tanto a su intimidad personal como a su propia imagen, es decir, muchos jóvenes emplean las redes sociales sin ningún tipo de control, ofreciendo gran información acerca de sus vidas, que puede ser empleada de forma poco ética por otros usuarios del mundo virtual. (p. 45).

Cantidades considerables de información son adquiridas al momento de utilizar una herramienta digital, esto se hace con la finalidad de mejorar y desarrollar servicios. Y aunque

existen políticas de privacidad, que brindan una idea directa de como se almacenan y usan los datos receptados y cuya información está explicada con fundamentos jurídicos. También existen páginas que almacenan información para aprovecharse de la intimidad y privacidad de las personas que acceden a ellas.

Lorca (2017) “La intimidad de las personas es un derecho natural consagrado en la mayoría de constituciones a nivel mundial, las mismas que garantizan a los ciudadanos el derecho de reservarse información de su vida privada” (p. 5).

La intimidad constituye un derecho fundamental que garantiza la privacidad de una persona sin la intromisión de terceros. En virtud de esto, el ser humano cuenta con la facultad de excluir aspectos de su vida hacia los demás, permitiendo al individuo el libre desenvolvimiento y desarrollo de su vida personal.

5. Materiales y metodos

Para la elaboración del presente trabajo de investigación se utilizó el enfoque cualitativo, esto en razón de la búsqueda, selección y análisis de toda la información recolectada acerca de los delitos informáticos y las características que estos presentan. Para lo cual se toma en consideración el peligro y el alcance que estos representan dentro de una sociedad consolidada y regulada por un conjunto de normas consagradas en diferentes cuerpos normativos que desarrollan los preceptos de un país, como lo es el Ecuador. Donde derechos como la intimidad personal son sumamente esenciales en la vida de los ciudadanos, para fomentar su desarrollo y preservar su seguridad, dignidad y demás derechos y garantías consolidadas en la Constitución de la República por parte del Estado ecuatoriano.

El nivel de profundidad de esta investigación fue descriptivo, debido a que se toman en cuenta facetas importantes de las ciencias informáticas y cuestiones aún más relevantes de las ciencias jurídicas. Orientándose en analizar y cuidadosamente entrecruzar jurídicamente la información conseguida referente a la informática, debido a que fue conveniente realizar un análisis intercalado para obtener resultados que suplementen la información obtenida referente a cada una de estas ciencias. Complementando a la par elementos relevantes de los que resulta un análisis de utilidad para el proyecto.

Se utilizó el método socio-jurídico, permitiendo estudiar minuciosamente la realidad referente al derecho a la intimidad personal y la incidencia que los delitos informáticos tienen en las víctimas. Determinando el nivel eficiencia del ordenamiento jurídico nacional y percibiendo la celeridad de actualización de la informática. En complemento a esto se utilizó el método analítico-sintético, puesto que de manera general se analizó el fenómeno que es objeto de estudio en este trabajo, y se identificó a los múltiples componentes que existen para posteriormente analizar analógicamente esta información.

Como técnicas de investigación se utilizó la revisión y análisis documental, debido a que se buscó, seleccionó y analizó información de diferentes estudios e investigaciones previas sobre delitos informáticos y derecho a la intimidad. Estas fuentes se obtuvieron indagando en bases de datos, repositorios digitales, bibliotecas físicas y virtuales que contienen publicaciones de libros, revistas jurídicas, artículos científicos e investigaciones nacionales e internacionales actualizadas que ostentan valor científico y que fueron de utilidad para desarrollar la investigación en relación con el tema planteado.

Para responder correctamente a la pregunta planteada se ejecutó un proceso de investigación que posteriormente condujo a la obtención de resultados, por medio del análisis documental de contenido, obteniendo información de calidad y de fuentes verídicas para responder la pregunta de investigación de manera correcta y cumplir con los objetivos establecidos. Sumado a esto se aplicó la técnica de la entrevista, la cual es necesaria porque de esta manera se podrá obtener información relevante mediante un diálogo con personas profesionales y entendidos en el tema de los delitos informáticos y el derecho a la intimidad.

La entrevista fue estructurada y se aplicó a un grupo de tres profesionales del Derecho penal, por medio de un cuestionario de seis preguntas abiertas sobre la el tema de investigación, de esta manera se puedo conseguir información relevante para posteriormente obtener resultados idóneos y poder llegar a las conclusiones correctas. Las entrevistas se aplicaron a fiscales por cuanto su función principal la representación de los intereses de la sociedad frente a una vulneración de derechos que se dan por medio de los delitos. Esto se lo hizo porque con base a su amplia experiencia laboral, ya que su aporte brindó información profunda y detallada de la que el entrevistador no tenía conocimiento previo.

6. Resultados y discusión

En este apartado de la investigación se expondrán y manifestarán los hallazgos de la selección, revisión y análisis de las diferentes fuentes documentales que se analizaron, las cuales son estudios previos en relación con la temática tanto de delitos informáticos como del derecho a la intimidad. Estas fuentes se obtuvieron investigando fichas bibliografías tanto físicas como virtuales, las cuales contienen información relevante de investigaciones, datos y documentos científicos relacionados directamente con la pregunta de investigación y con los objetivos establecidos en el proyecto.

De la misma manera se analizará la técnica de la entrevista, la cual permitió obtener información de profesionales que expresan libre y coherentemente su opinión y sus ideas referentes al tema del presente proyecto. Para posteriormente interpretar de manera correcta los resultados obtenidos en relación con los objetivos planteados. Detallando el resultado que tuvo la investigación, para finalmente concluir con la discusión, apartado en el cual se compran y confrontan los resultados de esta investigación con otros trabajos y con los resultados de las entrevistas realizadas.

6.1 Resultados

6.1.1 Resultados de la técnica de revisión documental

En este apartado se expondrán los resultados obtenidos de la respectiva revisión y análisis de las diferentes fuentes documentales que han sido consultadas, las cuales guardan relación directa con los objetivos específicos presentados en la investigación. Los cuáles serán presentados a manera de resultados claros y concretos. Demostrando sustentación y veracidad de cada uno de ellos, los cuales son: 1. Identificar la causa de esta problemática y la finalidad con la que se desarrollan estas actividades. 2. Describir los mecanismos por medio de los cuales se llevan a cabo los delitos informáticos y que tan eficaces pueden ser. 3. Analizar el alcance que pueden tener y la repercusión que causan en la intimidad personal de la víctima.

De esta manera, el resultado del primer objetivo específico correspondió a la necesidad de reconocer la procedencia de los delitos informáticos existentes, para lo cual primeramente se establecerá una directriz enfocada dentro de la sociedad, y, sobre todo, como entender esta cuestión es importante para percibir porque se cumplió el primer objetivo específico de manera correcta. Es así que tomando la postura de Repetto (2022) se menciona que conducta es toda acción por medio de la cual las personas manifiestan su comportamiento. Por lo tanto, debe ser

algo materializado y llevado a cabo, no solamente algo interiorizado o fantaseado por el individuo.

Mientras que el Código Orgánico Integral Penal (2014) establece en un sentido jurídico que "Infracción penal. - Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código" (art. 18). De esta manera se determinan las acciones que caracterizan a una conducta delictiva, puesto que el ser humano tiene libre albedrío, es decir, la habilidad de decidir libre y voluntariamente como actuar y conforme a su voluntad. Por lo tanto, una persona podría actuar con base a la ética y la moral, o actuar maliciosamente sin importar el perjuicio de sus acciones en las demás personas.

Respecto a esto, Encalada (2015) "El derecho existe en tanto regula las relaciones humanas, de modo que la conducta humana es el punto de partida de toda reacción jurídico-penal" (párr. 44). La importancia de un sistema normativo que regula el comportamiento externo de las personas es necesario para imponerse coactivamente sobre las conductas que el colectivo social pueda adoptar que causen perjuicio. Por lo tanto, es de suma importancia establecer responsabilidad penal cuando una conducta sea criminal, de esta manera se puede concatenar lo jurídico y lo social, permitiendo focalizar si el accionar social cometido requiere intervención penal.

Por esta razón, y en consecuencia del desarrollo que tiene la tecnología informática moderna, se han potencializado nuevas posibilidades de procedimientos fraudulentos relacionados con estos medios electrónicos. Algo que Fernández y Martínez (2020) exponen comprensiblemente al indicar que los delitos informáticos se originan en consecuencia a la variedad de instrumentos modernos que existen actualmente. Estos se producen de los delitos tradicionales, puesto que al coexistir en una sociedad donde tenemos herramientas tan extraordinarias y eficientes como la informática y el internet, estos son medios que en algún momento darán lugar a que sean mal utilizados. Causando que se brinde paso a nuevas modalidades delictivas como son los delitos informáticos. Por medio de estos delitos se puede afectar los derechos de las personas, y de esta manera es como la informática y las acciones negativas que se deriven de esta ciencia guardan una estrecha relación con el derecho a la intimidad, el cual puede verse afectado cuando un criminal comete actos ilícitos por estos medios.

Primeramente, se debe mencionar que las leyes no son normas morales, en consecuencia, se puede determinar que la principal causa de la problemática que se produce en torno a los delitos informáticos no es el acelerado desarrollo tecnológico que tiene impactos masivos en nuestra sociedad, ni el fácil acceso a un ordenador o internet. Si no la conducta criminal de los

individuos, la cual aflora y se exterioriza, y debido a la abundante cantidad de recursos, surgen estas conductas criminales, aprovechándose las herramientas modernas con las que se cuenta gracias a un amplio desarrollo informático. Además de esto, el entorno social en el que nos encontramos actualmente tiene un rol importante, ya que al encontrarnos sumergidos es una era digital, las herramientas de esta categoría son de uso diario.

Para complementar lo antes expuesto y en relación con el primer objetivo específico, Trujillo (2021) indica que la tecnología se ha fundamentado fuertemente en la sociedad moderna, brindando una infinidad de herramientas que permiten realizan un sinnúmero de actividades que tienen un gran alcance, algo que capta la atención de las mentes criminales que buscan lucrarse y beneficiarse. Sumado a los amplios beneficios que brinda la utilización de un sistema informático, es un medio atractivo para delinquir. De esta manera surgen las modalidades delictivas por medio de herramientas informáticas, puesto que la rentabilidad que se logra es similar o incluso mayor al cometer delitos fuera de estos sistemas, pero afectando a la víctima como si de un delito tradicional se tratara, ya que la vulneración de derechos está presente sin importar la modalidad criminal que se utilice.

De esta manera, en referencia al segundo objetivo específico que corresponde a la necesidad de describir y conocer los mecanismos y dispositivos por medio de los cuales se ejecutan los delitos informáticos. Primeramente, se debe mencionar que la tecnología es una herramienta que ha permitido que actividades que se realizaban cotidianamente sean digitalizadas. Por ejemplo, años atrás al escribir una carta se esperaban días para que esta llegue a su destino y obtener una respuesta, ahora por medio de la tecnología esto se puede hacer en pocos minutos por medio de un correo electrónico. Esta revolución tecnológica ha generado un gran impacto en la sociedad, ya que por este medio se pueden enriquecer una diversidad de conocimientos para beneficio persona y del colectivo social. Pero así mismo representa un instrumento que puede ser utilizado como un arma, esto cuando se usa las herramientas que nos brinda la tecnología para delinquir sin importar a quien se pueda afectar.

Las computadoras se implementan en casi todas partes y las hazañas que se realizan por estos medios con cada vez más constantes, pero a medida que se aumenta el uso de estas herramientas también lo hacen las exigencias de un rendimiento de mayor calidad, por lo que construir computadoras con sistemas más rápidos y más potentes no es algo irregular. Es común que las computadoras actualicen sus sistemas constantemente, permitiendo tener una eficacia mucho mayor y un mejor desarrollo en sus funciones. De esta manera se busca mejorar continuamente

las utilidades del sistema operático y corregir cuál falla existente, para evitar vulneraciones de seguridad o de funcionalidad.

Por lo tanto, las computadoras, al ser herramientas sumamente eficaces y de un alto nivel tecnológico, son el medio ideal para cometer delitos informáticos. Las conductas criminales conocidas tradicionalmente dentro de la sociedad se desplazan y usan estas herramientas para tener una mayor beneficio y alcance. Debido al alto uso de sistemas informáticos en la actualidad, la cantidad de datos y de información que se almacena es un atractivo para los delincuentes. Quienes actúan por medio de una computadora y en complemento a un amplio conocimiento del estas herramientas, logran realizar sus cometidos utilizando esta herramienta tan moderna y eficiente.

Referente a esto, Téllez (2009) expone que los delincuentes que utilizan estos medios, es decir, los cibercriminales, presentan una particularidad que los destaca sobre los demás criminales, que es el conocimiento de la informática y la habilidad de utilizar ampliamente estos sistemas. Algo que es totalmente verídico, ya que al hablar de delitos informáticos se entiende que la particularidad que estos presentan es la modalidad por la cual se comete el ilícito, es decir, que se desarrollan por medio de un ordenador, lo cual al complementar con amplios conocimientos en el tema de la informática, podrá dar como resultado un ataque de manera eficaz a quien sea víctima de estos delitos, y que muchas veces es imposible de rastrear debido a que se puede eliminar la huella y los rastros de las actividades realizadas.

Por lo tanto, es evidente que el mecanismo por medio del cual se llevan a cabo los cibercrímenes son los sistemas informáticos, que son el hardware, el software y se complementan con el elemento humano. Está sumado al uso de herramientas como el internet, dan como resultado una amplia cantidad de actividades que pueden ser llevadas a cabo, ya sea para realizar actividades cotidianas o cometer todo tipo de ilícitos, buscando el beneficio, personas que es el fin por el cual los cibercriminales actúan sin importar las repercusiones que puedan causar en sus víctimas. Por lo tanto, comprender la importancia de estas herramientas y sus complementos es importante para conocer la eficacia que tienen.

Algo que Castro (2019) menciona, cuando manifiesta que la cantidad de actividades diarias que deben desarrollarse digitalmente se acrecientan conforme transcurre el tiempo y la sociedad avanza. Dado la constante incorporación de nuevas tecnologías y diferentes plataformas y medios digitales que se involucran en distintos aspectos de las actividades humanas, sumado a la consecutiva recolección de datos e información personal, nos demuestra la eficacia de los

sistemas informáticos independiente del uso que se les esté dando, además del alcance que estos están teniendo actualmente.

De esta manera, y respecto al resultado del tercer objetivo específico que corresponde a analizar el alcance que pueden tener estas herramientas, Alcívar 2015 dice que la criminalidad que se comete informáticamente tiene un alcance mucho más amplio que los delitos tradicionales, idea que comparto con el autor, puesto que al desarrollarse en un ambiente electrónico y no físico, el alcance que se tiene es mucho mayor y el único medio necesario es una computadora, la cual es una herramienta que se encuentra en constante actualización y perfeccionamiento de sus funciones, además de esto se puede complementar con un amplio conocimiento en el área de la informática, la cual es una característica de los ciberdelincuentes que aprovechan todos estos beneficios para cometer delitos informáticos cada vez ms sofisticados. Adicionalmente, se puede cometer actos ilícitos tradicionales como el robo, chantaje, acoso, sin que el delincuente se exponga a ser descubierto y detenido y pueda borrar toda huella e historial de sus actividades.

Por esta razón se puede deducir naturalmente que el alcance que los delitos informáticos tiene en la sociedad moderna es muy alto, debido a factores como la constante actualización de los sistemas informáticos, y como los criminales aprovechan esto su favor. Además del conocimiento en el área de la informática de quienes cometen estos delitos, ya que para poder realizar estas actividades se necesita un conocimiento previo aceptable de como utilizar una computadora y sus funciones. Esto, sumando a la amplia cantidad de actividades que se pueden realizar por un espacio virtual sin exponer directamente la identidad de una persona, es un atractivo para los delincuentes informáticos.

Por otro lado, Rodríguez & Magdalena (2015) enuncian la importancia de conocer las consecuencias que pueden desencadenar el uso incorrecto de las herramientas informáticas modernas. Algo de total importancia, puesto que usar medios informáticos sin las debidas precauciones pueden generar repercusiones en la intimidad personal de los individuos y dependiendo del grado de información que haya sido comprimida, puede desestabilizar incluso la propia imagen de la persona, puesto que la información robada puede ser utilizada de manera poco ética en un espacio digital que es muy difícil de controlar.

Por lo tanto, es de suma importancia que las personas sean conscientes de la variedad de amenazas informáticas a las que la sociedad está expuesta y las consecuencias que estas pueden generar al ser víctimas de estas modalidades delictivas. Basta con navegar en una página de internet para poder encontrarse publicidad engañosa, la que por medio de links redirigen a la

persona a páginas en blanco que pueden tener malware, el cual es un software malicioso que se instala en el ordenador y por medio de este los criminales pueden acceder a información personal y datos personales de aquella persona. Es necesario concientizar a los miembros de nuestra sociedad en cuanto al peligro de estos delitos y como pueden violentar el derecho constitucional a la intimidad personal. Se debe tomar las precauciones necesarias al momento de ejecutar actividades informáticas, contar con la protección del sistema operativo es fundamental, permitiendo un blindaje informático del ordenador y la información que se encuentra almacenada. Por lo tanto, es importante saber que al momento que se violenta el derecho a la intimidad, no solamente se está limitando a la víctima al ejercicio de sus derechos y acciones, sino que está quebrantando y debilitando la tranquilidad social.

6.1.2 Resultados y análisis general de la técnica de entrevistas

Pregunta 1. ¿El ordenamiento jurídico actual tutela de manera apropiada la protección del derecho constitucional a la intimidad frente a los delitos informáticos?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Tenemos nosotros dentro del Código Orgánico Integral Penal el artículo 178 que nos habla de la violación a la intimidad, que nos indica que la persona que sin contar con el consentimiento o autorización legal acceda, intercepte, examine, retenga, grave, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información obtenida en soporte informático, comunicaciones personales o reservadas de otra persona por cualquier medio. Será sancionado con una pena privativa de libertad de 1 a 3 años. Así mismo se puede hablar con respecto a lo que dice el artículo 179, el 180, que hacen referencias a revelación de secreto y circulación de difusión de información restringida.	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno, primeramente, el ordenamiento jurídico como usted lo menciona partiendo de la Constitución de la República, en su artículo 66, específicamente en el numeral 20, garantiza el derecho a la intimidad personal y familiar concomitante con el numeral 19 que habla de la protección de datos de carácter personal que incluyen el acceso a la decisión sobre información y datos de carácter netamente personal o la difusión de los mismos. Considero que al existir como garantía o como derecho se estaría tutelando ya	

de una manera enmarcada dentro de la Constitución este derecho constitucional. Yéndonos a la práctica, pues realmente con el avance que existe actualmente y el acceso en todo caso, pues podríamos decir a redes sociales, a datos que las mismas personas, pues promueven a través de estas redes considero que muchas de las veces se escapa ya de la protección estatal porque realmente, pues como ciudadanos que tenemos también derechos de autodeterminación, es decir yo elijo que hacer sin afectar sin el derecho del otro, pues si es mi decisión subir datos, fotografías, exponer en todo caso mi intimidad, pues realmente el estado se vería limitado al poder evitar que esto se haga público cuando soy yo la persona que me expongo, en ese sentido considero yo de esta primera pregunta.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno, yo creo que se protege, existe la normativa nacional para proteger el derecho a la intimidad y dentro de eso también obviamente la intimidad abarca todo, no obviamente los delitos informáticos también. Entonces yo creo si hay la normativa legal y constitucional que protege el derecho a la intimidad y dentro de eso también a los delitos informáticos. En la práctica yo creería que sí, ósea que las personas, los delincuentes cometen delitos y atentan contra nuestra intimidad, en este caso ya se escapa de la normativa, es como decir el derecho a la propiedad, el derecho a la vida se encuentra garantizados en la Constitución, pero a diario roban, a diario matan, no solamente aquí sino en todo el país. Entonces la normativa existe, que se cumpla, no, no se cumple.	

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Pregunta 2. ¿Es necesario reformar la normativa nacional en cuanto a los delitos informáticos en el Ecuador?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Nosotros dentro de delitos informáticos tenemos varios articulados que hacen referencia a estos, cómo por ejemplo tenemos el artículo 191 de reprogramación, modificación de información de equipos terminales, tenemos así también el artículo 211, que hace referencia a delitos contra el derecho a la intimidad que también habla a	

personas que dañen, impidan, supriman, inscripciones. Tenemos otros cómo son interceptación ilegal de datos, tenemos como el 299 de la revelación ilegal de datos o base de datos, el 230 interceptación ilegal de datos. El 232 que hace referencia a sistemas informáticos, ataques a sistemas informáticos, tenemos por ejemplo el artículo 234 acceso no consentido a sistemas informáticos, entonces tenemos una amplia normatividad al respecto, pero como cada día se está utilizando más los sistemas, las apps, las redes sociales si se debería ampliar más, rápido basándonos en el buen nombre por ejemplo una foto que usted no quiera que se publique y tenía en redes sociales, se está yendo contra el derecho a la propiedad intelectual de esa foto y por el avance de los sistemas electrónicos si se debería aumentar cierto tipo de delitos.	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Partiendo de que los delitos o el catálogo de delitos que contiene en este caso, pues el COIP son el resultado de una política criminal, no necesariamente o no únicamente obedecen a copiar conductas de otros países, sino que obviamente se ha hecho, pues, un análisis o un estudio en cuanto a la política criminal, es decir el índice de tipos penal o de conductas que requieren ser tipificadas, más aún con el avance de la tecnología. Dentro del Ecuador, en este marco jurídico que es el COIP considero que se han abarcado ciertos tipos penales que son los más comunes, que, si bien es cierto, la protección estatal no puede extenderse a todas las conductas humanas, porque en sí la conducta humana o la vida social es un riesgo, toda la conducta o todo el ámbito de desarrollo humano es un riesgo, pero considero que el COIP ha procurado abarcar conductas que son parte de nuestra realidad social como Ecuador. Considero que no serían necesario en todo caso al momento alguna reforma dentro de la normativa del COIP.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Yo creería que la normativa, los delitos informáticos, se encuentran ahorita tipificados en el Código Orgánico Integral penal, más bien lo que se debería es dotar de los medios necesarios, dotar a la policía judicial, a la Fiscalía, en este caso, a los entes encargados de investigar este tipo de delitos para que se haga una investigación prolija y exhaustiva de estos delitos, ya que no existe personal capacitado y especializado en investigar estos delitos. Tenemos agentes investigadores que están en la ciudad de Quito y ellos nos	

colaboran desde allá investigando ese tipo de delitos, aquí en Ibarra por ejemplo no tenemos, entonces sería dotar de esos agentes investigadores de la policía judicial aquí y en cada ciudad para que podamos hacer una investigación más rápida, más exhaustiva y más prolija.

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Pregunta 3. ¿La Fiscalía cuenta con los elementos necesarios para investigar los delitos informáticos?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Cómo todas las fiscalías en el mundo no contamos con los suficientes equipos necesarios, peritos, instalaciones cómo para hacer una buena investigación. Por ejemplo, en nuestro caso todo lo que se investigue a nivel de delitos informáticos tiene que remitirse a la ciudad de Quito, entonces no contamos con los suficientes elementos necesarios para este tipo de investigaciones. Claro específicamente personas preparadas, acuérdese que tenemos hackers, tenemos un sinnúmero de personas que en otros países, los que hackeaban cuentas ahora están trabajando para el servicio secreto e inclusive presidencia de los Estados Unidos, entonces nosotros deberíamos tener ese mismo tipo de personal que nos pueda ayudar, aparte de equipos de última generación, en el aspecto informático todos los días aparecen equipos nuevos por ejemplo gama de celulares cada día aparece un nuevo equipo, entonces hay que estar a la par con la tecnología avanzando todos los días entonces si se debe realizar eso.	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno, en este punto, si ya hablamos lo que es la práctica, aquí la fiscalía amparada bajo el artículo 195 que es nuestra directriz de actuación, la Constitución nos dice a nosotros que actuemos impulsando la investigación pre procesal y procesal penal hasta llevar a una instancia de juicio a las personas responsables determinando la existencia de la información y responsabilidades. Esto es lo que nos dice en su inciso primero el artículo 195, también la misma fiscalía a través de este ordenamiento jurídico como es la Constitución en su segundo inciso dice que se contara con personal de investigación, organizado al mando de la fiscalía, pero realmente de la práctica que se puede observar	

que primeramente no contamos con una policía especializada que conozca los delitos informáticos porque más allá de conocer cosas básicas como manejo de Facebook, un correo si se requiere de conocimiento más profundo en torno a de donde viene cierta información. Nosotros aquí tenemos en la práctica el tema de dirección IP, de donde se produce la información, qué servidor la otorga, incluso al tener proveedores extranjeros, por ejemplo, de Facebook, de la mayoría, de WhatsApp, que realmente, pues sus bases o sus matrices están en otro país, para nosotros acceder a una información fidedigna y rápida sobre todo es imposible porque a nosotros nos toca aplicar lo que corresponde a la asistencia penal internacional, figura jurídica que si bien está en el COIP, pero la aplicación diaria es bastante complicada. Entonces considero que primero no se cuenta con las herramientas tecnológicas necesarias, personal o talento humano, en la investigación no existe tampoco y obviamente, pues el acceso directo a esa información a través de sus proveedores tampoco existe.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
En cuanto a los elementos se refiere al personal humano, los fiscales estamos asignados de FEDOTI ahora para investigar los delitos informáticos, tenemos en suficiente personal humano, no, no lo tenemos, tenemos una sobrecarga de delitos por investigar. Ahora la policía judicial que es nuestro brazo derecho que investiga los delitos, también tiene sobrecarga laboral y no abastecen a investigar ese tipo de delitos, más cuando aquí en Ibarra no tenemos agentes investigadores especializados en delitos informáticos, tenemos que remitir nuestras delegaciones a Pichincha, a Quito para que allá nos deleguen un agente y coordinarlo mediante vía telefónica, así estamos trabajando actualmente acá en Ibarra y entiendo que en el resto de ciudades del país debe ser igual, a excepción de ciudades grandes Quito, Guayaquil, Cuenca. Entonces, si Fiscalía cuanta con elementos necesarios no, yo podría concluir que primero porque el personal, número de fiscales que investiga este tipo de delitos es muy reducido, y más ahora que teníamos 5 fiscales y nos están rediciendo a 2 que van a investigar este tipo de delitos, entonces yo concluiría que no. Y respecto al tema que la tecnología se actualiza y se desarrolla constantemente, ¿la Fiscalía tiene los implementos, por ejemplo, tecnológicos, para poder investigar estos delitos? No, con mucho dolor tengo que decir que no, no tenemos a veces ni los insumos tan básicos como a veces un tóner para imprimir o una impresora, a veces tenemos que pasar días sin poder imprimir,	

entonces si no podemos ni siquiera imprimir unos documentos, no podemos sacar copias, hoy quise sacar copias de un expediente y no pudieron sacar copias porque no hay dinero para sacar copias, entonces el funcionario tiene que de su bolsillo tiene que sacar copias. Si no tenemos para un tóner, si no tenemos para unas copias, imagínese si tendremos medios tecnológicos para investigar. Con todo dolor y preocupación tengo que reconocer que no.

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Pregunta 4. ¿Existen conductas que deberían ser consideradas como delitos informáticos, pero no se encuentran tipificadas en el Código Orgánico Integral Penal?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Sí, existen varias, pero me voy a ir a una práctica, usted en el Facebook puede crearse un perfil verdadero, pero también puede crearse otro perfil para ingresar a buscar en las redes sociales de otra persona y no va a aparecer como usted sino como otra persona. Aquello no es sancionado, salvó que usted cometa algún tipo de infracción que se pueda sancionar, por ejemplo, hay el ciberacoso que se lo hace a través de aquello utilizando programas como el Tor que le aparece que usted está en otro país	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno para ser coherente con lo que manifesté que no se necesitaría ninguna reforma al momento normativa, considero de que el avance de la sociedad nos irá dando luces de que si existe la necesidad de positivar ciertas conductas más peligrosas o riesgosas, al momento considero de que se ha cubierto más aún cuando este Código Integral penal es prácticamente nuevo, a partir del 2014 es que estamos en uso y a partir de él se han hecho, también ya de esa fecha se han hecho reformas en el 2019, en el 2021 es decir se está al avance de la tecnología, al avance de la sociedad, considero pues de que otras conductas no se me viene a la mente para decir se debería en ese momento tipificar, pero considero pues de que con el avance de la sociedad podrían incluirse.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**

Yo creo que están tipificadas las conductas, yo creo que si se encuentran, el gran inconveniente va más allá de una tipificación, va del personal encargado de investigar las falencias, como le digo, desde el número de fiscales que investigan esto, personal de PJ que no tiene y no tenemos para investigar aquí, y el escaso número de agentes que están en Quito tienen que abastecerse a todas las ciudades del país, entonces no creería que es un problema de normativa, sino un problema personal humano especializado en investigar este tipo de delitos.

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Pregunta 5. ¿Qué medidas se pueden adoptar para garantizar la protección del derecho a la intimidad personal frente a un delito de carácter informático?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Bueno como por ejemplo a una analogía cómo en el caso de la violencia a la mujer se dan medidas de protección, como por ejemplo la de prohibir que el agresor se acerque, boletas de auxilio, restricciones, debería ser lo mismo aquí, que por ejemplo el juez pueda dar a una unidad especializada la potestad para que la información que conste en redes sociales o en algún archivo sea bloqueada y sea directamente reportada a los propietarios de esas páginas web, porque por ejemplo tenemos Facebook que no nos pertenece que no la tenemos aquí en el Ecuador, tenemos otras en la que se hacen citas y muchas veces se hacen citas fantasmas como en Tinder que sacan dinero, tenemos a través de redes informáticas mensajes de WhatsApp que extorsionan, entonces si se debería dar ese tipo de medidas cautelares cómo para bloquear números telefónicos o páginas web.	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno, existen en nuestro mismo Código Orgánico Integral Penal, medidas de protección que se hallan en el artículo 558, en este sentido, si veo ahí una falencia que de pronto no existen, podríamos decir medidas directas a las empresas que prestan estos servicios que sé yo, de Facebook, de Instagram, de varias redes, que por lo general son las que se utilizan pues para atentar contra la intimidad de las personas como se dice,	

pero considero de que a las personas jurídicas que se debería aplicar estas medidas de protección.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Bueno en algún delito de carácter informático, remitiéndose solamente a la cuestión de esto, de los delitos informáticos, bueno actualmente se puede contratar programas, puertos, servidores que bloquen este tipo de delitos informáticos, pero eso ya se encargan las instituciones, las empresas de contratar estos servicios. Yo creo que, si existe, pero, sin embargo, usted sabe que los hackers están más adelante, estos programadores de alguna manera, una forma como parar este número de delitos sería de esta manera, contratando estos programas, estos expertos en cuestión de sistemas que puedan evitar que las personas seamos víctimas de estos delitos informáticos. Pero yo también creo que una forma de evitar aquello es la educación a las personas, porque una persona educada, una persona con valores no cometería este tipo de delitos, entonces yo creo que a veces nos preocupamos solamente del tema de contratar programas, puertos para que nuestros trabajadores no sean víctimas de este delito que está muy bien. Pero también yo creo que el Estado en este caso debe preocuparse de la formación en valores a las personas, porque una persona con valores, educada, no va a cometer estos delitos. Entonces yo creo que iría a la par, esa sería la resolución.	

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Pregunta 6. ¿Es posible identificar al sujeto activo de un ciberdelito para procesarlo debido a que actua por medio de un ordenador en un espacio virtual?	
Entrevistado 1.	**Dr. Julio Ponce Lozada (Fiscal provincial de Imbabura)**
Puede ser posible, pero como explicaba hace un rato, existen programas como Tor por ejemplo de que usted aparece como que estuviera en otro país. Existen programas, apps por el cual usted puede robar internet mediante wifi, tenemos wifi gratuito, por ejemplo, aquí en esta ciudad de Ibarra, en los parques, usted se puede conectar a través de un teléfono celular, realizar un ciberacoso y sería difícil encontrarlo a usted porque si usted no tiene registrado el equipo a su nombre va a ser muy difícil ubicar el punto de dónde se está realizando dicho acoso. Tenemos por ejemplo para las terminales móviles, para	

cuando se los roban, uno trata de buscar el teléfono, pero nos da más o menos una cuadra de referencia, entonces si lo hacen zonas despobladas será la única casa que se encuentren el lugar. Pero si hablamos aquí en el centro más o menos es una cuadra, usted puede meterse al municipio, hacer ciberacoso y si la policía llega, a qué departamento iría, no podría encontrarlo, entonces todavía hay maneras de evitar, se descubra a los autores de estos delitos. Entonces, en algunos casos, podrá ser, cuando la gente es inexperta, que lo va a hacer desde si computadora personal, desde el internet de su domicilio, desde su casa. Pero va a haber personas que conozcan sobre el tema, que van a tener conocimientos más sofisticados, hablemos de ingenieros en sistemas, programadores, que van a saber este tipo de delitos y como tenemos por ejemplo los hackers que se encargan, pues justamente de vulnerar las seguridades que tienen los programas tanto de empresas privadas cuánto públicas.	
Entrevistado 2.	**Mgs. Lizandra Bastidas Ibujes (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Como manifestaba, pues el hecho de no contar con el personal especializado, de no contar con herramientas tecnológicas que nos ayuden a determinar en forma clara, precisa, contundente de qué persona en forma física, singularizando a quien realiza este acto pues si es, se vuelve imposible en algunos casos. En el caso de mi unidad, yo conozco delitos informáticos en torno a la afectación del patrimonio, no conozco en torno a la afectación de la intimidad personal, pero si del patrimonio y muchas de las veces se vuelve complicado, por no decirlo imposible el establecer que persona singularizada ha cometido esta infracción.	
Entrevistado 3.	**Mgs. Jhonny Hurtado Moreno (Fiscal de la unidad FEDOTI de la ciudad de Ibarra)**
Ese es el grave problema que tenemos en los delitos informáticos, a ver como usted ha hecho su trabajo, su investigación ya puedo hablar de aquello no cierto. Digamos que se detecta que, del servidor de aquí de la fiscalía, desde el computador del tercer piso se violentó la intimidad de una persona que vive en la ciudad de Quito, nosotros podemos lograr con la dirección IP llegar a la dirección IP de donde se produjo ese delito, podríamos llegar inclusos al computador que este asignado a ese servidor. Pero ahora como poder determinar que fue esa persona, si ese computador lo utilizan digamos 3, 4 o 5 personas, entonces lo que podríamos llegar es a la dirección IP, podríamos llegar al computador, podríamos pedir también quien está asignado a ese	

computador, pero no podríamos tener, lo ideal sería tener una cámara que esté grabando para saber el día y la hora que se produjo el delito, quien uso ese computador, al no tener aquello y muchas veces los señores jueces terminan resolviendo la duda a favor del reo porque las versiones, los testimonios dicen que ese computador utilizaban 10 personas por ejemplo, entonces yo como acusar a las 10 personas que cometieron ese delito. Determinamos el lugar, la dirección IP, el computador, de donde se cometió el delito, pero quien lo está utilizando ahí es donde se nos complica siempre. Entonces no tampoco es imposible, digo que se implica, pero por ejemplo si ese computador lo utilizan 10 personas, por ejemplo si ese día estuvieron enfermas 2 quedan 8, ese día 4 se fueron a un curso quedan 4, de los 4 si rinden las versiones yo estaba en tal cosa, yo estaba en tal cosa y el que utilizo el computador es Juan por ejemplo, entonces ahí podríamos llegar a determinar la persona que realmente, pero muchas veces se complica porque no saben quién fue, pero si podríamos llegar de esa manera a determinar quién fue la persona que cometió el delito, el sujeto activo.

Elaborado por: Juan Leandro Lucero Burbano

Fuente: Entrevistados

Conforme a lo que establece el cuestionario de la entrevista, los entrevistados manifiestan que al existir un ordenamiento jurídico nacional ya se está protegiendo el derecho a la intimidad. La normativa es un recurso que tiene el Estado ecuatoriano para garantizar los derechos de todos los ciudadanos, además, también se cuenta con las garantías necesarias para que en caso de que alguno de los derechos llegue a ser violentado se puedan interponer acciones y reclamar el cumplimiento de los diferentes derechos por medio de alguna reparación y que el responsable sea sancionado conforme a la ley. Al existir y habitar en una sociedad altamente desarrollada nos relacionamos socialmente con otros individuos, por lo que estamos expuestos a ser atacados en cualquier momento, ya que la normativa puede garantizar el cumplimiento y protección de derechos, pero son las personas quienes eligen que acciones realizar, y muchas veces lo hacen sin importar el perjuicio que puedan generar en los demás con acciones típicas, antijurídicas y culpables. Por lo que la normativa nacional si tutela de manera apropiada el derecho constitucional a la intimidad, pero al coexistir en una sociedad donde siempre existan delitos y conductas inapropiadas, ya es algo que se escapa de la protección estatal y de la normativa, porque así como existen derechos para proteger al individuo también existen obligaciones que las personas muchas veces no las cumplen y violentan el derecho de alguien más.

Al tener una normativa nacional compuesta basándonos en el desarrollo social que se ha producido por el transcurso del tiempo, existen un sin número de articulados que abarcan diversos temas y captan un amplio campo de aplicación, incluyendo temas como los delitos informáticos y el derecho a la intimidad. Pero así mismo las conductas humanas cambian, surgen y evolucionan, por lo que es algo muy complejo abarcar todas esas conductas humanas para poder sancionar todos cuando se cometen los actos ilícitos. En el área de la informática el desarrollo de conductas criminales puede ser más intenso y más rápido, esto debido a la constante actualización que tienen las tecnologías, entonces estas condutas se desarrollan a la par que el instrumento por el cual se cometen, por lo que identificar conductas irregulares que surgen como delitos que se cometen por estos medios y poder sancionarlas sería es necesario pero complejo. A pesar de que la normativa vigente es eficaz y resulta competente, también debe estar ligada a los medios que son necesarios para complementar un buen trabajo, por ejemplo se debe tener más herramientas para poder investigar de manera correcta y con más profundidad esta clase de delitos, así se obtendría resultados más positivos. La normativa nacional actual, en su rama penal, abarca las conductas informáticas que son dañinas para la sociedad, y las nuevas conductas que se han derivado son con base a las ya tipificadas, por lo que por ahora no es considerable una reforma de la normativa en lo que respecta a este tema.

La Fiscalía se encarga de investigar cuándo se da la vulneración de derechos por medio de algún delito, se aplican los respectivos procedimientos y formalidades que están sustentados conforme a la ley. Cuándo se trata de un delito informático, al ser un delito tipificado, el procedimiento es el mismo, ya que también estamos hablando de una conducta típica, antijurídica y culpable, solo que la modalidad por la que se comete es diferente. Hacer referencia a esto se debe tener en cuenta que se halla también de la práctica, y aunque la Fiscalía pueda llevar a cabo los procesos necesarios para cumplir con su labor no cuenta con las herramientas necesarias para poder cumplir totalmente con este trabajo, porque existe una sobrecarga considerable de casos y los recursos tanto humanos como tecnológicos son necesarios para poder llevar a cabo una investigación de manera correcta y así obtener resultados que garanticen el correcto cumplimiento de las funciones establecidas, algo que limita el obtener los resultados esperados, ya que desafortunadamente la Fiscalía no cuenta con los implementos necesarios para desarrollar su trabajo de manera completamente eficiente por lo que el procedimiento también se puede ver afectado y esto en comparación a las modalidades de delitos que surgen y qué son más eficientes puede ser contraproducente.

Al existir nuevas herramientas modernas e innovadoras, las actividades que se van a realizar por medio de estas también van a ser progresivas, por lo que las actividades criminales también se actualizarán. Pero al contar con una normativa eficiente se podrá captar y regular cualquier actividad que se encuentre fuera del marco de la ley y aunque estás conductas sean más peligrosas y se desarrollen, la sociedad también lo hará y de esta manera se pueden positivar las conductas que se consideren necesarias para salvaguardar los derechos de manera correcta. Las acciones que se encuentran tipificadas actualmente abarcan a la gran cantidad de delitos informáticos que surgen día a día, y los elementos normativos para investigar son eficientes, esto sumado a que el Código Orgánico Integral Penal ha pasado por algunas reformas, demuestra el avance que tiene esta normativa frente a las nuevas conductas cibercriminales que se puedan presentar y conforme avance de la sociedad también se podrán incluir y tipificar nuevas conductas negativas. Lo que realmente es una falencia es el limitado número de personal y de recursos que se tiene para poder investigar y dar solución a las problemáticas que surgen de los delitos informáticos, por lo tanto, esta sería una falencia que muchas veces puede ser aprovechada por los criminales.

El Código Orgánico Integral Penal brinda medidas de protección, pero de cierta manera existe una falencia, ya que no se puede contactar directamente con las empresas como Facebook o Instagram que prestan los servicios de redes sociales y por lo general cuándo se da la vulneración a la intimidad no se puede contactar directamente a estas entidades para que se puedan aplicar las respectivas medidas de protección. Las medidas que se pueden tomar son aquellas que brinda la propia aplicación o página, como por ejemplo bloquear o reportar ciertas actividades. Pero difícilmente se pueden dar medidas dictadas por un juez, por lo tanto, lo que se podría hacer es mejorar ciertos servicios y contar con programas especiales y personal capacitado y especialista capaz de hacer frente a quienes realizan estos delitos y qué es muchas veces se encuentran un paso más adelante. Esto en relación con la educación de las personas podría brindar una protección contra los delitos informáticos por qué una persona con valores y principios no cometerá actos ilícitos, por lo que también se le debe prestar atención a la sociedad de manera general. Es necesario considerar que los delitos informáticos se desarrollan por medio de herramientas, las cuales también brindan protección para ciertos ataques, por lo que contar con las repercusiones necesarias en un ordenador personal sería fundamental, de esta manera se mantiene alerta un sistema que modera las amenazas en las que estamos inmersos.

La característica principal de los ciberdelitos es la dificultad de encontrar a quien los cometen, ya que estos al realizarse por un espacio virtual son difíciles de rastrear, considerando que existen expertos en el campo de la informática como lo son los ingenieros en sistemas, programadores que van a tener amplios conocimientos en este tema y las actividades que realicen a tener un mayor alcance por lo que el personal que vaya a investigar esto también debe estar capacitado y preparado además de conocer ampliamente la informática. A pesar de esto, no es imposible rastrear a quién cometa estos delitos informáticos con la debida investigación se puede dar con el implicado, porque el Código Orgánico Integral Penal brinda las herramientas necesarias y los procedimientos correctos para actuar frente a estas situaciones por lo que a pesar de que sea difícil encontrar a un ciberdelincuente con la correcta investigación esto se podrá efectuar. Lo ideal para contrarrestar a estos delincuentes informáticos y las acciones criminales que realizan es contar con los recursos tanto tecnológicos como personal capacitado, los cuales puedan confrontar profesionalmente las diversas situaciones que puedan surgir con base a los ciberdelitos.

6.2 Discusión

En este apartado se manifiestan los resultados de la información obtenida de la opinión de los entrevistados, conjuntamente con la opinión propia y la de diferentes de estudios de delitos informáticos y el funcionamiento de los sistemas informáticos, en concordancia con los autores que realizan estudios sobre los derechos constitucionales y por consecuente el derecho a la intimidad. Una vez que se han organizado y analizado correctamente los datos obtenidos, con las técnicas de revisión y análisis documental, en complemento con la técnica de la entrevista se puede dar en manifiesto los aspectos más relevantes en cuanto a la investigación.

El tema de los delitos informáticos no es tan remoto, puesto que la tecnología informática que hoy tenemos es resultado del constante desarrollo que han tenido estos sistemas, los cuales tienen su origen de hace algunos años. Pero en poco tiempo se ha consolidado y actualmente es parte fundamental de nuestra sociedad, basta con observar a nuestro alrededor detenidamente para comprobar esta realidad, la cual se debe a que la sociedad en general, conjuntamente con las industrias, tienen un impacto profundo en la producción digital. Permitiendo que los procedimientos de desarrollo se multipliquen y mejoren, de manera que sus resultados estén al alcance de todos. Los sistemas informáticos han venido actualizándose constantemente hasta dar los resultados que conocemos hoy en día, por lo que los ciberdelincuentes aprovechan estás herramientas para cometer los diferentes ilícitos. Al ser algo innovador y de gran alcance, capta

la atención de las mentes criminales que buscan lucrarse mediantes el uso de estas herramientas, dando paso a la delincuencia informática, fenómeno al cual Acurio (2015) define como:

> (…) todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera. (p. 48).

De esta manera se entiende que los delitos informáticos surgen de una conducta ilícita, la cual ya está tipificada anteriormente en el ordenamiento jurídico. Pero al contar con las herramientas informáticas modernas, estas conductas se redirigen y se enfocan en el uso que les pueden dar a estos sistemas informáticos. Por lo tanto, al unificar una conducta criminal que utiliza estos medios, surgen los delitos informáticos, y debido a la variedad de acciones que se pueden realizar, es necesario tipificar las nuevas conductas resultado de estas operaciones delictivas. Y así mismo optimizar las normas establecidas para afrontar estas actividades ilícitas que al ser delitos naturalmente tiene un impacto negativo en la víctima, siendo esta la principal singularidad que presentan los delitos informáticos. Noción que se complementa con lo que autores como Fernández y Martínez (2020) exponen a continuación:

> Los delitos informaticos son delitos convencionales que toman nueva vida con el uso de las Tecnologías de la Información y la Comunicación (no representan un tipo de criminalidad específica y tienen lugar en el ciberespacio), que se caracterizan por el uso de redes de transmisión de datos y por su relación con los sistemas informáticos, y, que pueden afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (p. 28)

Teniendo en cuenta estos delitos al ser de carácter informático, se necesita de estos medios para que puedan ser catalogados de esta manera, por lo cual si falta esta particularidad serían delitos tradicionales. Por lo tanto, el mecanismo, el cual se desarrollan estas actividades es un ordenador, el cual al contar con implementos como diferentes programas y acceso a internet, lo convierten en la herramienta ideal para delinquir virtualmente. Pero causando los mismos efectos en la víctima como si de un delito tradicional se tratara, por lo que la lesión del derecho a la intimidad sigue estando presente. La eficacia de estos sistemas es alta, debido al desarrollo tecnológico con el que se cuenta en la actualidad. Esto, sumado a la habilidad que tiene los

ciberdelincuentes y lo difícil que puede ser rastrearlos, convierten a una computadora en una herramienta altamente eficaz para cometer ilícitos.

Haciendo énfasis en que la principal causa de los delitos informáticos es la conducta criminal de las personas llevada a cabo por medio de la tecnología, se puede inmiscuir que la influencia social es sumamente importante en este punto. Cuando un individuo demuestra su comportamiento, lo está haciendo conforme a lo aprendido en el entorno en el cual se desarrolló. Esto produce como resultado un determinado comportamiento que lo caracterizará dentro del colectivo social, y es aquí donde aquellos individuos que han sido influenciados por un entorno hostil desarrollan un comportamiento indebido y asocial dentro de nuestra comunidad y al buscar satisfacer sus necesidades optan por delinquir.

7. Conclusiones

- El Ecuador es un Estado de derechos, por lo que tutelar las garantías y derechos consagrados en la Constitución de la República del Ecuador es la principal obligación del Estado ecuatoriano. A pesar de esto, existen medidas en favor de la víctima, en caso de que se lleguen a violentar los derechos constitucionales. Estas medidas permiten hacer el reclamo respectivo para aplicar la correspondiente reparación del daño que se ha hecho. De esta manera se puede deducir que el ordenamiento jurídico nacional tutela de manera efectiva el derecho a la intimidad frente a los delitos informáticos, ya que el Estado ecuatoriano cuenta con los instrumentos necesarios como la Constitución de la República para garantizar el cumplimiento de los derechos de los ciudadanos que han sido establecidos.
- La Constitucion de la Republica del Ecuador garantiza la proteccion de los derechos de los ciudadanos, el Codigo Organico Integral Penal tipifica las conductas inapropiadas que deben ser sancionadas. Por lo tanto la normativa existe, el Estado Ecuatoriano garantiza la proteccion de derechos y sanciona a aquellos que incumplan las leyes, pero cuando una persona decide actuar con un comportamiento criminal es algo que se escapa de la proteccion estatal, ya que cada persona es responsable de su comportamiento y de sus acciones, porque la proteccion estatal no puede extenderse a todas las conductas humanas existentes.
- Los ciberdelincuentes han conseguido que delitos tradicionales como el robo y la extorsión puedan ser desplazados a las plataformas digitales y que de esta manera la modalidad de delinquir se desarrolle, no solamente incluyendo delitos que ya son conocidos en nuestro entorno social, sino que originando nuevas conductas delictivas gracias al uso de sistemas informáticos que cada vez más sofisticados y modernos, y por ende son una herramienta adecuada para delinquir y lucrarse.
- La dificultad para poder identificar a los autores de estos delitos es una de las principales características que se deben tener en cuenta. Puesto que, al desarrollarse por medio informático en un espacio digital, los ciberdelincuentes pueden encontrarse en cualquier lugar, y eliminar el resto de sus acciones. Adicionalmente que al ser personas que tienen amplios conocimientos en la informática, hace más difícil su rastreo y ubicación, reflejando el alcanse que se puede tener los delitos informaticos por causa de que la tegnologia se actualiza rapidamente permitiendo un sin numero de acciones.

8. Recomendaciones

- Los procesos de desarrollo a los que está sometida la sociedad hacen que esta progrese y se desarrolle, conjuntamente con esto elementos como los sistemas informáticos se actualizan, por lo que se debe tener en consideración que conforme se avanza pueden surgir nuevas conductas que necesiten ser reguladas, dando resultado nuevos delitos que deberán ser tipificados para seguridad de los ciudadanos.
- Brindar los recursos necesarios a la Fiscalía General del Estado para poder investigar estos delitos, se le debe dar a esta institución herramientas tecnológicas avanzadas que permitan reprimir el impacto de estos delitos en conjunto con personal capacitado se mejoraría notablemente al momento de investigar los delitos informáticos.
- Concientizar al colectivo social sobre del alcance y repercusiones que pueden tener los delitos informáticos en la información personal, además de la importancia de la seguridad digital. Estas medidas permiten tener las herramientas básicas de seguridad ante un posible delito informático.

9. Referencias bibliográficas

Acurio Del Pino, S. (2015). *Derecho Penal Informatico.* Quito, Ecuador: Corporación de Estudios y Publicaciones. Obtenido de http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Alcívar Trejo, C. (2015). La seguridad jurídica frente a los delitos informáticos. *Revista de Investigación Jurídica*, 63-79. Cajamarca, Perú. Obtenido de https://www.pensamientopenal.com.ar/doctrina/44051-seguridad-juridica-frente-delitos-informaticos

Asamblea Nacional Constituyente del Ecuador. (20 de Octubre de 2008). Constitución de la República del Ecuador. Registro Oficial 449. Montecristi. Obtenido de https://www.ambiente.gob.ec/wp-content/uploads/downloads/2018/09/Constitucion-de-la-Republica-del-Ecuador.pdf

Asamblea Nacional del Ecuador. (10 de Febrero de 2014). Código Orgánico Integral Penal (COIP). Quito, Pichincha, Ecuador. Obtenido de http://biblioteca.defensoria.gob.ec/handle/37000/3427

Ávila Santamaría, R. (2008). *La Constitución del 2008 en el contexto andino.* Quito: V&M Gráficas. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://biblioteca.cejamericas.org/bitstream/handle/2015/2358/3C2008CA.pdf?sequence=1&isAllowed=y

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México D.F, México: Grupo Editorial Patria. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/40458?page=15.

Barrio Andrés, M. (2018). *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos.* España: Wolters Kluwer España.

Calvo Andújar , A. (Abril de 2014). Evolución del derecho y cambios sociales en los siglos XIX y XX. *Tesis de Grado.* Universidad Pontificia Comillas, Madrid, España.

Castro Rosas, M. I. (2019). Protección de datos personales a través de herramientas de procesamiento automatizado de datos: desafíos y recomendaciones. *Tesis de Maestría.* INFOTEC, Ciudad de México.

Costas Santos, J. (2015). *Seguridad informática.* Madrid, España: RA-MA Editorial. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/62452?page=29.

Cuadros Añazco, X. (2019). El derecho a la protección de datos personales. *Revista Jurídica(33)*, 70-84. Guayas, Ecuador. Obtenido de https://www.revistajuridicaonline.com/wp-content/uploads/2022/06/EL-DERECHO-A-LA-PROTECCIO%CC%81N-DE-DATOS-PERSONALES.pdf

Encalada Hidalgo, P. (2015). *Teoría Constitucional del Delito.* Quito, Pichincha, Ecuador: Corporación de Estudios y Publicaciones. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/115667

Escrivá Gascó, G. (2013). *Seguridad Informática.* Madrid, España: Macmillan Iberia, S.A. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/43260?page=11

Fernández Bermejo, D., & Martínez Atienza, G. (2020). *Ciberdelitos.* España: Ediciones Experiencia.

Gil González, E. (2022). *El interés legítimo en el tratamiento de datos personales.* España: Wolters Kluwer España. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/218734?page=36.

Gómez Vieites, Á. (2010). *Seguridad Informática Básico.* España: Starbook Editorial.

Grijalva Jiménez, A. (2012). *Constitucionalismo en Ecuador.* Quito: Sector Público Gubernamental. Obtenido de file:///C:/Users/User/Downloads/constitucionalismo_en_ecuador.pdf

Hernández Encinas, L., Arroyo Guardeño, D., & Gayoso Martínez, V. (2020). *Ciberseguridad.* Madrid, España: Editorial CSIC Consejo Superior de Investigaciones Científicas. Obtenido de https://elibro.puce.elogim.com/es/ereader/puce/172

Lorca Ruiz , O. F. (2017). Violación a la intimidad en redes sociales en Ecuador. *Tesis de Grado.* Universidad Católica Santiago de Guayaquil, Guayaquil.

Nogueira Alcalá, H. (1998). El derecho a la privacidad y a la intimidad en el ordenamiento jurídico chileno. *Ius et Praxis, 4(2)*, 65-106. Talca, Chile. Obtenido de https://www.redalyc.org/articulo.oa?id=19740206

Poquet Catalá, R. (2018). La protección del derecho a la intimidad del teletrabajador. *Lex Social Revista jurídica de los derechos sociales, 8(1)*, 113-135. Obtenido de https://www.upo.es/revistas/index.php/lex_social/article/view/2918

Quispe Gomezjurado, H. D. (2019). El delito de la violación a la intimidad de los datos personales en relación a la cláusula de reserva y confidencialidad en redes sociales. *Titulo de Grado.* Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato.

Repetto, A. (Octubre de 2022). *Definición de Conducta*. Obtenido de Definición ABC: https://www.definicionabc.com/social/conducta.php

Rios Maza, B., & Vilela Pincay, E. (2021). Estudio doctrinal del derecho a la intimidad en las redes sociales. *Polo del Conocimiento, 6(8), 61*, 513-526. Machala, El Oro, Ecuador. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8042603

Rodríguez García, L., & Magdalena Benedito, J. R. (2016). Perspectiva de los jóvenes sobre seguridad y privacidad en las redes sociales. *ÍCONO 14, 14(1)*, 24-49. España. doi:ri14.v14i1.885

Téllez Valdés, J. (2009). *Derecho Informático - Cuarta Edición.* Ciudad de Mexico: Mc Graw Hill.

Trujillo Mariel, P. R. (2021). *Cibercriminología: ensayos y reflexiones.* Ciudad de México, México: Editorial Alfil, S. A. de C. V.

10. Anexos

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR “SEDE IBARRA”

ESCUELA DE JURISPRUDENCIA “CARRERA DE DERECHO”

PREGUNTAS DE ENTREVISTA

1. ¿El ordenamiento jurídico actual tutela de manera apropiada la protección del derecho constitucional a la intimidad frente a los delitos informáticos?
2. ¿Es necesario reformar la normativa nacional en cuanto a los delitos informáticos en el Ecuador?
3. ¿La Fiscalía cuenta con los elementos necesarios para investigar los delitos informáticos?
4. ¿Existen conductas que deberían ser consideradas como delitos informáticos pero no se encuentran tipificadas en el Código Orgánico Integral Penal?
5. ¿Qué medidas se pueden adoptar para garantizar la protección del derecho a la intimidad personal frente a un delito de carácter informático?
6. ¿Es posible identificar al sujeto activo de un ciberdelito para procesarlo debido a que actua por medio de un ordenador en un espacio virtual?