UNIVERSIDAD METROPOLITANA DEL ECUADOR

FACULTAD DE CIENCIAS SOCIALES, HUMANIDADES Y EDUCACIÓN

CARRERA DE DERECHO

SEDE QUITO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

TEMA: ABORDAJE DE LA PREVENCIÓN DEL DELITO CIBERNÉTICO Y EL DERECHO A LA INTIMIDAD EN ECUADOR.

AUTOR:

HECTOR GUILLERMO SALTOS PINTO

ASESORA:

DRA. AURA VIOLETA DÍAZ DE PERALES (PHD)

QUITO - 2022

CERTIFICACIÓN DE LA ASESORA

Dra. **AURA VIOLETA DÍAZ DE PERALES** (PhD), en calidad de Asesora del Trabajo de Investigación designado por la Dirección de la carrera de Derecho, sede Quito, certifico que el estudiante: **HECTOR GUILLERMO SALTOS PINTO,** titular de la CC N° **1717822983**, ha culminado el trabajo de investigación, con el Tema: **"ABORDAJE DE LA PREVENCIÓN DEL DELITO CIBERNÉTICO Y EL DERECHO A LA INTIMIDAD EN ECUADOR", quién** ha cumplido con todos los requisitos legales exigidos por lo que se aprueba la misma.

Es todo cuanto puedo decir en honor a la verdad, facultando a la interesada hacer uso de la presente, así como también se autoriza la presentación para la evaluación por parte del jurado respectivo.

Atentamente.

Dra. AURA VIOLETA DÍAZ DE PERALES
C.I: 1757825920

CERTIFICACIÓN DE AUTORÍA DE TRABAJO DE TITULACIÓN

Yo, **HECTOR GUILLERMO SALTOS PINTO,** titular de la CC N°**1717822983,** estudiante de la Universidad Metropolitana "UMET", carrera de Derecho sede Quito, declaro en forma libre y voluntaria que el presente trabajo de investigación que versa sobre: **"ABORDAJE DE LA PREVENCIÓN DEL DELITO CIBERNÉTICO Y EL DERECHO A LA INTIMIDAD EN ECUADOR",** y las expresiones vertidas en el misma, son autoría del compareciente, las cuales se han realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de esta y el cuidado al referirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

Firmado electrónicamente por:
HECTOR GUILLERMO SALTOS PINTO

Héctor Guillermo Saltos Pinto

C.I. 1717822983

AUTOR

CESIÓN DE DERECHOS DE AUTOR

Yo, **HECTOR GUILLERMO SALTOS PINTO**, titular de la **CC N°1717822983**, en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación, "**ABORDAJE DE LA PREVENCIÓN DEL DELITO CIBERNÉTICO Y EL DERECHO A LA INTIMIDAD EN ECUADOR**", modalidad Proyecto de Investigación, de conformidad con el artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, cedo a favor de la Universidad Metropolitana, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Metropolitana para que realice la digitalización y publicación de este trabajo de titulación en el repositorio virtual, de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Atentamente,

Firmado electrónicamente por:
HECTOR GUILLERMO SALTOS PINTO

Héctor Guillermo Saltos Pinto

C.I. 1717822983

AUTOR

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a Dios porque ha estado conmigo cuidándome en cada paso que doy, por ser mi inspiración y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados en mi vida.

A mis padres, pilares fundamentales en mi vida, quienes han velado por mi bienestar y educación siendo mi apoyo en todo momento, por su amor, trabajo, sacrificio y dedicación en todos estos años ya que son un gran ejemplo de inspiración de buenos padres incondicionales, comprensivos, gracias a ustedes he logrado llegar hasta aquí y poder convertirme en lo que soy, ha sido un verdadero orgullo y privilegio ser su hijo.

A mis hermanos, por ser un apoyo total y estar siempre presentes, acompañándome, apoyándome y guiándome en este proceso, gracias por ser referentes con su magnífica comprensión como hermanos, tíos y padres.

A mis maravillosos hijos, por ser la fuente de mi esfuerzo y dedicación, el tiempo que sacrifique con ustedes para llegar a esta meta hoy tiene sus frutos, gracias por su comprensión y entendimiento, estoy seguro de que vendrán tiempos mejores para nosotros ya que esta meta alcanzada no es solo mía, es tan suya como el de su sacrificio, y solo el tiempo será nuestro mejor juez, y esta carta será el mejor testigo entre el éxito que se nos aproxima.

A todas las personas que me han apoyado y han hecho que este trabajo se realice con éxito en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos a lo largo de mi carrera.

AGRADECIMIENTO

Agradezco a Dios por bendecir mi vida, por guiarme a lo largo de mi existencia, por ser el apoyo y fortaleza en aquellos momentos de dificultad y debilidad, tan solo el conoce muchos sacrificios, sin el nada de esto hubiera sido posible

Gracias a mis padres: GUSTAVO SALTOS CÁRDENAS Y ELSA MARGOTH PINTO CHIRIBOGA, por ser los principales promotores de alcanzar mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado y fomentado a lo largo de la vida. Gracias a mis hermanos que de una u otra manera son la razón por la cual me vi en este punto de mi vida, a puertas de un título profesional tan anhelado, gracias por compartir cada uno de sus conocimientos, experiencias, vivencias, por su tiempo, por su paciencia, por su cariño.

Agradezco a mis docentes de la escuela de Derecho de Universidad Metropolitana del Ecuador.

ÍNDICE

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

RESUMEN

El tema que trata esta investigación es el referido a los ciberdelitos y el abordaje de su prevención para evitar los ataques al derecho a la intimidad. La raíz del problema está en el avance desmesurado de las tecnologías de la información y la escasa protección de los ciudadanos frente a los actos delictivos de los ciberdelincuentes a pesar de las innumerables leyes que se han creado en los diferentes países para evitarlos, pero el ciberespacio es de tal manera libre, que se hace casi imposible frenar este gravísimo problema del mundo, pues los delitos en este espacio se multiplican y diversifican. Ecuador no se queda atrás en estos ataques de los ciberdelincuentes, quienes cometen todo tipo de tropelías contra personas tanto naturales como jurídicas, incluso, contra toda la población como ocurrió en el año 2019, cuando todos los habitantes de Ecuador quedaron sin protección frente a los ciberdelincuentes. Estas situaciones hicieron que las autoridades ecuatorianas tomaran acciones tales como la promulgación de una ley orgánica de protección de datos personales y las reformas pertinentes del COIP. Pero aun los problemas en este espacio persisten y se hace necesario pensar con mayor holgura incorporando a la población en general en los proyectos que se hagan para evitarlos, siendo este el propósito de esta investigación, la cual se desarrolló bajo el tipo mixto, donde se utilizaron métodos como el análisis, la síntesis, el de interpretación, el comparativo, entre otros. En la investigación de campo se utilizó la encuesta, la cual fue aplicada a una muestra de cinco abogados, especialistas en materia constitucional, a 12 abogados que viven en Quito y también a 10 ingenieros en computación. La investigación luego del análisis de resultados terminó con una propuesta para la prevención de los ciberdelitos en Ecuador.

Palabras clave: Ciberdelitos, prevención, víctimas, Derecho de intimidad, Constitución.

ABSTRACT

The topic that this research deals with is that referred to cybercrimes and the approach to their prevention to avoid attacks on the right to privacy. The root of the problem lies in the disproportionate advance of information technologies and the poor protection of citizens against the criminal acts of cybercriminals despite the innumerable laws that have been created in different countries to prevent them, but cyberspace it is so free that it is almost impossible to stop this very serious problem in the world, since crimes in this space multiply and diversify. Ecuador is not far behind in these attacks by cybercriminals, who commit all kinds of outrages against both natural and legal persons, even against the entire population, as happened in 2019, when all the inhabitants of Ecuador were left without protection against the attacks. cyber criminals. These situations led the Ecuadorian authorities to take actions such as the promulgation of an organic law for the protection of personal data and the pertinent reforms of the COIP. But even the problems in this space persist and it is necessary to think more freely incorporating the population in general in the projects that are done to avoid them, this being the purpose of this research, which was developed under the mixed type, where They used methods such as analysis, synthesis, interpretation, comparative, among others. In the field investigation, the survey was used, which was applied to a sample of five lawyers, specialists in constitutional matters,12 attorney who live in Quito, and also 10 computer engineers. The investigation after the analysis of results ended with a proposal for the prevention of cybercrimes in Ecuador.

Keywords: Cybercrime, prevention, victims, right to privacy, Constitution.

INTRODUCCIÓN

Grandes son los beneficios del avance tecnológico en el mundo, entendiendo por tecnología las soluciones y conocimiento que llegó para facilitar la vida de las personas en la sociedad, ella incluso, ha influenciado la forma de vivir, de comunicarse y de relacionarse con los demás. En este contexto, ya las amas de casa no tienen que hacer grandes sacrificios para lavar y planchar la ropa, limpiar, lavar los platos. Tampoco hay que recorrer grandes distancias para hacer mercado, pues los drones traen el mercado a casa, ni hacer grandes viajes para hablar con la familia que está muy lejos, pues los teléfonos, las redes y otros medios mantienen la familia unida. En las oficinas, ya ni siquiera es necesario gastar energías escribiendo porque las máquinas toman el dictado y escriben lo que sea necesario.

Es decir, la tecnología ha traído al mundo grandes ventajas para su desarrollo social, en este sentido no hay duda, que el mundo ha avanzado a pasos agigantados, pero a la vez, ha generado problemas tan graves, que ha sido capaz de destruir la honra e imagen de personas que no se recuperan jamás, ha causado muertes y destruido familias, ha hecho perder grandes fortunas en manos de los hackers, sufrir el espionaje político y empresarial, entre otros, todo ello violando el derecho que tiene toda persona de salvaguardar su intimidad, sean estas personas naturales o jurídicas.

El problema es que como dice la Oficina de las Naciones Unidas contra la Droga y el Delito "La tecnología de Internet hace que resulte fácil para una persona comunicarse con relativo anonimato, rapidez y eficacia, a través de las fronteras, con un público casi ilimitado" (Oficina de las Naciones Unidas contra la droga y el Delito, 2013)

Por eso, la creación de las nuevas tecnologías lamentablemente, ha traído nuevas posibilidades para el aprovechamiento indebido e ilícito, por su capacidad de procesamiento de datos así como de información y acceso generalizado en un medio interactivo que tiene características globales pues ello amplió las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales amigables y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto así como las posibilidades de anonimato en las comunicaciones.

La situación que se presenta en este caso es que, la tecnología implica un intercambio activo de datos personales para el disfrute de algunos servicios. Ello ha generado consecuencias de diversa índole, especialmente dolosas, tales como la estafa, el acoso, extorsión, usurpación de identidad, entre otros y otras situaciones peligrosas para la privacidad y seguridad de los usuarios.

Es entonces indudable, que las nuevas tecnologías hayan traído como consecuencia que la realidad social y la misma sociedad cambie y, por supuesto, con ello, la manera de concebir la comisión de los delitos e incluso, las nuevas tecnologías han hecho emerger nuevos delitos hasta ahora desconocidos. Esta situación tan grave se ha llegado a identificar con el nombre de ingeniería social cuyo objeto es nada más y nada menos que cometer delitos por internet, tales como el hurto de información personal, datos bancarios, así como suplantación de identidad, entre otras, para lo que se utilizan técnicas tales como el phishing, el spam o correo electrónico no deseado, o el programa maligno (malware). Por ello, se han buscado las maneras de controlar estos delitos con soluciones antifraude.

El phishing o también llamado suplantación de identidad, es una manera de engañar a las víctimas usando trucos y engaños para que ésta comparta ya sea contraseñas, números de tarjeta de crédito, y demás información absolutamente confidencial, todo ello en detrimento de la buena fe de las personas que ingenuamente creen que no pasa nada irregular. Es decir, que el phishing no es más que una técnica creada por ciberdelincuentes para cometer fraude, engañar y timar a sus víctimas manipulándolas para que ellas mismas por presión del ciberdelincuente revelen información personal propia confidencial.

El spam, correo basura digital, correo electrónico no deseado o comunicación electrónica no solicitada, por su parte, contiene un programa destinado a infectar tu equipo, dejando que la información y datos personales del usuario de internet sea hackeada por los ciberdelincuentes representando ello indudablemente una seria y costosa amenaza para la víctima.

Finalmente, el malware es una amenaza informática, un tipo de software cuyo objeto es infiltrarse o dañar una computadora o un sistema de información, lógicamente, sin que el propietario lo sepa.

Pues bien, así como se han hecho grandes esfuerzos para prevenir los delitos tradicionales, hay que hacer esfuerzos de prevención de los ciberdelitos reales y contundentes frente a las diversas

formas de esta ciberdelincuencia y esto es exactamente lo que se pretende a través de esta investigación titulada "Abordaje de la prevención del delito y el derecho a la intimidad en Ecuador, año 2021".

La investigación está ubicada en la línea de investigación titulada "Contribución al desarrollo social, a través del mejoramiento de la educación, la salud, y la seguridad ciudadana" así como al Programa "Estudios socio jurídicos sobre políticas del Derecho y prevención de la violencia" y específicamente en el Proyecto de investigación de la carrera de Derecho de la Universidad Metropolitana sede Quito titulado "La prevención del delito como estrategia de control social para el desarrollo de una cultura de paz."

Esta investigación parte entonces de la siguiente formulación de problema, ¿Cómo debe prevenirse la comisión de ciberdelitos para proteger el derecho a la intimidad en Ecuador?

Objetivos.

De esta formulación de problema surgen los siguientes objetivos de investigación:

Objetivo general:

Analizar la forma de prevenir la comisión de ciberdelitos para proteger el derecho a la intimidad en Ecuador

Objetivos específicos:

1. Identificar los fundamentos jurídicos de la prevención del delito y el derecho a la intimidad en Ecuador
2. Diagnosticar la situación de la violación al derecho a la intimidad en Ecuador a través de ciberdelitos.
3. Comparar los fundamentos jurídicos de la prevención del delito y el derecho a la intimidad en Ecuador, Colombia, Perú, Chile y España para el año 2021.
4. Contrastar lo expuesto por la Constitución y las leyes, el diagnóstico y el estudio comparativo en torno a la prevención del delito cibernético y el derecho a la intimidad en Ecuador.

Esta investigación se justifica desde el punto de vista teórico, práctico y jurídico. En lo teórico, porque el análisis y las conclusiones harán un importante aporte a la teoría relacionada con

la prevención de los ciberdelitos y el derecho constitucional a la intimidad en Ecuador, tema que por su novedad ha sido escasamente estudiado en el país.

Desde el punto de vista práctico, el estudio dará importantes aportes para que los organismos del Estado implementen con fundamento en él, políticas para la prevención de los ciberdelitos y se pueda tener mayor seguridad en el uso de las nuevas tecnologías para la protección del derecho constitucional a la intimidad personal.

Desde el punto de vista jurídico, la investigación enriquecerá indiscutiblemente, la ciencia criminológica, especialmente, en lo que a prevención del delito se refiere.

Metodológicamente, esta es una investigación mixta porque utiliza tanto la investigación documental como la de campo. En el caso de la investigación documental se utilizarán las técnicas propias de este tipo de estudios, tales como: la recolección y selección de información, la lectura general y detenida, el subrayado, la integración de contenidos entre otras.

En la investigación de campo se utilizó la encuesta, la cual fue aplicada a una muestra de cinco abogados, especialistas en materia constitucional, a 12 abogados que viven en Quito y también a 10 ingenieros en computación.

El trabajo se desarrolló bajo los parámetros de los métodos de análisis, síntesis, inductivo, deductivo, descriptivo, comparativo, histórico y exegético.

El informe de investigación se estructuró en tres capítulos. En el primero, se desarrolló el contexto teórico. En el segundo capítulo se desarrolló el marco metodológico y en el tercero se hizo el análisis de resultados, las conclusiones y recomendaciones. Este informe consta también de unas páginas preliminares, introducción y referencias bibliográficas.

CAPÍTULO I

PREVENCIÓN DEL DELITO CIBERNÉTICO EN ECUADOR.

1.1 Antecedentes de la Investigación.

1.1.1 Internacionales.

En el año 2018, Vicente Pons Gamón realizó una investigación con nivel doctoral en la Universidad Nacional de España a Distancia (UNED), titulada "Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa nacional e internacional". En esta investigación se trabajó con encuestas y estudios de casos, así como un robusto estudio documental y en sus conclusiones destaca aspectos de interés para la presente investigación, tales como la afirmación de que, con la aparición del ciberespacio, los delitos aumentaron exponencialmente, lo que indica una desventaja del uso de las nuevas tecnologías.

En este sentido indica, que el ciberterrorismo aumenta y en particular, el yihadista, convirtiéndose en una pesadilla para la seguridad de los Estados occidentales, lo que exige una respuesta rápida, contundente y unida para frenas las consecuencias de este nuevo mal para la humanidad.

Otra conclusión es que el internet juega un papel protagónico en esta situación, en este sentido indica que:

> La posibilidad de colgar contenidos en una plataforma fácilmente accesible y sujeta a pocas censuras ha conllevado a aparición de manuales electrónicos, en los que se explica detalladamente cómo y dónde adoctrinarse e instruirse para cometer actos terroristas. Este fenómeno se denomina Universidad Abierta para la Yihad. Los menos desarrollados despiertan forzados por el voraz riesgo a principios-mediados de la década de los noventa. Muchos países son todavía vulnerables al ataque de un hacker. (Pons V. , 2018).

Una información también muy importante que da este estudio es que "son los países desarrollados los primeros que reaccionan contra los delitos cibernéticos, en este sentido, indica que Alemania y Estados Unidos en 1986 formalizan sus primeras actas y normativas". Así mismo indica, que se han fijado estrategias para atacar la ciberdelincuencia y una de ellas es elaborar leyes para frenar todos los delitos que se cometen usando el ciberespacio. (Pons V. , 2018).

Esta investigación no sólo pone al descubierto las consecuencias del uso de las nuevas tecnologías, sino que, además, muestra el rostro de un nuevo delito surgido a las sombras de internet, lo que representa un aporte para este estudio, en el que se afirma que las nuevas tecnologías traen muchos beneficios, pero también muchos perjuicios tanto societales como individuales, por lo que urge tomar medidas contundentes de prevención del delito para minimizar estos males.

En el año 2017, Diego Alexander Alarcón Ariza y Javier Antonio Barrera Barón, realizaron en Lima, Perú una investigación titulada "Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016". (Alarcón & Barrera, 2017)

En el primer capítulo del informe de investigación, se indica que en los últimos años del siglo pasado y lo que va del siglo XXI, ha habido un extraordinario avance de las Tecnologías de la información y la comunicación amenaza a la seguridad. (TICs), por lo que se han presentado nuevos retos en el mundo globalizado, que obliga a estudiar a profundidad los temas que van apareciendo cada día.

En dicha investigación se tuvo como muestra a los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, encontrándose en la indagación que sobre ellos se hizo que, en el año 2016, el 7% de los estudiantes fueron sancionados por plagio y el 5% por fraude en tareas y evaluaciones. Así mismo se encontró, que en la Fiscalía del municipio reposaban el 9,8% de los 16 procesos seguidos por delitos informáticos bajo la modalidad de ciberbullying en las redes sociales por parte de estudiantes de educación Superior.

La investigación fue del tipo cuantitativa correlacional, con diseño no experimental, centrándose en determinar la relación entre el uso del internet y los delitos informáticos, en él se registran datos y se comparan con la teoría e interpretan con los resultados de la estadística.

Este estudio contribuye de manera importante, a evidenciar que los delitos cibernéticos se dan en distintos ámbitos, donde la irresponsabilidad juvenil sirve para solazarse en la maldad y el delito sin importar que las víctimas son sus propios compañeros a quienes exponen al desprecio y burla pública, violentándole el derecho a su intimidad, y con absoluto desprecio por la obtención de conocimiento genuino, cometen delitos como el de plagio.

En el año 2016, Amir Nayi Abushihab Collazos (Abushihab, 2016), realizó una investigación titulada "Cibercrimen. Una aproximación a la delincuencia informática". En esta investigación se destaca la importancia de la informática en la actualidad, incluso cita a Vásquez (2012), quien sostiene que:

> Si volteamos a nuestro alrededor, no es difícil advertir, que nos encontramos inmersos en un mundo digital, totalmente diferente, plagado de avances tecnológicos que facilitan la vida del hombre, pero a la vez, lleno de retos, que nos obligan al conocimiento y a la vez genera nuevos cambios y mayores transformaciones, entre las cuales, definitivamente se encuentran las de tipo jurídico. (Vásquez, 2012).

Dentro de los tópicos que toca en el trabajo se destaca como fundamental para el presente estudio, el aspecto titulado "La tecnología como nuevo factor generador de criminalidad", donde el autor señala que:

> Históricamente, la dogmática jurídico-penal y la criminología han reconocido a la criminalidad como una consecuencia de diferentes factores, los cuales han sido desde siempre las razones que han llevado a las personas inmersas en una colectividad social a la comisión de los diferentes delitos (Abushihab, 2016).

En este estudio se destaca que, si bien es cierto que la tecnología provee de grandes beneficios, también tiene grandes retos, pues además de fallar como cualquier elemento elaborado por el ser humano, puede, además, ser un elemento activo para el abuso de los derechos de propiedad intelectual y violación de la intimidad personal. Es decir, hay vandalismo digital y por eso, hace interpretación en un interesante cuadro esquemático de diversos artículos del Código Penal colombiano, que es de amplio interés para la presente investigación para la realización de la exégesis de las normas del Código Orgánico Integral Penal (COIP) del Ecuador y otras leyes relacionadas con esta importante materia.

Concluye el estudio indicando que el aparecimiento y desarrollo inusitado de las nuevas tecnologías, generan nuevos riesgos concretados en conductas lesivas que inciden sobre el nuevo bien jurídico existente" la información y los datos", por lo que el mismo debe protegerse penalmente.

En 2014, Jorge Adair Larios y Rodrigo Julián Sánchez (Larios & Sánchez, 2014), desarrollaron en México una investigación titulada "Ciberdelito" de tipo estrictamente documental,

donde se estudian aspectos básicos que enriquecen esta investigación tales como: la historia del nacimiento de internet, los delitos contra los sistemas informáticos, delitos relacionados con el contenido, el derecho informático y los ciberdelitos, entre otros.

Entre los delitos cibernéticos explica el hacker, el acceso ilícito a sistemas privados, describiendo los ataques más comunes y a equipos sin contraseña, las utilidades de captura de barrenadores de bios, contraseñas de inicio de sesión, acceso ilícito de manera remota, la inyección de código SQL, entre otros.

La investigación concluyó que:

> Las tecnologías de la información son herramientas y métodos creados para hacer la vida más fácil con las personas con las que se puede recabar, retener, manipular o distribuir información, por ejemplo, enviar correos. Sin embargo, este tipo de tecnologías han sido utilizadas como herramientas para infringir la ley, dañar a terceros o para ocasionar desastres económicos y en algunos casos, hasta sociales. (Larios & Sánchez, 2014).

Esta investigación aportó importantes insumos teóricos al presente estudio, ayudando a comprender no sólo los delitos informáticos sino especialmente, como atacar esos delitos a través de la prevención.

En el año 2007, Libardo Orlando Riascos Gómez (Riascos, 2007), desarrolló la tesis Doctoral en la Universidad de Lleida, España, titulada "El derecho a la intimidad, la visión iusinformática y el delito de los datos personales", que, aunque es una investigación de antigua data, sin embargo, no pierde vigencia y al contrario, hoy cobra más vigencia que nunca, pues a pesar que en su oportunidad indicaba, que los esfuerzos que se han hecho a nivel legal sobre el tema, aun resultan insuficientes, hoy todavía se sigue insistiendo en el mismo problema. En esta investigación se precisa que:

> Un ser humano desde antes de nacer, luego con su nacimiento, crecimiento, desarrollo, muerte, y aún después de ésta, produce una serie de actos, hechos, sucesos susceptibles de documentación (certificados de cualquier tipo y finalidad, registros públicos y privados, obligaciones y contratos); en fin, de informaciones y datos personales, familiares y sociales, los cuales, en mayor o menor grado son sujeto u objeto del derecho y en mayores proporciones de la vida cotidiana, al ser puros y simples y reveladores de la venida, paso y extinción de la vitae humanum. (Riascos, 2007)

Estos datos son absolutamente personales y solo la dueña de estos está en capacidad de autorizar a terceros para que los conozca, lo demás que se haga es una violación a los datos personales.

Esta investigación documental concluye que, en la actualidad, en todos los campos del derecho: legislativo, doctrinal y jurisprudencial hay una gran explosión de documentos jurídicos que llenan las Bibliotecas públicas y privadas en todas partes del mundo, por eso, con el advenimiento de las tecnologías y el apoyo de la informática jurídica documental, hoy se puede acceder a esas bibliotecas para consultar y a la vez, transferir información pertinente, oportuna y eficaz.

Es decir, que la información jurídica se traslada por todo el universo digital sin límites, lo que puede convertirse en una forma de control del Estado al tener el poder de acumular, organizar, manejar y autorizar el acceso a estos datos, así como su utilización, e incluso, recuperación de la información por medios también informáticos.

Todo lo antes expuesto ha dado origen a una rama de la informática jurídica denominada iusinformática, cuyo objeto es el estudio de los datos personales, los cuales se encuentran conceptualizados, definidos, regulados, organizados por categorías y protegidos en las normas jurídicas.

Esta investigación se constituyó en un aporte esencial para el presente estudio toda vez que clarifica en detalle todo lo concerniente a los datos personales.

1.1.2 Nacionales

Alexandra Catalina Ochoa Marcillo en el pasado año 2021, realizó una investigación en Ecuador titulada "Desafíos globales del cibercrimen. Caso Ecuador período 2014 – 2019" (Ochoa, 2021). Esta investigación incorporada metodológicamente al estudio de caso tiene un profuso estudio documental, en el que se tratan aspectos tales como. La definición de cibercrimen, su tipología, teorías, desafíos para el mercado, los usuarios y para el Estado, pero especial importancia para el presente estudio es la mención que se hace a la corriente criminológica en el estudio del cibercrimen y los esfuerzos de implementación de medidas de ciberseguridad. Así como la regulación del cibercrimen en Ecuador, los tipos de amenazas del cibercrimen en Ecuador y los procesos de investigación en esta materia. (Ochoa, 2021).

Se hizo también un análisis de casos relacionados a la revelación ilegal de datos y violación a la intimidad de los ecuatorianos y el hurto de sus datos personales.

La investigación concluye indicando que el ciberdelito se está dando a nivel global a pesar de que ya existe una normatividad legal para regular este tipo de delitos. Ecuador no se queda rezagado en este aspecto, enfrentando los mismos desafíos de todo el mundo; pero la investigadora afirma que son las formas de respuesta que da el Estado el nivel de seguridad informática y protección de los datos privados de los ciudadanos, los que se encuentran expuestos a los delitos de vulneración de los datos que pertenecen a su intimidad.

En todo caso, se evidenció a través de la investigación comparada, que los cuerpos legales con sus respectivas normativas no son suficientes para el control del ciberdelito, así como tampoco son suficientes las políticas hasta ahora adoptadas en esta materia, haciendo falta políticas fomentadoras y consolidadoras de una cultura cibernética, así como compartir experiencias en el campo público y privado sobre la adopción de medidas de ciberseguridad para la protección de datos personales sensibles y la adopción de políticas claras y precisas en esta área, pues su ausencia ocasiona que los actores puedan hacer uso de bases de datos reservados sin control estatal, o incluso, transferir información de datos sensibles de personas a diferentes lugares e instituciones, sin ninguna autorización, como pareciera que fue el caso de la empresa Novaestrat, quien presuntamente provocó el hurto de información de toda la población ecuatoriana en el año 2019.

Esta investigación fue de gran ayuda para el presente debido, a que se presentan los casos específicos y las razones que llevaron al hurto de los datos personales de diferentes personas del Ecuador, poniendo en peligro a todos los que fueron objeto de este delito.

En el año 2018 Carol de las Mercedes Rodríguez Cevallos realizó en Quito, Ecuador una investigación titulada "Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos legales y el proceso para propuesta de ley". (Rodríguez C. , 2018)

Esta investigación de carácter mixto conjugó el trabajo de campo con la investigación documental formuló una clasificación de los delitos en redes sociales, indicando que estos delitos en principio se clasifican en delitos que afectan al software y a los datos, delitos que afectan al

patrimonio, delitos que afectan a la sociedad o a un grupo de personas, delitos que afectan a la persona.

Dentro de estos últimos se ubican: el delito de acoso, delito de amenaza, suplantación de Identidad, delitos contra la intimidad, delitos contra el honor, provocación al asesinato. Dentro del delito de suplantación de identidad esta tanto el delito de suplantación de identidad propiamente dicha como el delito de usurpación de identidad. Dentro de los delitos contra la intimidad se ubican la violación a la intimidad, la pornografía infantil, el sexting y la revelación de secretos. (Rodríguez C. , 2018).

Pero además esta investigación consiguió fuertes vacíos legales en el Código Orgánico Integral Penal (COIP), tales como la falta de tipificación de los delitos de ciberacoso, el child grooming, el sextin, la injuria, pues ésta no se encuentra tipificada como tal, sino que el COIP lo define como calumnia. Tampoco aparece la amenaza, el Phishing, el enaltecimiento al terrorismo y la provocación al asesinato.

Para el momento en que se hizo la investigación existía falta de conocimiento sobre los delitos informáticos en redes sociales, falta de legislación en el Ecuador para sancionar vacíos legales en redes sociales y falta de una adecuada clasificación actual de los delitos que se presentan en redes sociales, por lo que muchos y variados casos de delitos informáticos quedan impunes, a pesar de que el Estado estuvo en conocimiento que en el año 2016 hubo 530 denuncias ante la Fiscalía General del Estado del Ecuador por delitos informáticos.

Adicionalmente el 3 de junio del 2020 se publica la Ley Contra los Ciberdelitos, debido a la existencia de diversos delitos, para ello el Ministerio de Telecomunicaciones promulgo el acuerdo ministerial 017 del 2020.

La investigación concluye que los usuarios de las redes sociales Facebook, Twitter, YouTube y otras, son generadores y consumidores de información, lo que incrementa la probabilidad de ser atacados por ciberdelincuentes, por lo que se hace perentorio, que los usuarios conozcan a cabalidad todo lo relacionado con los delitos informáticos, lo que es de suma importancia para esta investigación. (Rodríguez C. , 2018).

Trávez Carrasco Nathaly Fernanda en el año 2018 (Trávez, 2018), realizó una investigación en Quito titulada "La vulneración de los Derechos Constitucionales por la falta de tipificación de

las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación (TICs)", en la que se expresa que la criminalidad informática nace a partir del aparecimiento y consolidación de las nuevas tecnologías, creándose delitos virtuales sin limitación alguna, lógicamente para hacer daño desde cualquier parte del mundo, a personas naturales o jurídicas, muchas veces atentando contra su intimidad personal, familiar o patrimonial. (Trávez, 2018).

La autora de la investigación para reforzar su opinión sobre las consecuencias de las nuevas tecnologías en el mundo jurídico cita a Javier Alonso González quien sostiene que:

Lamentablemente las leyes no se han adaptado a esta nueva realidad, y existen vacíos y ambigüedades en la normativa que se aplica al mundo digital; las leyes existentes no son coherentes con la naturaleza de internet, un medio que propicia la viralidad de contenidos, la existencia de identidades virtuales, la continua fricción de derechos de autor, o la sátira y el humor gráfico como vehículo de opiniones (González, 2017).

Altamente interesante resulta el análisis que se hace en esta investigación sobre la teoría del delito aplicada a los delitos informáticos y otro elemento fundamental de mencionar, es que la investigación trata en un apartado específicamente el delito contra la intimidad, por lo que resulta de alto interés para el presente estudio.

Saab Carrillo María Daniela y Vinces Fortún Dayana Solange (Saab & Vinces, 2020)en el año 2020 realizaron una investigación en la Universidad Católica de Santiago de Guayaquil titulada "Análisis Jurídico del Derecho a la Intimidad". Esta investigación de tipo documental hace un recorrido histórico del derecho a la intimidad, lo define, señala el contenido y elementos del Derecho a la Intimidad y se refiere puntualmente a la dignidad Humana en relación con este Derecho y luego de analizar los límites a los derechos humanos, desarrolla también un análisis de los límites al derecho a la intimidad y específicamente en Ecuador.

La investigación concluye que el derecho a la intimidad aporta seguridad a la persona humana, que se comporta como unidad frente a los demás humanos, lo que obliga a su respeto sin consideraciones subjetivas. La protección del derecho a la intimidad genera una reacción de protección en cadena de otros derechos humanos. Sin embargo, de acuerdo con esta investigación, el Estado y los administrados pueden llegar a extralimitarse, por lo que se hace necesario poner un

límite de no intervención por terceros, pues el individuo por el hecho de formar parte de un grupo no deja de ser único, autónomo, por lo que ese ámbito de individualidad debe ser protegido.

Además, concluye que tanto la protección de los derechos humanos como el contexto histórico ha generado que este derecho cobre gran importancia y contenido, además, el garantismo hace que este derecho se invoque y aplique con mayor frecuencia, sobre todo en la actualidad cuando las nuevas tecnologías pueden facilitar diversas violaciones a este derecho. Finalmente, los autores concluyen que es un reto para el derecho a la intimidad ponerle límites frente al ejercicio de otros derechos, por lo que puede afirmarse, que a este derecho aun es cuando le queda análisis. (Saab & Vinces, 2020).

El acuerdo ministerial No. - 012-2019 emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información el 11 de junio del 2019 (Ecuador, Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019), expide la guía para el tratamiento de los datos personales en la administración pública.

De conformidad a lo que establece el numeral 12 del artículo 66 de la Constitución de la República del Ecuador.

> Se reconoce y garantiza a las personas, el derecho a la protección de datos e carácter personal, que incluye el acceso y la decisión sobre la información y datos de este carácter, así como su correspondiente protección, la recolección, archivo, procesamiento. Distribución y difusión de estos datos o información requerirán la autorización del titular o el mandato de ley (Ecuador, Asamblea Constituyente, 2008)

1.1.1. Bases Teóricas

1.1.1.1. La prevención del delito

Prevenir significa tomar medidas adelantadas para evitar un suceso. En el caso de la prevención del delito, es tomar medidas prontas ya sea para impedir o para limitar la comisión de hechos que transgredan la ley.

Diego Torrente Robles (1999) afirma que el concepto de prevención se ha venido utilizando para indicar aquellas actuaciones que se orientan a evitar o minimizar tanto el alcance como la severidad de la delincuencia. Es decir, que "Cuando se habla de prevención, se suele pensar en acciones planificadas o realizadas desde el Estado" (Torrente, 1999)

Científicamente, se ha definido la prevención del delito al conjunto de medidas convertidas en políticas cuya finalidad es poner freno a las actividades criminales, imposibilitándolas debido a las dificultades que se les pone o por lo menos haciéndolas menos probables. Así que se trata de medidas que anticipan una dificultad para las personas que quieren cometer un ilícito.

Van Dijk en su oportunidad se refirió a la prevención del delito indicando que son "todas las políticas, medidas y técnicas, fuera de los límites del sistema de justicia penal, dirigidas a la reducción de las diversas clases de daños producidos por actos definidos como delitos por el Estado" (Dijk, 1989). De esta definición se desprende que el autor sustrae la prevención del delito de la justicia penal y que la define como conjunto de políticas, técnicas y medidas para reducir los daños ocasionados por el delito y no como una manera de disminuir el delito incidiendo en sus causas.

Por el contrario el autor Maurice Cusson, afirma que la prevención del delito está referida a la intervención del Estado sobre las causas de los delitos sin la intervención de la justicia penal, con el único objetivo de reducir los riesgos que estos delitos conllevan, en este sentido expresa que combatir el delito, es combatir sus causas; es decir, inhibir las condiciones que originan el acto punible. (Cusson, 2005)

Para Rodríguez Manzanera, prevenir es "conocer de antemano un daño o perjuicio, así como preparar, aparejar y disponer con anticipación las cosas necesarias para un fin" (Rodríguez L. , 1997, pág. 126). Ante ello es obvio, que se requieren entonces, los medios y estrategias para evitar esa conducta criminal con efectos dañosos.

Francisco Álvarez Álvarez, opina que la prevención del delito "constituye el tercer pilar de toda lucha democrática contra la criminalidad y sus causas. La prevención consiste en evitar las conductas delictivas, luchando no solo contra las manifestaciones de estas, sino sobre todo centrándose en sus causas". (Álvarez, 2015)

Obsérvese que, en esta importante cita, a la prevención del delito se le cataloga como el tercer pilar de toda lucha democrática contra la criminalidad y sus causas". Esta frase tan bien lograda significa que la prevención del delito es un mecanismo pacifico, planificado, para evitar que los ciudadanos delincan y así no tener que recurrir a la represión propia del derecho penal y especialmente de los sistemas autocráticos. Así que, en un sistema democrático, todo el esfuerzo

de sus gobernantes debe estar centrado en formular políticas antidelictivas: más educación, más inversión en la pequeña y mediana industria, comercio y producción primaria, más apoyo a la gente y más control sobre los dineros del Estado y freno al narcotráfico.

El autor de esta investigación considera que la frase expresada por Francisco Álvarez Álvarez es muy afortunada y llama a profunda reflexión de los gobiernos del mundo.

Antonio García al referirse a la prevención, indica que hay varias posturas doctrinarias sobre el tema; algunos la relacionan con la disuasión o la obstaculización para que el delito no se produzca. Prevenir entonces sería sinónimo de disuadir al criminal a través de la amenaza del castigo, mientras que otros doctrinarios al tratar el tema hacen referencia es al escenario criminal, aumentando el control mediante obstáculos para encarecer los costes del delito. Una tercera postura en el tema lo tienen los penitenciaritas, para quienes la prevención tiene un efecto teleológico de resocialización y reinserción social.

Antonio García deja bien establecido que, estando el concepto de prevención fundado en las ciencias de la conducta como la psicología, Psiquiatría, antropología, pedagogía, entre otras, es un tema complejo, con una noción mucho más amplia y pluridimensional que lo tratado por el derecho penal.

Pero en definitiva para el doctrinario Antonio García, la prevención del delito va más allá, que son las causas que provocan que una persona delinca, por ejemplo, la pobreza, la falta de empleo, es decir, que al hablar de prevención se está refiriendo a la prevención social. Este doctrinario termina aportando una clasificación de los modelos teóricos de prevención.

César Herrero en consonancia con lo establecido por Antonio García, sostiene que:

> El concepto de prevención ha de trascender, por ello, los ámbitos del derecho y, sobre todo, las fronteras del Derecho Penal en su triple dimensión: sustantiva, procesal y penitenciaria. Un auténtico esquema preventivo ha de descansar, para ser mínimamente eficiente, sobre las bases de una política criminal (Herrero, 1997)

Entonces para Herrero César, la prevención debe ser tratada en diferentes dimensiones, pero siempre fundamentada en las políticas establecidas para poner freno al delito, sin tocar en absoluto el derecho penal. Lo que deja claro que el delito no es un tema exclusivo del Derecho Penal, sino

que existe la ciencia criminológica que también trata sobre el delito, pero especialmente, como prevenirlo atendiendo sus causas a través de políticas criminales sólidas.

Para cerrar estas definiciones de prevención del delito se dejó a propósito para el final del tema, la dada por Franz Vanderschueren, quien según el autor de esta investigación es la más completa, en este sentido, el autor citado sostiene que la prevención del delito "es un concepto proactivo dado que busca anticiparse a los hechos. Se trata de evitar, mediante intervenciones anticipatorias de política pública que los niveles de criminalidad en una sociedad lleguen a niveles intolerables". (Vanderschueren, 2006., pág. 20).

Dos cosas destacan en esta definición, por una parte, que la prevención del delito es evitar hechos delictivos por la anticipación que se haga para su no ocurrencia, segundo que para ello es importante tener políticas públicas relacionadas a la problemática de los delitos, pero además se reconoce en esta definición que el delito siempre va a existir pero que su ocurrencia puede estar en un nivel tolerable. Claro habría que ver cuál es ese nivel tolerable y para quien es tolerable, porque seguramente la o las víctimas de un delito no aceptarán que hay niveles de tolerancia del delito.

En este mismo orden, la Organización de Naciones Unidas (ONU) citada en "La Prevención del Delito en Chile. Una visión desde la comunidad" (Dammert & Lunecke, 2004), define también la prevención del delito como:

> Toda acción orientada a evitar que el delito ocurra, promoviendo la seguridad no sólo a través del sistema formal de justicia criminal, sino que también a través de la promoción e implementación de estrategias que involucran a los diferentes sistemas informales de prevención como los colegios, instituciones religiosas y ciudadanía en general. (Dammert & Lunecke, 2004).

Obsérvese que la Organización de Naciones Unidas al igual que Franz Vanderschueren al tratar el tema de la prevención del delito se refieren a ella como una acción anticipatoria al delito, pero le da además el beneficio de promover la seguridad ciudadana y aquí además acepta que existe una prevención formal y una informal, incorporando en esta última la educación la religión y la propia ciudadanía.

Estas definiciones dadas, especialmente las dos últimas, se sintetizan en el artículo 393 de la Constitución vigente en Ecuador, la cual establece:

> El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno. (Ecuador, Asamblea Constituyente, 2008)

Para la Constitución de Ecuador, son las políticas y acciones integradas, que responden a lo que se ha denominado prevención del delito, lo que genera seguridad.

Luis Salvatierra Párraga y Mercedes Cedeño Barreto en el año 2019, se referían a que:

> Las medidas de prevención social en el ámbito de seguridad integral se adoptan debido a causales de carácter social como la pobreza, el desempleo, la deserción escolar, la drogadicción, características culturales que exacerban factores que generan amenazas a la integridad individual y colectiva. Estas aportan al mejoramiento de las condiciones de seguridad de los entornos urbanos y barriales, desarrollando intervenciones orientadas a la solución de problemas y reducción del desorden físico en áreas específicas, lo cual incrementa la participación, responsabilidad, cohesión y la reducción del miedo que presenta la comunidad ante ciertas prácticas en espacios públicos que han sido violentados o se han vuelto vulnerables (Salvatierra & Cedeño, 2019)

En este caso, los autores plantean con claridad las causas de la delincuencia: la pobreza, el desempleo, la deserción escolar, la drogadicción, características culturales que exacerban factores que generan amenazas a la integridad individual y colectiva, todas ellas, son objeto de estudio de la prevención del delito indicándose que éstas causas se minimizan a través de las acciones de la prevención del delito.

Llegado a este punto es necesario definir las políticas a las cuales hacen referencia los diferentes autores como aquellas que "se encargan de estudiar e implementar medidas para la prevención y control del delito". (Serrano, 2009)

Es evidente entonces, que el tema de la prevención del delito viene siendo tratado desde hace muchos años, como una alternativa a la justicia penal objetiva y castigadora. No se puede decir, que la justicia penal sobra o no hace falta, porque luego de cometerse un delito, se hace necesario que el culpable sea sancionado proporcionalmente al delito cometido, pero, si esto es necesario, más lo es, que el Estado busque las causas que provocan esos delitos y para ello, se encuentra en posesión de los estudios criminológicos sobre la prevención del delito que va más hacia las causas que los provocan y las políticas que deben establecerse para evitarlos.

El Estado es el responsable de administrar los recursos, fomentar estrategias y ofrecer a la ciudadanía seguridad. Por lo que es inexplicable, entonces, que teniendo el Estado estas responsabilidades, se dedique más al castigo, que a poner coto mediante sus políticas al cometimiento de delitos. ¿Educa de verdad el Estado a sus ciudadanos? ¿Les garantiza de verdad el empleo digno? ¿Los funcionarios del Estado realmente manejan los fondos públicos con pulcritud para evitar la corrupción y el escape de dinero que puede servir para ofrecer servicios dignos a la población? Estas y muchas preguntas más están en el debate público, pero lamentablemente, las respuestas no son las más deseables.

Existe una especie de interés no manifestado, pero si evidente, que las graves situaciones por la que atraviesan los pueblos sigan así: hambre, pobreza, ignorancia, corrupción, delitos, porque de esa manera, es más fácil controlar a la población para fines propios e inconfesables. Muchas ideologías dominantes, conquistan a los pobres con discursos mesiánicos, con el único objeto de hacer uso de ellos de manera pacífica poniéndolos a su servicio. Es el asunto de la pobreza manipulada.

Por eso precisamente, la Organización de Naciones Unidas ha venido exponiendo su preocupación en torno a conocer las causas de la criminalidad, como el narcotráfico, el consumo de drogas, los procesos que ocasionan pobreza con sus secuelas de falta de educación, desarrollo económico y desarrollo social, y del atraso de las naciones. En este sentido, la Organización de las Naciones Unidas ubica dentro de los factores criminógenos y a la vez preventivos informales del delito a la familia, la comunidad, la educación, los medios de comunicación social entre otros, y ha sostenido, que las políticas, estrategias y programas de prevención del delito deben tener una sólida base de conocimientos multidisciplinarios sobre la delincuencia, las causas que la producen y las prácticas que deben implantarse, para lograr el objetivo de minimizar el delito y sus daños subsecuentes.

Es decir, que los órganos de gobierno si quieren entender la criminalidad con fines de minimizarla, deben darle prioridad a planes y programas con suficientes fondos a fin de ofrecer a la ciudadanía buenos servicios de salud física y mental, de prevención tratamiento y rehabilitación en materia de drogas y alcoholismo, buena alimentación , vivienda, transporte, servicio educativo, de recreación y cultura, y estar pendientes de que los fondos sean bien administrados

Es decir, se requiere una buena planificación, ejecución y evaluación de las acciones emprendidas. En este sentido, el Estado debe propiciar la prevención más que la represión, pues la historia de la humanidad viene indicando, que se gastan ingentes recursos en la represión y el delito en vez de disminuir, aumenta.

En el caso específico de Ecuador, la ex ministra del Interior expresaba en la introducción del Plan Nacional de Seguridad Ciudadana y Convivencia Pacífica 2019-2030:

> Gran parte de las violencias que subsisten en nuestro país encuentran sus causas en aspectos culturales y estructurales, que deben ser comprendidos y abordados de forma integral. El origen de estas violencias está estrechamente ligado con la discriminación, la falta de educación, la falta de oportunidades, la pobreza, el desempleo, la inequidad, la exclusión social, entre otros factores que generan condiciones que fomentan la violencia en nuestro entorno social. Estos elementos facilitadores de la violencia se constituyen al mismo tiempo en factores de vulnerabilidad para nuestra sociedad. (Ecuador, Ministerio del Interior, 2019).

1.1.1.2 El delito cibernético

El senado de México definió el delito informático o cibernético de la siguiente manera:

> Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como un delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática. A partir de los atentados del 11 de septiembre esta definición se amplió y hoy día es, básicamente, cualquier delito perpetrado a través de un ordenador, sea cual sea su fin. Hay cientos de tipos de ciberdelitos, los más frecuentes son el Phising, el Fraude bancario, el uso de redes para el tráfico de drogas y el SPAM. (México, Senado de la República, 2015)

Joel Meléndez Verdesoto por su parte define el delito cibernético como:

> Aquellos que afectan la información y al dato como bienes jurídicos protegidos, es decir, la información que un usuario tiene dentro de una cuenta de correo electrónico y el dato protegido de una cuenta bancaria, los datos que se contienen en un celular, los datos que se contienen en el sector

> público o privado, la identidad de ciertas personas que están protegidas por el Estado y la ley. (Meléndez, 2018)

Recalca Meléndez, que:

> Los delitos informáticos son aquellos actos cometidos a través de las TIC, que afectan a bienes jurídicos protegidos mediante el uso indebido de equipos informáticos, a simple vista podríamos decir que son: el patrimonio, la intimidad, la integridad física y/o lógica de los equipos de cómputo y/o páginas web cuando ella no impliquen las dos anteriores, como también otros bienes jurídicos tutelados por la Constitución. Los delitos informáticos o ciberdelitos, es toda actividad ilícita que: a). Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o b) Tienen por objeto robo de información, robo de contraseñas, fraude a cuentas bancarias (Meléndez, 2018) .

Enrique Ruiz Vadillo haciéndose eco de la definición que hace la Organización de Cooperación y Desarrollo Económico (OCDE), expresa que es "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos" (Ruíz, 1996). Por su parte, el Ministerio del Interior y Seguridad Pública de Chile, ha definido este delito como:

> Todos aquellos delitos tradicionales que terceras personas cometen utilizando medios tecnológicos. Estos no cumplen los requisitos de los informáticos, pero son igualmente sancionados por otros tipos penales de nuestra legislación. Ejemplos de delitos computacionales: Usurpación de nombre, estafas y otras defraudaciones, amenazas, delitos contra la propiedad, entre otros (Chile, Ministerio del Interior y Seguridad Pública, s.f.).

Finalmente, Gustavo Sain, especifica que:

> En la actualidad, no existe un consenso global en relación con este tipo de conductas ilícitas, tanto en el ámbito de derecho como en la criminología. La ausencia de una definición específica se demuestra a partir de las diferentes denominaciones que reciben este tipo de conductas, "delitos informáticos", "crímenes cibernéticos" "delitos relacionados con computadoras" "delitos electrónicos", "crímenes por computadoras", "cibercrimen", "delitos telemáticos", entre otros. (Saín, 2012)

En base a las definiciones anteriormente citadas, puedo establecer que el delito informático hace referencia a un acto o conducta criminal típica, antijurídica y culpable, antiética que se da por

vías informáticas con el objeto de destruir y dañar ordenadores, medios electrónicos y redes de Internet, para lograr un fin que puede ser económico, ideológico político o religioso o de venganza, afectando con ello la información y al dato como bienes jurídicos protegidos.

Ya dilucidada la definición del ciberdelito, delito informático o cibercrimen, se inicia el gran debate teórico indicando que, la delincuencia internacional ha crecido de una manera exponencial gracias a las nuevas tecnologías, por las características de ser transfronteriza, en este contexto, el delito cibernético es una manera emergente de esta delincuencia transnacional, que crece a pasos agigantados y ello debido indiscutiblemente, al crecimiento y mejoramiento cada vez mayor del internet en cuanto a medio que ofrece una infinita gama de informaciones y comunicación.

Guillermo Chas al referirse al aumento del ciberdelito ha mencionado que:

> En pleno Siglo XXI, no es de extrañar que los delincuentes hayan adaptado su modus operandi para aprovecharse de las ventajas que les ofrecen herramientas como internet para cometer actos ilícitos. Por el contrario, las redes son hoy un nuevo espacio público, donde, al igual que en el espacio público tradicional, se pueden cometer, y de hecho se cometen, numerosos delitos (Chas, 2021)

En este sentido, en la actualidad según los indicadores dados por las mismas empresas que ofrecen el internet, indican que este medio tiene aproximadamente dos mil millones de usuarios en el mundo, convirtiéndose así el ciberespacio como un lugar extraordinario para los transgresores de la ley, debido a que pueden permanecer anónimos y a su vez lograr el acceso a toda la información personal de los incautos que, utilizan este medio para guardar su información, poniendo al servicio de los ciberdelincuentes esta información.

De aquí que hoy, según los estudios especializados en la materia indican que últimamente el delito cibernético ha alcanzado aproximadamente a más de cuatrocientos treinta y un millón de víctimas adultas en el mundo y su crecimiento es tan grande, que se ha convertido en un negocio que supera los tres mil billones de dólares al año.

Ahora bien, el delito cibernético presenta diversas caras, pero al parecer los más comunes son los delitos relacionados con la identidad, lo que ocurre por phishing engañando a los usuarios para que aporten sus datos personales. También está el malware que consiste en un software, que ha sido instalado involuntariamente a través especialmente de cookies, que también se apropia de

información personal y, el hacking que significa acceder ilegalmente a la computadora de un particular de manera remota. El acceso de los ciberdelincuentes a los datos personales es para robar información especialmente de dinero y tarjetas de crédito.

Pero no conformes con hurtar datos personales, internet se ha convertido en un verdadero paraíso para delitos que tienen que ver con los derechos de autor y derechos de propiedad intelectual; así como para los delitos relacionados con pornografía infantil. A estos delitos ayuda el hecho de que, a esta altura del avance de internet, los ciberdelincuentes ya no necesitan grandes habilidades para convertirse en amenaza y en este sentido, pueden localizar puertos abiertos, y anular la protección de contraseñas comprándolas en línea, con gran dificultad para encontrar a los responsables de los ciberdelitos debido al anonimato del ciberespacio, lo que dificulta a la policía identificar a los delincuentes organizados.

Es tal la organización de este tipo de delincuentes, que hace absolutamente necesario que los Estados también se organicen con normativas adecuadas y ampliando su capacidad de lucha contra ellos, pues es indiscutible, que los ciberdelincuentes avanzan con mayor rapidez, que las leyes protectoras, Guillermo Chas al referirse a esto indica "el derecho siempre corre atrás de los hechos" (y que, por ese motivo) hay conductas delictivas del mundo digital todavía no están tipificadas en las leyes penales" (Chas, 2021)

Por lo que hace falta un esfuerzo más sostenido e inteligente de todos los países del mundo para acechar a estos delincuentes y sancionarlos, porque cada día ellos ganan más espacio y las víctimas crecen, al extremo que el Informe Norton sobre delincuencia cibernética de hace diez años indica, que aproximadamente se producen un millón de víctimas diarias, una víctima adulta por segundo, especialmente por el mal uso de las tarjetas de crédito. Sobre este particular, Guillermo Chas afirma que "el gran desafío de la justicia es combatir al cibercrimen" (Chas, 2021)

En este contexto, el investigador considera que lo más importante para atacar a los ciberdelincuentes, es entender que ellos se esconden en el anonimato para cometer sus fechorías.

Según Gustavo Saín, la Organización de Naciones Unidas reconoce como tipos de delitos informáticos los siguientes:

> Fraudes cometidos mediante manipulación de computadoras**;** en este se reúne: la manipulación de datos de entrada (sustraer datos), manipulación de programas (modificar programas del sistema o

> insertar nuevos programas o rutinas), manipulación de los datos de salida (fijación de un objeto al funcionamiento de sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a otras). Manipulación de datos de entrada; como objetivo cuando se altera directamente los datos de una información computarizada. Como instrumento cuando se usan las computadoras como medio de falsificación de documentos. Daños o modificaciones de programas o datos computarizados**;** entran tres formas de delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por sabotaje) (Saín, 2012)**.**

De la cita se desprende que, son muy variados y complejos los ciberdelitos, porque en la actualidad es prácticamente imposible utilizar otro medio que no sean las computadoras, para trabajar, para estar informado y hasta para recrearse. El problema radica en buscar los mecanismos para usar este recurso sin riesgo, porque, además, toda transacción monetaria que se haga utiliza este recurso.

1.1.1.3 Historia de los delitos cibernéticos

Nada que ocurra hoy, se inició hoy, siempre hay una historia que lo respalda, en este sentido, si se quiere entender el ciberdelito hoy, es necesario remostarse a décadas pasadas, cuando este delito empezó a echar raíces. Así que, a decir de Gustavo Saín:

> Los orígenes de los delitos informáticos pueden rastrearse a partir de los años 60s por el temor infundido por la literatura de la época en relación con la recolección y almacenamiento de datos personales en computadoras. Éste tiene como referencia la obra "1984" de George Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías. (Saín, 2015)

En la década de los 60 diversos periódicos se refirieron a casos relacionados con los delitos cibernéticos, lo que dio origen a un tipo de literatura para tratar estos temas denominado ciberpunk. En esta misma época durante la guerra de Vietnam, algunos programadores norteamericanos boicoteaban el financiamiento del gobierno a esta guerra utilizando el servicio telefónico gratuito. Los hippies, también hackearon la telefonía para hacer llamadas gratuitas, pero a posteriori, el hackeo se perfeccionó para transferir dinero utilizando también las redes telefónicas vulnerables.

Refiere Vicente Pons Gamón que: "A partir del desarrollo acelerado de la internet, también emerge el lado oscuro y surgen nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio" (Pons V. , 2017)

Las características de estos delitos son destacadas por Subijana Zunzunegui, cuando explica que:

> Se cometen fácilmente; requieren escasos recursos en relación con el perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas (Subijana, 2008)

Para la década de 1970 empiezan a aparecer preocupantes casos de hackeo donde se pierden ingentes sumas de dinero del sector privado. Es decir, que aparecen los delitos económicos informáticos, a través del espionaje, la piratería de software, el sabotaje y la extorsión.

Según indica Saín:

> En relación con el espionaje, estos se llevaban a cabo mediante la copia directa desde los dispositivos informáticos, el robo directo de los mismos para la extracción de información -discos duros, diskettes-, y la absorción de emisiones electromagnéticas para la captación de datos. Los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas (Saín, Pensamiento penal, 2015) .

La piratería de software por su parte tiene como modalidad específica, la copia sin autorización alguna, de los programas de computación para después venderlos, lo que entra en el tipo de espionaje industrial.

Pero eran el sabotaje y la extorsión informática, los delitos que preocupaban y siguen preocupando más a los gobiernos y empresas, debido a que estos entes guardan una alta cantidad de datos electrónicos. En el pasado, los objetivos tanto del sabotaje como de la extorsión informática eran atacar bienes tangibles, como son los dispositivos físicos, a la vez que atacaban bienes intangibles, tales como los datos e información, con lo que afectaban tanto el hardware como el software de los dispositivos.

Un ejemplo concreto de los daños que causaban era la postura de bombas caseras en la década de los 70, para acabar con instalaciones y dispositivos informáticos, especialmente de empresas como venganza por problemas laborales.

Pero en esta década de los 70 del siglo pasado, también se produjeron grandes fraudes financieros con el uso de las nuevas tecnologías, especialmente, en Estados Unidos aprovechando las fallas en los sistemas de seguridad de las redes y la escasa experiencia de los administradores de los sistemas. En este preciso caso, se ha dicho que el modo de operar era, manipulando facturas relacionados con pagos de salarios de personal y, además, los balances de pagos de los bancos.

Pero la década de los 80 demostró que los delincuentes informáticos habían obtenido una mayor especialización en sus delitos, lo que les permitió cometer más fraudes a través de la manipulación de tarjetas de débito especialmente en cajeros automáticos, vulnerando de las bandas magnéticas. Pero esto también ayudó a que las empresas pusieran en práctica nuevas ideas preventivas, como es el uso de chips en los plásticos.

La situación llegó a ser tan grave, que después de casi treinta años de estarse desarrollando y perfeccionando los delitos informáticos, que se empiezan a promulgar leyes en Europa para su protección, especialmente, del dinero electrónico, situación ésta que ya se había iniciado en Estados Unidos a finales de la década de los 70. Sin embargo, a pesar del tiempo que lleva la problemática de este tipo de delitos, en Latinoamérica empezó tardíamente la estrategia de poner coto a estos delitos con medidas de orden legal.

Pero a medida que se avanzaba en las leyes que protegían contra los delitos informáticos que iban apareciendo, los delincuentes de esta área también iban perfeccionándose en otros delitos tales como la publicación en las redes de contenidos ilícitos, en los que entraban las amenazas, la incitación al odio, la pornografía infantil, y los mensajes racistas y xenofóbicos. Pero lo más grave fue cuando los ciberdelincuentes empezaron a manipular los sistemas de vuelo o los sistemas hospitalarios y de salud, lo que fue catalogado como ciberataques contra la vida.

Pero al parecer las primeras definiciones acerca de los delitos informáticos se produjo en el año 1983**,** cuando la Organización de Cooperación y Desarrollo Económico (OCDE), citada por Joel Meléndez Verdezoto señalaba que era "cualquier comportamiento antijurídico, no ético o no

autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos" (Meléndez, 2018) .

Por otra parte, Meléndez Verdesoto también reporta que el virus informático denominado "Troyano"**,** fue el nombre del primer virus masivo reportado IBM PC en 1984, a raíz de esto, varios Estados de los E.E.U.U. fueron los primeros en contar con una ley específica para proteger los sistemas informáticos de las instituciones públicas. (Meléndez, 2018)

Esta grave situación llevó a los gobiernos, especialmente al alemán a identificar los delincuentes cibernéticos, como fue el caso de los hackers que estaban utilizando las redes internacionales para acceder a información privilegiada de los Estados Unidos y Gran Bretaña para luego venderla a los rusos.

A finales de los años 90, se produce la apertura global de Internet por parte de la administración norteamericana y el vaciado de las empresas y bancos a la red con el objetivo de desarrollar el comercio electrónico, y allí nace una nueva preocupación que era el desarrollo de estándares de encriptación muy seguros para desarrollar operaciones comerciales y financieras, especialmente para usar estas redes para la compraventa de productos en línea. En este sentido, la encriptación de datos o también llamado cifrado de archivos consiste en un procedimiento mediante el cual los archivos u otros documentos, se convierten en totalmente ilegibles utilizando un algoritmo que desordena sus componentes. De esta manera, quien no tenga la clave correcta no puede acceder a la información.

Finalmente, muchos problemas han tenido que enfrentar tanto la industria discográfica como la cinematográfica por el plagio de sus obras protegidas, violándose de esa manera los derechos de autor, siendo el modus operandi, la descarga en línea de música y películas.

De esta manera, empezó a verse un movimiento internacional más concertado para atacar a los delincuentes cibernéticos, pero aun hoy, en el año 2022 del siglo XX, no se han encontrado los remedios eficaces para atacar esta problemática que es mundial y que perjudica en alto grado las transacciones comerciales, el manejo financiero y los derechos internacional y constitucionalmente protegidos. Al parecer tiene razón Meléndez Verdesoto cuando expresa "El delito informático o delito cibernético, son los nuevos verdugos de esta sociedad tecnificada, mientras que la tecnología evoluciona, el delito crece" (Meléndez, 2018) .

En cuanto a los ciberdelitos en la actualidad deben destacarse fundamentalmente cinco aspectos puntuales: el ciberterrorismo, el cyberespionaje, la ingeniería social, la Ciberguerra y el aparecimiento de nuevos virus informáticos.

1.2 Tipos de delitos cibernéticos

1.2.1 El ciberterrorismo

La autora Alicia Chicharro Lázaro define ciberterrorismo como "el uso de las nuevas tecnologías con fines terroristas" (Chicharro, 2009) y el Consejo de Europa lo define como "El uso de las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos" (Subijana, 2008)

Los terroristas, sean ellos de tipo religioso, político y con interés económico, utilizan las nuevas tecnologías para ocasionar daño y lograr sus fines preconcebidos por ello no es extraño que actúen con la intención de causar pánico colectivo, y alarma social. En este sentido, los cyberterroristas lanzan sus ataques a sus objetivos, siendo ellos, equipos informáticos, redes o simplemente la información recogida en estos equipos. Así mismo, pueden atacar sistemas individuales y redes, e incluso, servirse de las redes, especialmente internet para hacer propaganda, incitar a la rebelión, amenazar a sus expositores, realizar proselitismo especialmente religioso o político y realizar el reclutamiento a nuevos miembros para sus causas.

Un ejemplo, es la existencia en internet de sitios "yihadistas", que apoyan el terrorismo y constituyen verdaderas escuelas donde se debate, se intercambian ideas e información de todo tipo, incluso, se enseña a construir bombas y como hacerlas estallar en un ataquen y lo que ocurre es que los cyberterroristas lo que desean siempre es desestabilizar las estructuras sociales existentes. Los países que más han sufrido actos terroristas son el Reino Unido, Estados Unidos, España y Francia.

1.2.2 El ciber espionaje

El Servicio de Seguridad MI5 del Reino Unido, citado en el Módulo 14 de la Serie de Módulos Universitarios: Delitos Cibernéticos de la UNODC, define el cyberespionaje cuando indica que:

> Aunque no existe una definición única y universal de espionaje, éste se ha descrito como un método de recopilación de datos de inteligencia: en particular, como un proceso de obtención de información que normalmente no está disponible públicamente, utilizando fuentes humanas (agentes) o medios técnicos (como el hackeo de sistemas informáticos) (Oficina de las Naciones Unidas conre la Droga y el Delito, 2019).

En definitiva, el cyberespionaje se define como una actividad de personas, empresas o grupos, consistente en el uso de las tecnologías de la información y la comunicación (TIC) para lograr sus beneficios económicos o personales El ciber espionaje también puede ser perpetrado por personeros gubernamentales o grupos dirigidos por el Estado, para obtener acceso no autorizado a sistemas y datos siendo su objeto, recopilar información de inteligencia para entre otras cosas, mejorar la seguridad nacional, u obtener información para la competitividad económica o la fuerza militar del país y como es de esperarse las TICS han jugado un papel relevante en la aplicación de la inteligencia ilícita en beneficio del país o empresa que contrata este servicio.

Las tácticas utilizadas por los autores de ciberespionaje, son entre otras, la denominada ingeniería social, la distribución de programas maliciosos, el spear phishing y los ataques de watering hole. En el caso específico de Gauss, el mismo fue diseñado para colectar datos especialmente sobre las conexiones de red, así como los controladores y los sistemas de procesos y carpetas, a ello se le agregó, infectar con programas espía con el fin de obtener información de otros sistemas y poder transmitir esta información a un servidor bajo el control del espía.

En cuanto a la ingeniería social, ella es una herramienta destinada al ciberespionaje que se define como engaño del objetivo con el fin de que revele información o realice otra acción. La táctica más utilizada en este caso es el spear phishing, el cual cumple la tarea de enviar correos electrónicos con archivos adjuntos o también enlaces infectados lógicamente diseñados para engañar al receptor y que cliquee los archivos adjuntos o enlaces.

Edgar Jair Sandoval al tratar el tema de la ingeniería social sostiene que:

> La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo. La Ingeniería Social se sustenta en un sencillo principio: "el usuario es el eslabón más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una

> vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla (Sandoval).

Un ejemplo de ingeniería social fue lo que ocurrió con la campaña Night Dragon, donde se utilizaron tácticas combinadas de ingeniería social, a lo que se sumaron una serie de programas maliciosos con el objeto de obtener acceso ilegal a los sistemas de las empresas de energía del mundo en muchos países, y por supuesto, para lograr información sobre las operaciones que realizaban. Una situación en este caso de alta significación es que existen empresas privadas que son contratadas para que ayuden con los actos de ingeniería social.

1.2.3 La ciberguerra

La Ciberguerra o también denominada guerra tecnológica es el uso de ataques digitales de un país con el propósito de dañarle los sistemas informáticos más esenciales a otro país, para lo cual se pueden utilizar virus informáticos o incluso, lanzar ataques de piratería informática. Esta Cyberguerra tiene como objeto hallar las vulnerabilidades técnicas y tecnológicas de los sistemas informáticos del país que se tiene como enemigo, por supuesto para atacarla y a través de ello, obtener información sensible, o puede ser incluso, por el placer de dañar o destruir servicios esenciales de ese país considerado enemigo. Estas Cyberguerra las hacen los hackers a distancia, a través de medios tecnológicos altamente sofisticados.

Lo grave de la cyberguerra, es que ella es fuente de fuertes conflictos internacionales para lo que no existen normas y si las hay son absolutamente endebles, lo que significa un alto riesgo por el uso de estas armas, pues, el ataque en una guerra cibernética, son de gran alcance y están dirigidos a sitios estratégicos. Hoy puede decirse sin lugar a dudas, que las potencias más desarrolladas en cyberguerra son: Estados Unidos, China, Rusia, Israel, Irán, Australia, India, Paquistán y Corea del Sur.

1.3 Los nuevos virus informáticos

Se ha dicho, que los nuevos virus informáticos son más virulentos que los anteriores, especialmente para hurtar datos confidenciales y dañar para siempre la computadora. Los cuatro virus más peligrosos actualmente son: los CryptoMix Clop Ransomware, el Jokeroo, el Trojan Glupteba y el Slammer Worm.

El primero, es una amenaza tanto para los datos confidenciales como para los datos de otras personas que estén conectadas a la misma red, lo que significa, que este virus no sólo se orienta a una computadora individual, sino que tiene como objetivo toda la red, desactivando el antivirus protector de la computadora. Pero es que, además, cifra los archivos que están en la computadora y es capaz de cambiar la extensión a extensión. Después se le informa a la compañía o a las personas, sobre la realización del ataque y lo más grave es que además de ocasionarte daños, el hacker exige un pago para el rescate de la información y amenazan con deshabilitar todas las herramientas de protección si no se accede fácilmente a llegar a acuerdos con ellos.

1.3.1 Jokeroo

Los Joker son los que colocan los virus. En el caso del Jokeroo este virus funciona en la misma forma del Ransomware, al ingresar a la computadora la deja totalmente limpia de dinero, y clave para descifrar datos.

1.3.2 Troyano Glupteba

Es un virus que está en pleno crecimiento y consolidación. Su técnica de entrada al sistema es parasitaria de otro malware y una vez que se empodera en el software del sistema, no hay manera de saber que el ordenador ya se infectó del virus, pues finge una legitimidad que no tiene para comunicarse en forma directa con la dirección IP y por supuesto, los puertos y así es como logra recopilar información de tipo confidencial, dirigiéndolo además hacia otros malos dominios tales como travelsreview.wo, sportpics. xyzkinosport.top, entre otros. Pero existe una forma para proteger la computadora que es habilitando los filtros de correo electrónico y web, y, además, restringir las macros.

1.3.3 Gusano Slammer

La velocidad de este virus es lo que lo caracteriza e infecta más de 75000 PC en tan solo 10 minutos y entre otras cosas, ralentiza Internet, además, ya infectada se extiende hacia otras computadoras por su propia replicación.

De esta manera, estos virus, por acción de los delincuentes cibernéticos, infectan las computadoras, causando graves daños, pues para nadie es desconocido, que las computadoras personales son un verdadero depósito de información también personalísima de cada persona que la posee, donde deposita todo tipo de información, tales como. Claves, recibos, números de cuentas bancarias, comunicaciones de todo tipo, documentos profesionales y comerciales, e incluso, propagandas, de interés de la persona.

1.4 El caso de hackeo de datos en Ecuador

Lizette Abril en el año 2021, realizó una publicación en el periódico El Comercio, comentando que:

> La transformación digital que vive el mundo, sobre todo en época de pandemia, ha hecho que la industria del cibercrimen se prolifere por ser un negocio multimillonario. Cada vez es más común que se perpetúen ataques a los datos financieros y personales de las personas a través de malware. De acuerdo con el reporte de seguridad de ESET de 2021, entre los cinco códigos maliciosos más usados por los hackers están los virus, troyanos, gusanos, spyware y ransomware. Solo durante 2020, según ESET, en Ecuador hubo más de 51 mil registros relacionados con cryptominers (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de exploits (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de ransomware (malware para el secuestro de información) y casi ocho mil detecciones de spyware (software espía), como datos de algunos tipos de software malicioso. (Abril, 2021)

En este contexto, Ecuador tiene aproximadamente entre 17 y 18 millones de habitantes actualmente, y, al parecer, la mayoría de los datos personales como número de cédula, dirección, información de contacto, de la población ecuatoriana, fueron filtrados el 19 de septiembre del año 2019, debido a que presuntamente un servidor sin los protocolos de protección requeridos fue utilizado por la empresa Novaestrat, ubicada en Miami, dedicada al análisis de datos contentiva de información personal sobre los ecuatorianos.

Ante tan grave situación el gobierno ecuatoriano se avocó a la investigación de los hechos y logró confirmar la grave y real situación de filtración de datos. Necesario es aclarar, que la filtración de datos se define como la grave violación de información confidencial o de datos sensibles, de los usuarios en Internet. Estas situaciones traen como consecuencia exponer a las personas a una situación de riesgo entre otras de robo de identidad y además fraude financiero, entre otros.

Lo interesante vino cuando un hackeo ético hecho por la empresa vpn Mentor logró descubrir el problema de seguridad que expuso los datos de los ecuatorianos, catalogando la brecha de seguridad encontrada como la más grande filtración de datos del país en toda su historia. Para hacer el estudio se utilizó la información del Biess, de la Asociación de Empresas Automotrices del Ecuador y del Banco Nacional.

1.5 Aspectos constitucionales y legales para la prevención del delito cibernético y el derecho a la intimidad en Ecuador.

1.5.1 Un nivel internacional

La privacidad, en algunas de sus variadas modalidades está definido como un derecho humano fundamental que es reconocido en los tratados internacionales. En este sentido, el artículo 12 de la Declaración Universal de Derechos Humanos de 1948, establece que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Organización de Naciones Unidas, 1948).

Como se observa, la más grande Declaración Internacional de sobre derechos humanos de los últimos dos siglos, ha sido clara y tajante en disponer la protección de todos los seres humanos contra las injerencias de terceros en su vida privada, pues la dignidad de la cual hace gala no tolera que se irrespete su derecho de intimidad.

En este mismo contexto, el Pacto Internacional de Derechos Civiles y Políticos, expone en su artículo 17:

> Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. (Organización de Naciones Unidas, 1966)

Este Pacto lo que hace es reproducir el texto de la Declaración Universal de los Derechos Humanos, obsérvese, que, en ambos textos internacionales, no sólo se protege al, sino también a su familia.

La Convención Americana sobre Derechos Humanos, conocida como Pacto de San José de Costa Rica, del año 1969, expone en su artículo 11 que:

> Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques (Organización de Naciones Unidas, 1969).

Nuevamente, este texto legal internacional reproduce el texto de la Declaración de los Derechos Humanos. Así que, a nivel internacional si ha habido la preocupación por la protección de la intimidad de los individuos como parte de la dignidad humana.

Con respecto a la privacidad en menores de 18 años, la Convención Internacional sobre los Derechos del Niño de 1989, en su artículo 16, establece que:

> 1.Nadie tiene derecho a invadir, sin una razón legal, tu privacidad, es decir, tu vida privada o tu vida familiar. Tu casa, tu correo, así como tu honor y tu reputación, constituyen tu privacidad y están igualmente protegidos. 2. El estado debe crear leyes que protejan todos los aspectos de tu privacidad (Organización de Naciones Unidas, 1989)

La Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, de 1990, que expresa en su artículo 14:

> Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques (Organización de las Naciones Unidas, 1990)

Finalmente, se cita el artículo 14 de la Declaración Internacional sobre los Datos Genéticos Humanos**,** del año 2003, el cual expresa:

> a) Los Estados deberían esforzarse por proteger la privacidad de las personas y la confidencialidad de los datos genéticos humanos asociados con una persona, una familia o, en su

> caso, un grupo identificables, de conformidad con el derecho interno compatible con el derecho internacional relativo a los derechos humanos; b) Los datos genéticos humanos, los datos proteómicos humanos y las muestras biológicas asociados con una persona identificable no deberían ser dados a conocer ni puestos a disposición de terceros, en particular de empleadores, compañías de seguros, establecimientos de enseñanza y familiares de la persona en cuestión, salvo por una razón importante de interés público en los restringidos casos previstos en el derecho interno compatible con el derecho internacional relativo a los derechos humanos o cuando se haya obtenido el consentimiento previo, libre, informado y expreso de esa persona, siempre que éste sea conforme al derecho interno y al derecho internacional relativo a los derechos humanos. Debería protegerse la privacidad de toda persona que participe en un estudio en que se utilicen datos genéticos humanos, datos proteómicos humanos o muestras biológicas, y esos datos deberían revestir carácter confidencial. c) Por regla general, los datos genéticos humanos, datos proteómicos humanos y muestras biológicas obtenidos con fines de investigación científica no deberían estar asociados con una persona identificable. Aun cuando estén disociados de la identidad de una persona, deberían adoptarse las precauciones necesarias para garantizar la seguridad de esos datos o esas muestras biológicas. d) Los datos genéticos humanos, datos proteómicos humanos y muestras biológicas obtenidos con fines de investigación médica y científica sólo podrán seguir estando asociados con una persona identificable cuando ello sea necesario para llevar a cabo la investigación, y a condición de que la privacidad de la persona y la confidencialidad de los datos o las muestras biológicas en cuestión queden protegidas con arreglo al derecho interno. e) Los datos genéticos humanos y los datos proteómicos humanos no deberían conservarse de manera tal que sea posible identificar a la persona a quien correspondan por más tiempo del necesario para cumplir los fines con los que fueron recolectados o ulteriormente tratados. (Organización de Naciones Unidas, 2003)

En efecto, los tratados y pactos internacionales propugnan la defensa de la intimidad individual, pero son los Estados los que deben hacerla una realidad siendo garantes de estos derechos legítimos de la gente, pues no puede haber interferencias en su cumplimiento, y para ello deben existir los más estrictos controles, de manera de limitar las circunstancias que pueden provocar estas injerencias malsanas, así lo expone Ben Emerson Relator especial de las Naciones Unidas, cuando indica:

> La dura verdad es que el uso de la tecnología de vigilancia masiva suprime efectivamente el derecho a la privacidad de las comunicaciones en Internet por completo (Con la vigilancia masiva), las comunicaciones de literalmente cada usuario de Internet están potencialmente abiertas para la inspección de agencias legales y de inteligencia de los Estados concernidos, los individuos tienen

> derecho a compartir información e ideas con otros sin la interferencia del Estado, con la certeza de que sus comunicaciones serán leídas sólo por sus destinatarios (Emmerson, 2014).

Esa es una confesión que dejó perplejo al mundo completo, y mucho más con las revelaciones hechas por Edward Snowden en el año 2013, sobre los programas de vigilancia global masiva, desarrollados por los servicios secretos de algunos países desarrollados como Estados Unidos, el Reino Unido, Nueva Zelanda, Australia y también Canadá.

1.5.2 Un nivel nacional

La Constitución de Ecuador expresa en su artículo 10 que "Las personas, comunidades, pueblos, nacionalidades y colectivos son titulares y gozarán de los derechos garantizados en la Constitución y en los instrumentos internacionales". (Ecuador, Asamblea Constituyente, 2008). Lo que significa, que estos grupos humanos deben ser respetados en su derecho a no tener una acción injerencista arbitraria o ilegal de nadie en su vida privada, en su familia, su hogar, correspondencia ni mucho menos, ataques contra su honor y buen nombre, porque así lo expresan tanto la Declaración Universal de Derechos Humanos, como los pactos Internacionales sociales y políticos, y demás Declaraciones internacionales.

En el artículo 11 numeral 3 de la Constitución se expresa:

> Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. Para el ejercicio de los derechos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley. Los derechos serán plenamente justiciables. No podrá alegarse falta de norma jurídica para justificar su violación o desconocimiento, para desechar la acción por esos hechos ni para negar su reconocimiento. (Ecuador, Asamblea Constituyente, 2008)

Es decir, que los ciudadanos no sólo tienen los derechos que protegen su intimidad y su vida de intromisiones ilegales, sino que, además, de acuerdo con la Constitución, estos son derechos humanos, que permanecen con la persona y son de aplicación inmediata en el mismo momento en que se vulneran.

La Constitución en su artículo 16 numeral 2 dispone como derecho de los ciudadanos, el acceso universal a las tecnologías de la información y la comunicación lo que se complementa con el artículo 18 constitucional que estipula que:

> Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información (Ecuador, Asamblea Constituyente, 2008) .

Este importante artículo constitucional da pautas claras en cuanto a la información, indicando no sólo que debe ser una información veraz, sino que, además, la persona que informa tiene una responsabilidad posterior por las cosas que informa, y cuando en derecho se habla de responsabilidad significa, responsabilidad penal, civil, administrativa o disciplinaria. O sea, que la información no puede perjudicar de ninguna manera los derechos humanos de nadie. También la Constitución dispone la publicidad de los actos, cuando ellos violen los derechos humanos y en especial, los que tienen que ver con la intimidad, la reputación y el buen nombre de las personas.

Finalmente, el artículo 19 de la Constitución expresa:

> La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos (Ecuador, Asamblea Constituyente, 2008).

Es precisamente en este artículo 19, donde está contenido el deber del Estado de controlar la información, para evitar que la población sufra los rigores de las informaciones maliciosas que perjudican su honor, su honra y su buen nombre y, además, controla los contenidos de las informaciones, en este sentido, controla el lenguaje que se utiliza, los contenidos subliminales y los aspectos vulgares y ofensivos.

En cuanto al Código Orgánico Integral Penal (COIP), este en su articulado contempla las infracciones delictivas que pueden catalogarse ya sea como delitos informáticos, electrónicos y computacionales, entre estas tipificaciones están el artículo 174, el cual establece una pena entre 7 y 10 años, para quien oferte servicios sexuales con menores de dieciocho años utilizando los medios electrónicos. (Ecuador, Asamblea Nacional, 2014)

En el artículo 178 por su parte, trata sobre el delito de la violación a la intimidad, sancionando con una pena de 1 a 3 años de pérdida de la libertad para el sujeto activo del delito y en el 186.2, se establece el delito de estafa con una pena de 5 a 7 años de prisión al sujeto activo del delito, definiendo en este caso la estafa como la que "Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares" (Ecuador, Asamblea Nacional, 2014). En este caso según el COIP se aplica la pena máxima.

En el artículo 190 del COIP se establece la pena de 1 a 3 años de privación de libertad para quienes se apoderen fraudulentamente de medios electrónicos para cometer un ataque a un bien ajeno apoderándose de él. En este sentido, el COIP expresa:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. (Ecuador, Asamblea Nacional, 2014)

El artículo 191 del COIP dispone pena de 1 a 3 años para la persona que haga reprogramación o modificación de información de equipos terminales móviles. Este artículo expresa "La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años". (Ecuador, Asamblea Nacional, 2014)

El artículo 192 del COIP trata sobre la pena de 1 a 3 años de privación de la libertad para quienes hagan intercambio, comercialización o compra de información de equipos terminales móviles, definidos éstos como aquellos destinados a ser conectados a la Red Pública de Telecomunicaciones los cuales son capaces de procesar, recibir, conmutar o transmitir señales por medio de conexiones de radio o cable, a través de un punto de conexión terminal.

El artículo 193 del COIP expresa:

> La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años. (Ecuador, Asamblea Nacional, 2014)

El artículo 194 del COIP, trata sobre la comercialización ilícita de terminales móviles, en este sentido expresa "La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años". (Ecuador, Asamblea Nacional, 2014)

El artículo 195 del COIP, prevé:

> La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles (Ecuador, Asamblea Nacional, 2014) .

Altamente interesante resulta el artículo 229 del COIP que trata sobre la revelación ilegal de base de datos, indicando que:

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (Ecuador, Asamblea Nacional, 2014) .

El artículo 230 del COIP, es particularmente importante, pues se refiere a la interceptación ilegal de datos, al estipular que:

> Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (Ecuador, Asamblea Nacional, 2014)

El artículo 231 del COIP trata de la transferencia electrónica de activo patrimonial, perjudicando a otro, al indicar que:

> La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Ecuador, Asamblea Nacional, 2014).

El artículo 232 del COIP trata sobre el ataque a la integridad de sistemas informáticos, indicando que:

> La persona que destruya dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco

> años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (Ecuador, Asamblea Nacional, 2014)

El artículo 233 del COIP se refiere a los delitos contra la información pública reservada legalmente, al momento de indicar que la persona que:

> destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad (Ecuador, Asamblea Nacional, 2014).

Finalmente, el artículo 234 del COIP expresa sobre el acceso no consentido a un sistema informático, telemático o de telecomunicaciones:

> La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Ecuador, Asamblea Nacional, 2014).

Como se observa, el COIP ha tratado de incluir en su articulado, todos los tipos y modalidades de delitos que puedan cometerse a través de la utilización de medios electrónicos, informáticos y Computacionales. El problema radica en que este articulado es muy poco conocido por la población en general, ese es uno de los graves problemas que presentan los ecuatorianos a la hora de defenderse en los órganos jurisdiccionales.

En todo caso, Edwin Pérez exfiscal general de la Nación y ex Coordinador del Subsistema de Interceptación de Comunicaciones o Datos Informáticos de la Fiscalía, consideraba en su momento que "la investigación de los ciberdelitos es compleja, debido principalmente al desconocimiento de técnicas en la investigación y la falta de coordinación interinstitucional del sector a cargo de las telecomunicaciones". (Ecuador, Fiscalia General del Estado, 2015) En general podría decirse, que el COIP ha acogido de alguna manera el fraude como lo hace el Departamento de Justicia de los Estados Unidos, quien define como fraudes cibernéticos, citado por Joel Meléndez.

> Cualquier tipo de fraude que utiliza uno o más componentes de Internet, salas de chat, correos electrónicos, grupos de discusión o sitios Web para presentar solicitudes a posibles víctimas para llevar a cabo transacciones fraudulentas o para transmitir las procedencias del fraude a instituciones financieras u otras. (Meléndez, 2018).

En cuanto a la Ley Orgánica de Protección de Datos Personales, (Ecuador, Asamblea Nacional, 2021) ésta se promulgo a raíz de los lamentables hechos ciberdelincuenciales en los que se vio envuelta toda la República del Ecuador en el año 2021, ley que fue publicada en el Registro Oficial Suplemento No. 459 del 26 de mayo de 2021, cuyo objeto es garantizar el derecho de todos los ecuatorianos a la protección de sus datos personales, lo que incluye en forma amplia, tanto el acceso como la decisión sobre la información y datos y su protección.

En el artículo 2 de esta ley se desarrolla su ámbito de aplicación en el que se dice textualmente que "se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior". (Ecuador, Asamblea Nacional, 2021)

Es altamente interesante en esta ley el artículo 7 en el cual se expone el tratamiento legítimo de datos personales que debe hacerse:

> Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas; 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal; o por orden judicial, 3) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley,4) para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento

> de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, o por un tercero legalmente habilitado; 5) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad, 6) Para tratamiento de datos personales que consten en bases de datos de acceso público; o incluso, 7) para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma (Ecuador, Asamblea Nacional, 2021).

1.5.3 El derecho a la intimidad

En el resumen de su investigación publicada en el año 2016**,** José Martínez de Pisón señalaba que:

> La intimidad es cada vez más un bien socialmente valorado en las sociedades desarrolladas. Eso ha motivado, primero, su reconocimiento como derecho fundamental, especialmente, a partir de la Declaración Universal de Derechos Humanos. En el caso del ordenamiento jurídico español, a raíz del art. 18 de la Constitución. Y, segundo, un aumento de las reclamaciones de protección del derecho ante el Tribunal Constitucional. La doctrina elaborada por la jurisprudencia constitucional española en torno al derecho a la intimidad personal y familiar es amplia e interesante (Martínez, 2016).

Interesante es saber que la configuración jurídica de la intimidad como derecho es reciente, siendo la Declaración Universal de los Derechos Humanos de 1948, la primera en reconocerlo en su artículo 12 cuando expresa:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Organización de Naciones Unidas, 1948).

Este es un derecho de primera generación en el ámbito de los derechos humanos. José Martínez de Pisón opina sobre este derecho que:

> Por parte de este conjunto de libertades fundamentales vinculadas muy estrechamente a la persona y a la concepción civil y política de la ciudadanía. No solo eso, sino que, en los últimos tiempos, debido especialmente al desarrollo tecnológico, la protección del derecho a la intimidad y al haz de derechos que lo constituyen ha adquirido una mayor relevancia social y, por tanto, jurídica, que,

> incluso, supera a otras libertades individuales tradicionalmente mucho más importantes. (Martínez, 2016)

Lo cierto que el término intimidad, ha despertado innumerables debates de todo tipo, éticos, morales, jurídicos, psicológicos, sociológicos y hasta políticos.

Pero ¿cómo se define el derecho a la intimidad? Antonio Pérez Luño, citado por José Martínez Pisón, al referirse a este derecho indica que, este es producto de una:

> Composición de la intimidad ligada a las diferentes esferas a partir de las cuales el individuo manifiesta sus intereses personales y la voluntad de estructurar su vida. Intimsphäre (esfera íntima) hace referencia a lo más secreto de la persona, a lo relacionado con sus opiniones, decisiones y acciones más íntimas. Compondría una primera esfera, el círculo más cercano al individuo. Privatsphäre (esfera privada) constituye un segundo círculo más amplio en el que el individuo sigue ejerciendo su privacidad, su vida privada, su intimidad personal y familiar y que, por ello, quiere que esté asegurada y protegida frente a terceros. Finalmente, Individualsphäre (esfera individual), el último de los círculos de la intimidad antes de la vida pública, que estaría constituido por otros aspectos vinculados a la misma, como el honor y la imagen personal, que también reflejan la personalidad del individuo. Más allá de estas esferas nos encontraríamos con la vida pública, con el ámbito de las relaciones sociales, para las cuales no cabe pedir la imposición de límites a la participación de terceros. (Pérez, 2004)

De esta cita se desprende, que para el autor Antonio Pérez, el derecho a la intimidad es complejo y encierra un manojo de situaciones que deben considerarse al definirlo, por ejemplo, la significación de la esfera íntima, la privada, y la esfera individual, cada una con sus características propias.

Para los anglosajones, el derecho a la intimidad lo denominan The Right to Privacy y lo definen como un derecho integral que ha pasado por diferentes facetas en su evolución, siendo la última de estas facetas, el que se corresponde con la sociedad del conocimiento y la información basada en las nuevas tecnologías TICs.

Lo cierto es que el derecho a la intimidad es considerado un derecho fundamental, autónomo, ampliamente protegido por el Estado, cuya raíz se hunde en la dignidad humana, centro del iusnaturalismo más puro, además del respeto a la persona, el libre desarrollo de su personalidad y en los principios y atribuciones que le corresponde a cada ser humano, con el agravante, que no

es un concepto fácil, al contrario, es de gran complejidad, y con limitaciones en relación con otros derechos jerárquicamente iguales, por el ordenamiento jurídico, así como por los intereses, valores y principios constitucionales.

En la actualidad, los esfuerzos de los Estados se hacen mayor para proteger este derecho que está siendo constreñido por los pluriofensivos riesgos de tipo jurídico-tradicional y por los actuales avances tecnológicos de la información y la comunicación, a lo que se suma el desarrollo imparable de la informática, la electrónica y la telemática.

1.6 Comparación de los fundamentos jurídicos de la prevención del delito y el derecho a la intimidad en Ecuador, Colombia, Perú, Chile y España para el año 2021.

1.6.1 Colombia

En Colombia desde el año 2009 existe la Ley 1273 o sea, Ley de Delitos Informáticos (Colombia, Congreso , 2009) según la cual además de modificar el Código Penal, crea el bien jurídico de la información y de los datos, preservándose los mismos, así como los sistemas tecnológicos de la información y la comunicación. Estos delitos a su vez se clasifican en dos: primero, “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informáticos” y segundo, “De los atentados informáticos y otras infracciones”.

En la ley antes citada se tipificaron como delitos las conductas contrarias al correcto manejo de datos personales, por lo que ni las personas naturales ni las jurídicas deben transgredir dicha ley incurriendo en algún tipo penal de los previstos, como clonación de tarjetas de crédito, vulneración y alteración de los sistemas para recibir ilegalmente transferencias electrónicas de fondos de los cajeros automáticos y, sufrir las consecuencias de sus actos que son penas que alcanzan hasta 120 meses de privación de libertad y multas que alcanzan hasta los 1500 salarios mínimos legales mensuales vigentes. Es de hacer notar aquí que, según informaciones oficiales, en el año 2007en Colombia los bancos y otras empresas fueron desfalcadas en más de 6.6 billones de pesos.

Pero en Colombia no sólo existe la ley de delitos informáticos, que tipifica los delitos de este tipo, sino que también el Código penal colombiano llamada Ley 599 del año 2000, lo hace en el artículo 269: donde se prevé el acceso abusivo a un sistema informático, penándose este delito con privación de la libertad por un tiempo de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes. Otros delitos previstos en este ámbito son: la obstaculización ilegítima de sistema informático o red de telecomunicación; la interceptación de datos informáticos, el daño

informático, uso de software malicioso, violación de datos personales, hurtos, transferencias no acordadas, entre otros.

Según los datos estadísticos oficiales, los delitos informáticos que más se cometen en Colombia son el hurto por medios informáticos y semejantes donde se produjeron en 2018, 8.817 denuncias, en segundo lugar, está el delito de violación de datos personales con 2.180 casos denunciados y, en tercer lugar, el acceso abusivo a un sistema informático con 2.005 denuncias.

1.6.2 Perú

En Perú, la Constitución del año 2021 expresa en su artículo 1 que:" La defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado" (Perú, Congreso Constituyente Democrático, 1993) . En el artículo 2, la Constitución peruana expresa que toda persona tiene derecho:

> 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. 7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. 8. A la libertad de creación intelectual, artística, técnica y científica, así como a la propiedad sobre dichas creaciones y a su producto. El Estado propicia el acceso a la cultura y fomenta su desarrollo y difusión. (Perú, Congreso Constituyente Democrático, 1993)

Es decir, que es una Constitución clara y tajante en cuanto a la estipulación de los derechos informáticos, computarizados o no, pero con las limitaciones de rigor, siendo estas, el respeto a la intimidad personal y familiar, al honor y a la buena reputación, así como a la voz y a la imagen propias.

Ahora bien, desde el año 2011 se promulgó la Ley de protección de datos personales o ley 29733, en la cual se destaca su objeto que es la protección de los datos personales a través de su tratamiento adecuado. Posteriormente, igual que en la ley ecuatoriana se hace una amplia definición de términos y se estipulan los alcances de los datos personales y sus limitaciones, así como un catálogo de derechos conexos con el de la información y la comunicación (Perú, Congreso Nacional, 2011).

Pero, también existe en Perú la ley 30096, o ley de delitos informáticos, en cuyo artículo 1 expresa el objeto de la ley que es:

> Prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal cometidos mediante la utilización de tecnologías de la información o de la comunicación con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia (Perú, Congreso Nacional, 2013).

1.6.3 Chile

La Constitución Política de Chile establece en su artículo 5, lo siguiente:

> El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes. (Chile, Congreso Nacional, 2005)

El artículo 19.4 expresa "La Constitución asegura a todas las personas el respeto y protección a la vida privada y a la honra de la persona y su familia" (Chile, Congreso Nacional, 2005), además, el artículo 19.5 indica "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley". (Chile, Congreso Nacional, 2005)

Así mismo, el artículo 19.12 expresa que:

> La libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley, la que deber ser de quórum calificado. (Chile, Congreso Nacional, 2005)

El artículo 19.4 de la Constitución preceptúa como garantía el aseguramiento a todas las personas del respeto y protección a su vida privada, a su honra y la de su familia, así como la protección de sus datos personales, así mismo dispone, que "El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley" (Chile, Congreso Nacional, 2005) .

Como se observa, la Constitución chilena igual que otras constituciones latinoamericanas, proveen los insumos suficientes, para promulgar leyes que propendan a la protección de los datos de las personas naturales y jurídicas, y es precisamente con fundamento en este último artículo constitucional que se promulgó la Ley N° 19.628 sobre protección de la vida privada, publicada en el año 1999.

1.6.4 España

El Código Penal español es el que contiene los delitos informáticos. Lo curioso es que el mismo catálogo de delitos comunes con sus respectivas sanciones, se aplica a los ciberdelitos. En este sentido, los delitos tipificados en la citada ley penal en su artículo 186 del Código Penal, del 23 de noviembre de 1995, son entre otros: la difusión, venta o exhibición de material pornográfico entre menores de edad o personas discapacitadas por cualquier medio, es castigado con pena privativa de libertad de 6 meses a un año o imposición de multa de 12 a 24 meses.

En este mismo orden, el artículo 189 del Código penal dispone que se castigará con privación de libertad de uno a cinco años a quienes utilicen o capten menores de edad o personas con discapacidad para espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para la elaboración venta y difusión de este material. (España, Congreso Nacional, 1995)

En este delito de elaboración, venta y distribución de pornografía infantil fueron encontrados culpables 40 personas y 34 de ellos eran menores.

Otro delito que aparece en el Código Penal es el relacionado con el descubrimiento y revelación de secretos, en este sentido, el Código Penal establece en su artículo 197.1 del 23 de noviembre de 1995, que:

> Aquel individuo que para descubrir los secretos o vulnerar la intimidad de otro se apropien de cualquier documentación, intercepte telecomunicaciones o utilice artilugios de grabación, escucha, transmisión o reproducción de señales será castigado con penas de prisión de entre uno a cuatro años y multa de doce a veinticuatro meses. Las mismas penas se impondrán a aquellos que se apoderen, accedan, utilicen o modifiquen datos reservados de carácter personal o familiar registrados o almacenados, sin estar autorizado. Aquellos que difundan, revelen o cedan a terceros datos o hechos descubiertos o imágenes captadas de los anteriores puntos serán castigados con penas de prisión de entre dos a cinco años. Se impondrán penas de entre 3 a 5 años y multa de 12 a 24

> meses, al que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento realice la conducta descrita en el párrafo anterior. (España, Congreso Nacional, 1995)

En cuanto a las estafas cometidas por personas que, con ánimo de lucro, utilizan el engaño logrando a través de sus artimañas, que se realicen acciones con perjuicio propio y a veces con ayuda de medios informáticos para hacerse transferencias sin consentimiento del otro.

De manera, que según el artículo 248 del Código Penal español (España, Congreso Nacional, 1995), quienes fabriquen, posean o de alguna manera faciliten programas de este tipo para la comisión de estafas y además, los que usen tarjetas de crédito o tarjetas de débito, cheques viajeros u otros datos para con artimañas cometer acciones en contra de terceros, realizar operaciones para el perjuicio del titular o un tercero, serán castigados con penas de privación de la libertad con un tiempo de seis meses a tres años, dependiendo del monto defraudado, el daño causado a la víctima, las relaciones existentes entre víctima y victimario, los medios empleados para cometer el delito y otras circunstancias agravantes, según se estipula en el artículo 249 del Código Penal.

Necesario es indicar, que el Código Penal español considera agravante de la estafa, que esta haya sido cometida con afectación a cosas de primera necesidad, o viviendas y bienes de utilidad social, delito que según el artículo 251 tienen pena de privación de libertad de 1 a 6 años además de una multa de seis a doce meses. La pena aumenta de 4 a 8 años, y multa de 12 a 24 meses, no solo si afecta a benes de primera necesidad, sino que además la estafa superes los 250.000 euros.

En este caso se subsume la conducta delictual de 45 personas que estafaron a cerca de 200 personas utilizando el internet en Málaga, que operaban desde Benín (África).

Otros delitos son la piratería contra la propiedad intelectual e industrial, el mercado y a los consumidores, lo que se sanciona con privación de libertad de seis meses a cuatro años y una multa de doce a veinticuatro meses, pero la misma tiene agravantes.

Otro delito es el espionaje Industrial con apoderamiento ya sea de datos o documentos. Este delito tiene agravantes si se difunden o revelan y más aún, si hay apoderamiento o destrucción soportes informáticos. Finalmente, está el delito de manipulación de datos, programas y documentos informáticos, en este caso se trata de que el ciberdelincuente por cualquier medio altere, destruya o dañe programas datos, y documentos en sistemas informáticos. Así mismo, son castigados quienes cometan fraudes empleando las telecomunicaciones.

Como se ve, a través del derecho comparado, todas las naciones seleccionadas tienen normas penales para castigar los delitos informáticos, computacionales o electrónicos, fundamentándose en el Código Penal y en las leyes que han promulgado para la protección de los datos, sin embargo, se observa en toda una gran debilidad en cuanto a las sanciones y a lo escasamente adelantado que está el tema legal en relación al avance desmesurado de las nuevas tecnologías, por lo que pareciera que en este caso, lo más sensato podría ser, capacitar a toda la población sobre estas situaciones producidas por los ciberdelitos que tanto daño hace tanto a personas naturales como jurídicas.

CAPÍTULO II

METODOLOGÍA

La metodología está referida al proceso del cómo se desarrolla la investigación para obtener nuevos conocimientos fiables. En este sentido, el informe de esta parte de la investigación incluye: tipo de investigación, métodos, población y muestra, e instrumentos de investigación.

2.1. Tipo de investigación

Carlos Manuel Villabella Armengol, al tratar el tema del tipo de investigación indica que:

> Cuando en la literatura especializada se habla de tipos de investigación se hace referencia a la forma que puede adoptar ésta en relación con diferentes variables. Se produce así una diversa taxonomía: documental o de campo; cuantitativa o cualitativa; exploratoria, descriptiva o explicativa; histórica, descriptiva-actual o experimental; transversal, longitudinal o transaccional; de laboratorio, de campo o bibliográfica; experimental, no experimental o cuasiexperimental; pura o aplicada, entre otras (Villabella, 2020).

En el caso de esta, se trata de una investigación mixta que utiliza tanto la investigación documental como la de campo para llegar a conclusiones precisas. En la primera se utilizan las técnicas de recolección y selección del material, subrayado, lectura rápida y lectura interpretativa, elaboración de esquemas, borradores, entre otras. En el trabajo de campo, se utilizó la encuesta para recoger la información in situ.

2.2. Métodos

Literalmente, la palabra métodos se deriva de dos raíces griegas: meta, que significa hacia y odos, que significa camino, por lo que en conjunto se traduce como el camino hacia algo, la vía hacia el cumplimiento de una meta. En este sentido, la metodología es simplemente, el procedimiento que va desarrollando el investigador para estudiar un objeto o fenómeno de su interés; es entonces, la estrategia con la cual se investiga un problema de tipo científico, adentrándose en lo desconocido con los instrumentos y técnicas para obtener un conocimiento nuevo. Dentro de los métodos que se utilizaron en esta investigación están el de análisis, síntesis, inductivo, deductivo, descriptivo, comparativo, histórico y exegético.

2.2.1. Método de análisis

Cuando se habla del análisis, simplemente se está haciendo referencia a la descomposición del objeto en partes o elementos, es decir, es una desconstrucción del objeto, en este sentido, el objeto de la presente investigación fue indagar, examinar la forma de prevenir la comisión de ciberdelitos para proteger el derecho a la intimidad en Ecuador, este gran tema, fue desglosado en partes tales como: la prevención del delito, el delito cibernético, historia de los delitos informáticos, tipos de ciberdelitos**,** el caso del hackeo de datos en Ecuador, aspectos constitucionales y legales para la prevención del delito cibernético y el derecho a la intimidad en Ecuador, el derecho a la intimidad, comparación de las legislaciones de distintos países sobre el control de los ciberdelitos.

2.2.2. Método de síntesis

La síntesis representa la recomposición o integración del discurso, es decir, que mediante ella se integra el objeto y así se obtiene una comprensión general partiendo de la de los elementos analizados previamente, destacando el sistema de relaciones existentes entre las partes analizadas y el todo. La síntesis precisamente va a indicar como se relacionaron los elementos del todo y que resultados produjo, es decir, a través de la síntesis se produce la comprensión del todo. La síntesis normalmente se ve a través de las conclusiones generales de una investigación y en esta no es la excepción.

2.2.3. Método inductivo

Este método va guiando la investigación de lo particular a lo general. En el caso de esta investigación, parte de la prevención del delito, se expande a los delitos cibernéticos a los que estudia en todas sus partes, posteriormente pasa a las normas que sustentan el tema, la comparación con otras legislaciones, hasta llegar a las conclusiones generales sobre el delito cibernético en Ecuador.

2.2.4. Método deductivo

Este método va desarrollando la investigación desde lo general hacia las particularizaciones. En el presente caso, la investigación va desde la premisa de la existencia del

delito, pasando por los delitos informáticos hasta llegar a indicar, la existencia de estos delitos en Ecuador.

2.2.5. Método descriptivo

Este método está referido a la caracterización del objeto de la investigación. En el presente tema, la caracterización del objeto la da tanto la investigación documental como la de campo.

2.2.6. Método comparativo

Este interesante método permite comparar las instituciones del derecho en diferentes aspectos. En el presente caso sirvió para comparar la legislación que protege los derechos personales, entre ellos, la intimidad, en Ecuador, Perú, Colombia, Chile y España.

2.2.7. Método histórico

Este Método de las ciencias sociales, ubica al investigador en el origen y la evolución de una institución del derecho, permite estudiar lo acontecido en el pasado con el fin de encontrar una explicación causal a las manifestaciones actuales.

En este caso, se estudió el origen y la evolución de los delitos informáticos concluyendo que estos delitos pueden rastrearse a partir de los años 60s, o sea, que ya el historial de los delitos informáticos en el mundo alcanza más de 60 años y hay países como Uruguay, que aún no cuentan con una ley de protección de datos, y un país como Ecuador, que por no haber protegido sus datos con una ley y unas políticas actualizadas, expuso los datos personales de toda su población a los hackers, lo que indica, lo atrasado del derecho en torno a los nuevos problemas que van surgiendo en la sociedad.

2.2.8. Método exegético

Se utilizó en esta investigación en el estudio de las normas que sustentan su objeto artículo por artículo, especialmente de la Constitución y el Código Orgánico Integral Penal. para descubrir el alcance de las normas, describirlas y encontrar su verdadero significado.

2.3. Población y muestra

La población de esta investigación es indeterminada, pero la muestra si estuvo constituida por 12 abogados en ejercicio y 10 ingenieros en computación. Esa muestra fue del tipo intencional dadas las circunstancias de crisis por la que atraviesa el mundo y la escasa accesibilidad a los informantes. Lo importante de la muestra, es que todos los sujetos muestrales además de ser profesionales tienen un componente de investigación por ser magister y, además, cuentan con bastante experiencia en su campo laboral.

2.4. Instrumentos y técnicas de recolección de información

Para la investigación documental se utilizaron las técnicas propias de este tipo de estudio: recolección del material especializado en el área especialmente de los delitos informáticos, selección del material de acuerdo con la necesidad del punto a tratar, elaboración de un plan para el desarrollo de los diferentes aspectos a tratar, desarrollo de cada aspecto tratado con las técnicas de lectura general y lectura interpretativa, subrayado, elaboración de esquemas, entre otros.

En el trabajo de campo, el mismo que se hizo en Quito, Ecuador, se utilizó la encuesta, la cual fue elaborada y validada por expertos, llamado expertos a dos ingenieros en computación y dos abogados, todos con maestría y años de experiencia. La encuesta constó de diez (10) preguntas de una sola alternativa de selección. Las preguntas estuvieron todas dirigidas a extraer información sobre el objeto de la investigación.

2.5. Resultados

Cuadro 1. Tiene información sobre los delitos cibernéticos

Respuesta	F	%
Si	22	100
No	0	0
Muy buena	21	94
Buena	1	6
Regular	0	0
Ninguna	0	0

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 1. Información sobre los delitos cibernéticos

Elaborado por: Héctor Guillermo Saltos Pinto

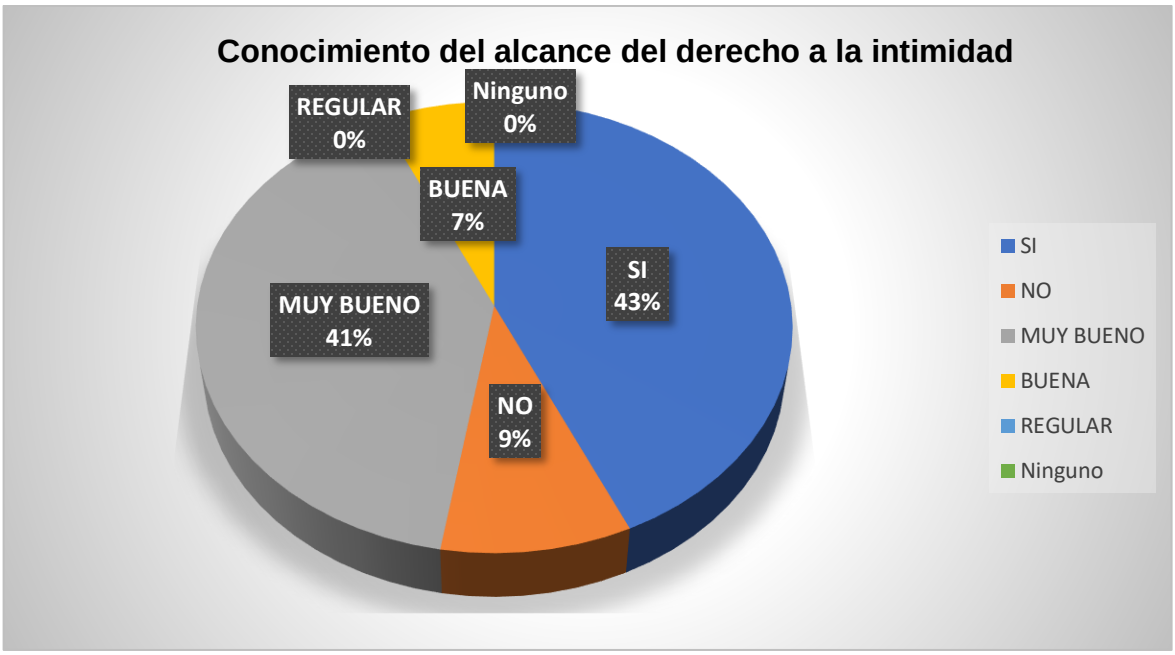
El cuadro y gráfico 1 informan que el 100% de la muestra si está informada y el 94% muy bien sobre los delitos cibernéticos o ciberdelitos, lo que significa, que la muestra es altamente calificada para responder las interrogantes de la encuesta.

Cuadro 2. Conocimiento sobre el alcance del derecho a la intimidad

Respuesta	F	%
Si	18	82
No	4	18
Muy bueno	17	77
Buena	2	13
Regular	0	0
Ninguno	0	0

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 2. Conocimiento sobre el alcance del derecho a la intimidad



Elaborado por: Héctor Guillermo Saltos Pinto

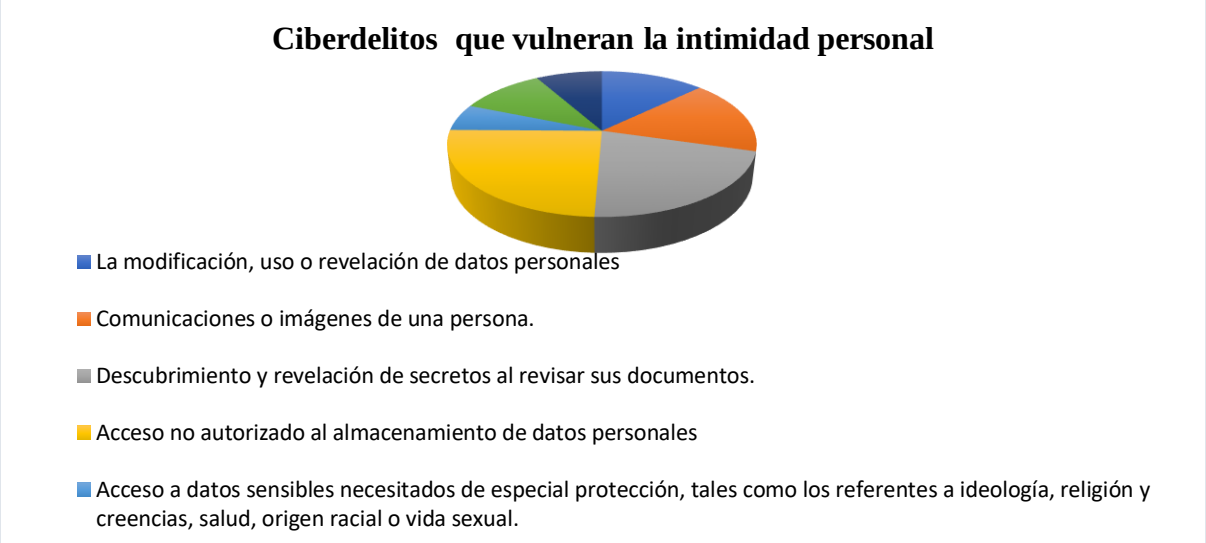
Los datos del cuadro y gráfico 2 están indicando, que la mayoría de la muestra si tiene conocimiento y muy bueno sobre el alcance del derecho a la intimidad, lo que es altamente significativo para esta investigación, porque entonces sus respuestas gozarán de validez.

Cuadro 3. Delitos cibernéticos que vulneran el derecho a la intimidad.

Respuesta	F	%
La modificación, uso o revelación de datos personales	11	50
Comunicaciones o imágenes de una persona.	14	64
Descubrimiento y revelación de secretos al revisar sus documentos.	18	82
Acceso no autorizado al almacenamiento de datos personales	21	95
Acceso a datos sensibles necesitados de especial protección, tales como los referentes a ideología, religión y creencias, salud, origen racial o vida sexual.	5	23
Difusión de grabaciones o imágenes obtenidas sin consentimiento	9	41
Otros	7	32

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 3. Delitos cibernéticos que vulneran el derecho a la intimidad



Elaborado por: Héctor Guillermo Saltos Pinto

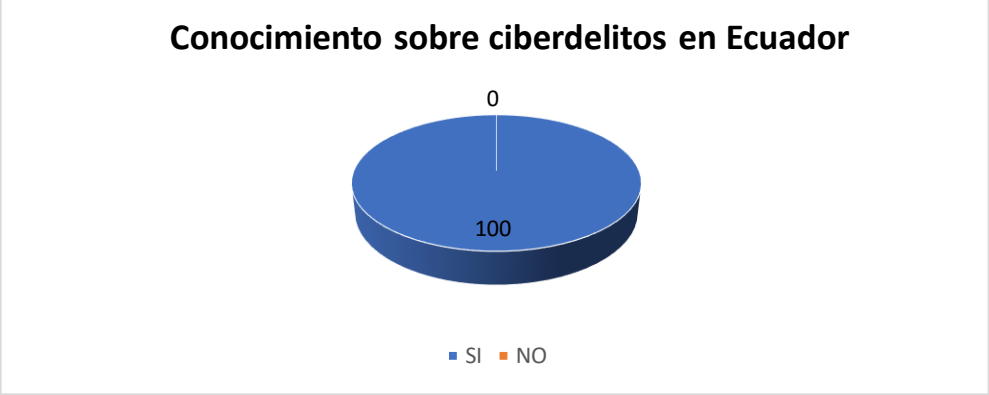
Los datos del cuadro y gráfico 3 revelan que el descubrimiento y revelación de secretos al revisar sus documentos y el acceso no autorizado al almacenamiento de datos personales, son los delitos que más se producen.

Cuadro 4. Conocimiento sobre si en Ecuador se producen delitos contra la intimidad.

Alternativa	F	%
SI	22	100
NO	0	0

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 4. Conocimiento sobre si en Ecuador se producen delitos contra la intimidad.



Elaborado por: Héctor Guillermo Saltos Pinto

En el cuadro y gráfico 4 se observa que la totalidad de la muestra opina que en Ecuador si se producen ciberdelitos contra la intimidad.

Cuadro 5. Experiencia personal en torno a algún ciberdelito contra su intimidad

Alternativa	F	%
SI	14	64
NO	8	36

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 5. Experiencia personal en torno a algún ciberdelito contra su intimidad

Elaborado por: Héctor Guillermo Saltos Pinto

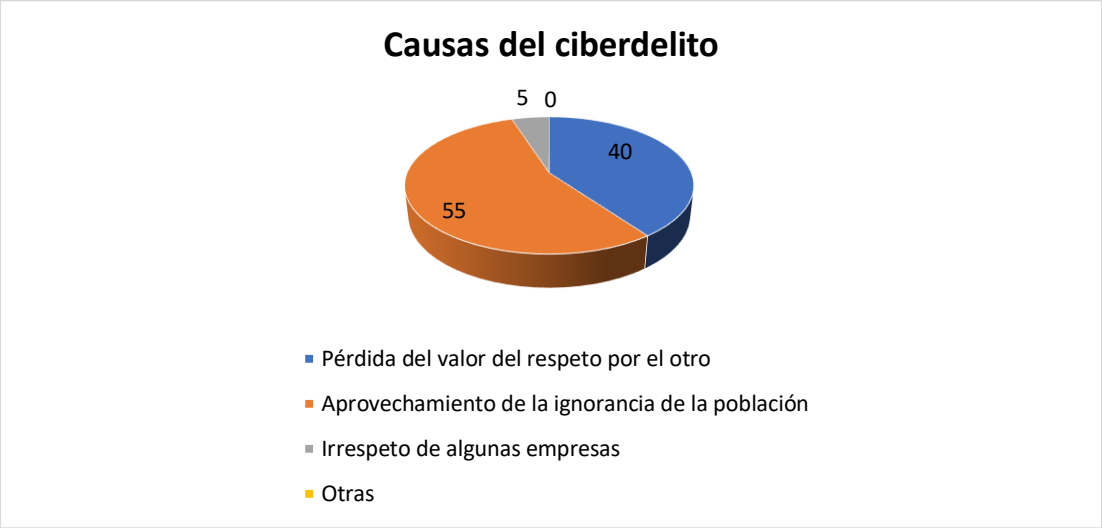
Como se observa en el cuadro y gráfico 5, la mayoría significativa del 64% de la muestra tiene experiencia personal sobre ciberdelitos en Ecuador.

Cuadro 6. Causas de los ciberdelitos contra la intimidad personal en Ecuador

Alternativas	**F**	**%**
Pérdida del valor del respeto por el otro	9	40
Aprovechamiento de la ignorancia de la población	12	55
Irrespeto de algunas empresas	1	5
Otras	0	0

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 6. Causas de los ciberdelitos contra la intimidad personal en Ecuador



Elaborado por: Héctor Guillermo Saltos Pinto

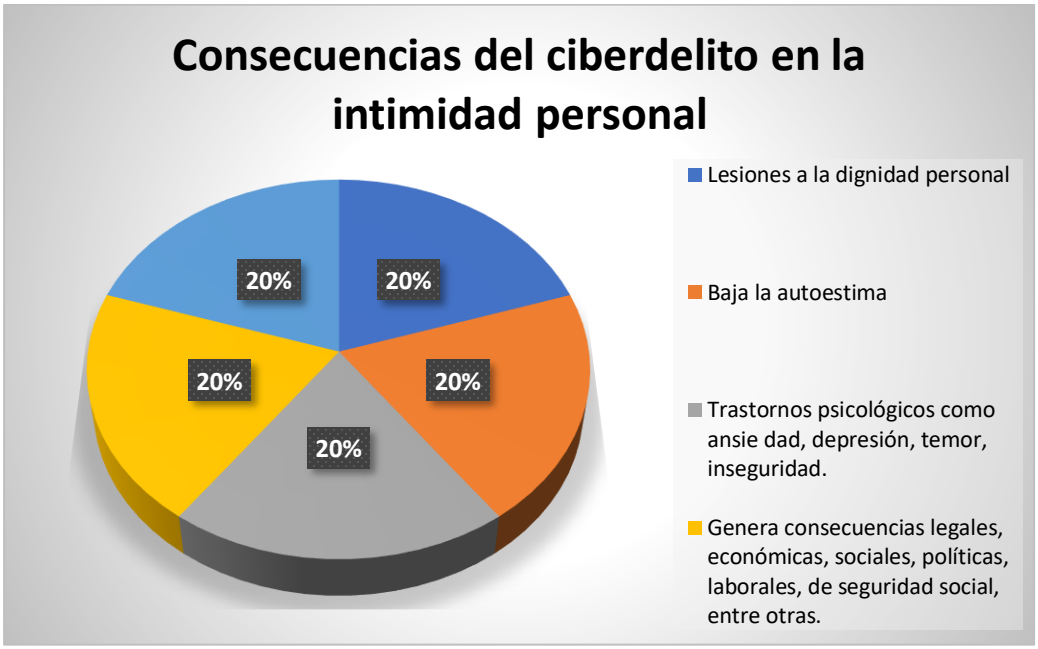
Los datos del cuadro y gráfico 6 indican que la muestra en su mayoría es de la opinión, que dentro de las causas que originan los ciberdelitos está el aprovechamiento de la ignorancia de la población, seguida por pérdida del valor del respeto por el otro.

Cuadro 7. Consecuencias del ciberdelito en su injerencia a la intimidad Personal.

Alternativas	**F**	**%**
Lesiones a la dignidad personal	22	100
Baja la autoestima	22	100
Trastornos psicológicos como ansiedad, depresión, temor, inseguridad.	22	100
Genera consecuencias legales, económicas, sociales, políticas, laborales, de seguridad social, entre otras.	22	100
Otras	22	100

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 7. Consecuencias de injerencia del ciberdelito en la intimidad Personal



Elaborado por: Héctor Guillermo Saltos Pinto

Los datos del cuadro y gráfico 7 indican que la totalidad de la muestra señalan como consecuencias del ciberdelito en la vulneración de la intimidad personal, las lesiones a la dignidad personal, la baja autoestima, trastornos psicológicos y consecuencias legales.

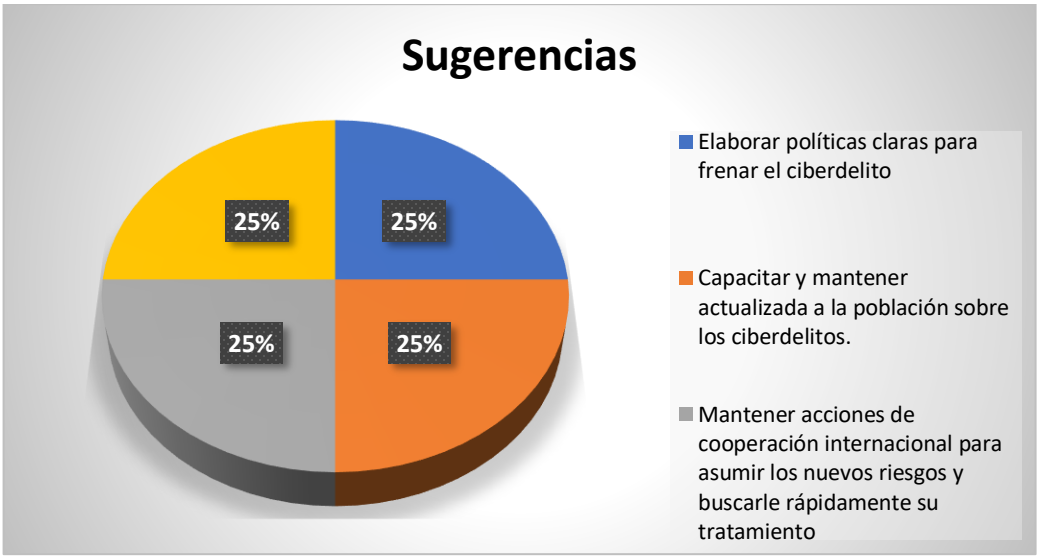
Cuadro 8. Sugerencias para frenar el ciberdelito en Ecuador

Alternativas	**F**	**%**
Elaborar políticas claras para frenar el ciberdelito.	22	100
Capacitar y mantener actualizada a la población sobre los ciberdelitos.	22	100
Mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento.	22	100

Reforzar los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.	22	100

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 8. Sugerencias para frenar el ciberdelito en Ecuador



Elaborado por: Héctor Guillermo Saltos Pinto

Los datos aportados en el cuadro y gráfico 8 indican que la muestra destacó como sugerencias para frenar el ciberdelito las siguientes: elaborar políticas claras para frenar el ciberdelito; capacitar y mantener actualizada a la población sobre los ciberdelitos; mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento; reforzar los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.

Cuadro 9. Necesidad de propuestas de los ciudadanos para frenar los problemas de los ciberdelitos contra el derecho a la intimidad personal

Alternativas	**F**	**%**
SI	20	91
NO	2	9

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 9. Necesidad de propuestas de los ciudadanos para frenar los problemas de los ciberdelitos contra el derecho a la intimidad personal

Elaborado por: Héctor Guillermo Saltos Pinto

Los datos del Cuadro y Gráfico 9 indican que una mayoría determinante de la muestra opinó que, si existe la necesidad de la elaboración de propuestas de los ciudadanos para frenar los problemas de los ciberdelitos contra el derecho a la intimidad personal, sólo un 9% considera que no son necesarias.

Cuadro 10. Una propuesta contra los ciberdelitos tendría factibilidad de ponerse en práctica

Alternativas	**F**	**%**
SI	22	100
NO	0	0

Elaborado por: Héctor Guillermo Saltos Pinto

Gráfico 10 Una propuesta contra los ciberdelitos tendría factibilidad de ponerse en práctica.

Elaborado por: Héctor Guillermo Saltos Pinto

Los datos del cuadro y gráfico 10 indican que la totalidad de la muestra se pronunció señalando que una propuesta contra los ciberdelitos tendría factibilidad de ponerse en práctica, lo que le da un insumo importante a la presente investigación.

CAPÍTULO III

3.ANÁLISIS DE RESULTADOS Y PROPUESTA

3.1. Análisis

La aplicación del instrumento a la muestra seleccionada da como resultado que la totalidad de ella si está informada muy bien sobre los delitos cibernéticos o ciberdelitos. No podía ser de otra manera, puesto que dicha muestra está integrada tanto por abogados como por profesionales del mundo de la informática y como dice Josefina Quevedo González en su tesis doctoral:

> Los ciberdelitos para su investigación y prueba exigen la adopción de especiales precauciones para evitar que se frustre la labor investigadora o se vulneren derechos fundamentales. Por ello se estudian cuestiones básicas que suscitan los ciberdelitos como la competencia para saber de los mismos, los conflictos de jurisdicción entre Estados, la cooperación internacional y los sujetos especializados en la investigación. (Quevedo, 2017).

Lo primero que destaca la autora, es la precaución que debe tenerse a la hora de investigar los ciberdelitos, para que no se dañe la investigación o lo que es más grave, que se vulneren derechos humanos. Esto lo completa la autora expresando que:

> Internet ha influido significativamente en la actividad criminal al generar nuevas formas de criminalidad y servir como instrumento para la comisión de otros delitos tradicionales. Por ello, la investigación del denominado ciberdelito exige conocer las características técnicas básicas de internet (Quevedo, 2017).

Queda claro entonces, que el ciberdelito engloba parte del mundo del derecho y las tecnologías de la información y la comunicación por lo que hoy más que nunca existe la exigencia de unirse abogados y expertos las nuevas tecnologías de la información y la comunicación para atacar el cibercrimen.

En este mismo contexto, Jorge Eliezer Ojeda y otros, han indicado que:

> Frente a esos dos fenómenos: el positivo o neutro de la globalización por la tecnología, la información y las comunicaciones, y el negativo de la ciberdelincuencia, las organizaciones y algunos gobiernos del mundo han venido tomando conciencia de la perspectiva de futuro y la amenaza subyacente, para actuar mancomunadamente y construir barreras no sólo tecnológicas,

> sino también jurídicas y sociales que permitan enfrentar con probabilidades de éxito ese gran mapa de riesgos generado por los delitos informáticos. Como consecuencia, se han diseñado, divulgado y aplicado no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad. (Ojeda, Arias, Rincón, & Daza, 2010)

Es decir, que debe existir una integración entre abogados y los ingenieros en las nuevas tecnologías de la información y comunicación para trabajan en forma conjunta los elementos preventivos de los ciberdelitos. Por esto es que no resulta extraño que la respuesta de la muestra mayoritariamente es que si están muy bien informados sobre los delitos cibernéticos o ciberdelitos.

Los datos del cuadro y gráfico 2 están indicando, que la mayoría de la muestra si tiene conocimiento y muy bueno sobre el alcance del derecho a la intimidad, lo que es altamente significativo para esta investigación, porque entonces sus respuestas gozarán de validez. Pero no solamente esto, sino que esta respuesta mayoritaria tiene encaje perfecto con los datos aportados en el cuadro y gráfico 1, pues la mayor cantidad de ciberdelitos tienen que ver con la vulneración dl derecho a la intimidad, la razón es que a través del delito contra la intimidad logran cometer otros como, por ejemplo, la defraudación y otros delitos de tipo económico.

Los datos del cuadro y gráfico 3 revelan que el descubrimiento y revelación de secretos al revisar sus documentos y el acceso no autorizado al almacenamiento de datos personales, son los delitos que más se producen. Esta información concuerda con la información que aporta un boletín de prensa de la fiscalía general del Estado que indica:

> La diligencia se efectuó para recabar elementos sobre un presunto delito de violación a la intimidad, luego de que la Institución conociera sobre la filtración de información de cerca de 20 millones de ecuatorianos, incluidos alrededor de 7 millones de menores (y personas ya fallecidas). Los datos presuntamente salieron de un servidor ubicado en Estados Unidos, que sería propiedad de la empresa Novaestrat, una consultora que provee servicios como análisis de datos y desarrollo de software. Durante el allanamiento se incautaron equipos electrónicos, computadores y dispositivos de almacenamiento, además de documentación, entre otros elementos. Fiscalía continuará practicando más diligencias que servirán para la investigación del presunto delito (Ecuador, Fiscalia General del Estado, 2019).

Este caso que consternó a todo el Estado ecuatoriano demuestra la debilidad en cuanto a la seguridad de los órganos del Estado en materia de protección de Datos, por eso para tratar de llenar el vacío se promulgó la Ley Orgánica de Protección de Datos Personales el 26 de mayo de 2021 (Ecuador, Asamblea Nacional, 2021).

En el cuadro y gráfico 4 se observa que la totalidad de la muestra opina que en Ecuador si se producen ciberdelitos contra la intimidad, esto se refuerza con la situación que se produjo en 2019 sobre el atentado que se hizo de sobre la sustracción de datos personales de toda la población ecuatoriana. Pero además se ha reportado, que en el año 2020-2021 hubo más de 600 denuncias sobre ciberdelitos de todo tipo.

En el cuadro y gráfico 5, la mayoría significativa del 64% de la muestra tiene experiencia personal sobre ciberdelitos en Ecuador, lo que es lógico pues ya antes se ha dicho, que aproximadamente 600 denuncias se hicieron entre los años 2020 y 2021, además de la grave situación que se presentó en 2019 con el ataque a los datos de todos los ecuatorianos. Sobre este particular, el equipo de comunicaciones y Escuela de Seguridad Digital afirma que:

> Durante la pandemia por Covid-19 la ciberdelincuencia se ha disparado de forma alarmante, la suplantación de identidad se da a mayor medida a través de correos electrónicos con los cuales se busca la falsificación de documentos para acceder a cuentas bancarias, obtener créditos financieros y hasta para realizar compras por internet (Equipo de comunicaciones y Escuela de Seguridad Digital, 2021).

Los datos del cuadro y gráfico 6 indican que la muestra en su mayoría es de la opinión, que dentro de las causas que originan los ciberdelitos está el aprovechamiento de la ignorancia de la población, seguida por pérdida del valor del respeto por el otro. En este sentido, Roberto Lemaitre Picado, al ser interrogado sobre la ciber sociedad costarricense respondió que uno de los principales problemas era "la falta de una cultura informática en la población" (Lemaitre, 2010).

Los datos del cuadro y gráfico 7 indican que la totalidad de la muestra señalan como consecuencias del ciberdelito en la vulneración de la intimidad personal, las lesiones a la dignidad personal, la baja autoestima, trastornos psicológicos y consecuencias legales. Para Pablo Maza las consecuencias del ciberdelito son entre otras:

> Este tipo de delitos informáticos afecta directamente a la intimidad documental y de las conversaciones o comunicaciones, de los secretos, el derecho a la propia imagen, así como los secretos de las personas jurídicas. Dentro de este grupo de delitos se encuentran: Violación del secreto de las comunicaciones; interceptación de comunicaciones personales de manera ilegal; utilización y modificación de los datos de carácter personal sin consentimiento; acceso ilegal a datos y sistemas informáticos; difusión de datos, hechos descubiertos o imágenes captadas ilícitamente, falsificación de documentos privados, falsificación de certificados y falsificación de tarjetas bancarias, daños patrimoniales y económicos (Maza, 2022)**.**

De alta utilidad es el aporte que dio la muestra, para frenar el ciberdelito, sugiriendo la elaboración de políticas claras; capacitar y mantener actualizada a la población sobre los ciberdelitos; mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento; reforzar los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.

Se logró a través de la información que dio la muestra, que realmente se justificara en esta investigación una propuesta, pues una mayoría determinante opinó que, existe la necesidad de ella para frenar los problemas de los ciberdelitos contra el derecho a la intimidad personal, así mismo indicó, que una propuesta contra los ciberdelitos tendría factibilidad de ponerse en práctica, lo que le da un insumo importante a la presente investigación.

3.2. Propuesta para la prevención del delito cibernético y el derecho a la intimidad en Ecuador

3.2.1. Presentación de la propuesta

A través de la investigación se destacó el papel del avance de la tecnología de la información y la comunicación en la presente etapa histórica de evolución de la humanidad, se vio que la misma es imparable y que el mundo ya no volverá a ser nunca el mismo de los siglos pasados.

El problema radica en que estos avances tecnológicos trajeron consigo, la inestabilidad e incertidumbre que ocasiona el delito, pues los delincuentes aprovechando los beneficios de la tecnología y el uso infinito del espacio, han creado todo tipo de delitos para hurtar, aterrorizar, satisfacer sus deseos sexuales y dañar a otros con amenazas, calumnias y todo tipo de maldades,

que pone a la víctima en condiciones precarias, pues les es difícil defenderse contra estos ataques maliciosos.

Ante esta grave situación surgen investigaciones como la presente, que tiene como propósito, hacer una propuesta para contribuir de alguna manera a frenar las consecuencias de estos delitos en la población previniéndolos a través de acciones propias de la prevención del delito. La propuesta contiene presentación, objetivos, justificación y estructura, aspectos estos que se desarrollan a continuación:

3.2.2. Objetivos de la propuesta

3.2.2.1 Objetivo general

Estructurar acciones que contribuyan a frenar las consecuencias de los ciberdelitos en el derecho a la intimidad a través de acciones propias de la prevención del delito.

3.2.2.2 Objetivos específicos

1. Justificar la propuesta
2. Explicar la factibilidad de la propuesta
3. Estructurar la propuesta con las acciones que contribuyan a frenar las consecuencias de los ciberdelitos en el derecho a la intimidad a través de acciones propias de la prevención del delito.

3.2.3 Justificación de la propuesta

Uno de los graves problemas que se tiene en Ecuador, según observa el investigador, es que, igual que en el resto de los países en vías de desarrollo, el nacimiento y desarrollo desaforado de la tecnología tomó por sorpresa a toda la estructura del Estado, quien evidentemente no estaba preparado para recibir la avalancha de transformaciones que el mundo desarrollado había iniciado y desplegado de manera arrolladora. Por eso, la Comisión Económica para América latina y el Caribe (CEPAL), reconoce que:

> Existen profundas desigualdades en el acceso a las nuevas tecnologías de la información y la comunicación (TIC) en los hogares latinoamericanos que constituyen el punto de partida". Estas desigualdades se refieren a la denominada brecha digital, la que presenta dos dimensiones. Por una

> parte, la brecha internacional donde destaca el rezago latinoamericano respecto al avance de las TIC en los países más desarrollados. Por otra parte, las desigualdades al interior de los países latinoamericanos que están asociadas a nivel de ingresos, lugar de residencia y "ciclo de vida familiar", entre otros factores. (Comisión Económica para América latina y El Caribe, 2006)

La Comisión Económica para América latina y El Caribe lo que hace es oficialmente poner al descubierto, lo que los latinoamericanos sienten: la profunda desigualdad entre los adelantos de los países del tercer mundo y estos países. Pero lo más grave es que estas brechas traen graves consecuencias, pues mientras los países desarrollados mejoran indetenidamente estas tecnologías y las ponen al servicio de la humanidad, los países con rezago en estas tecnologías apenas empiezan a explorarlas, asombrándose de sus potencialidades y descubriendo lentamente la manera de frenar sus elementos maliciosos.

En este mismo orden Ecured afirma que:

> El 60% del total de la población de los países subdesarrollados habita en zonas rurales, sin embargo, más del 80% de sus escasas líneas telefónicas están situadas en las zonas urbanas... La llamada brecha digital entre los países industrializados y los países en desarrollo es aún más amplia que las brechas que los separan en términos de otros indicadores de productividad, bienestar socioeconómico y capacidad de innovación científico-tecnológica. Lo mismo ocurre al interior de cada país, entre sectores de altos y bajos ingresos. Los países latinoamericanos en el año 2000 tenían sólo 3,5% de los usuarios de la red Internet y menos del 1% del comercio electrónico global. Tal como sucede en otros aspectos del proceso de globalización, la transformación en el ámbito de las TIC está marcada por una dinámica de injusta distribución, tanto entre países como al interior de ellos, una gran dispersión en términos de costo y cobertura de telecomunicaciones, de capacitación de los recursos humanos para hacer un uso eficaz de los mismos, así como de preparación de las estructuras estatales y empresariales para la economía digital. (EcuRed, s.f.)

Lo que queda claro es que, los pueblos de América latina despierten a las realidades que está viviendo el mundo actual, deje de quejarse y recrearse en su propias limitaciones y poniendo manos a la obra, hagan propuestas sólidas que ayuden de alguna manera a resolver los ingentes problemas que atosigan a la población, entre ellos, ser objeto de los saqueos a la intimidad producidos por quienes han tenido la oportunidad inmensa de formarse en el mundo de las

tecnologías del ciberespacio y ponen sus conocimientos al servicio del delito. De allí la importancia y vigencia de la presente propuesta.

3.2.4 Factibilidad de la propuesta

Esta propuesta tiene factibilidad social, económica, educativa y legal. La factibilidad social se la da la propia temática tratada, pues representando los ciberdelitos un problema para la sociedad, ella se interesa por su solución, pues como quedó dicho en la investigación las consecuencias que traen estos delitos en la vulneración del derecho constitucional a la intimidad son graves. Por eso, la muestra que sirvió de base a esta investigación afirmó con contundencia de los datos, que esta propuesta si tuviera factibilidad de ejecución.

La factibilidad económica de la propuesta viene dada, porque no se requieren grandes esfuerzos económicos para desarrollarla, toda vez que el Estado ecuatoriano cuenta con un presupuesto y una gran cantidad de ingenieros en los distintos campos de la información y la comunicación, que junto con el ejército de abogados jóvenes que tiene, puede enfrentar el reto de capacitar a la población en el área de los ciberdelitos.

En el ámbito educativo, la propuesta es factible, por cuanto se orienta a la capacitación de toda la población para que esté alerta contra los ciberdelitos y conozca la manera de enfrentarlos a través de la prevención.

En el ámbito legal la propuesta es factible, pues a través de la investigación se vio que existe un sustento constitucional y legal para evitar los ciberdelitos.

3.2.5 Estructura de la propuesta

La estructura de la propuesta está conformada por acciones preventivas para evitar ser objeto de ciberdelitos, en este sentido, se proponen las siguientes acciones específicas:

3.2.5.1 Del ciudadano

1. No abrir los emails ni WhatsApp de empresas o personas que no son de confianza plena.
2. Desconfiar de los mensajes e e'mails donde indican que hay grabaciones personales donde están ejecutando actos sexuales comprometedores, así mismo, que tienen en sus manos

conversaciones íntimas, porque eso es para desestabilizar a la persona y que entregue sumas de dinero para que borren esas situaciones.

3. Desconfía de los mensajes de WhatsApp o correos donde se indica que tus cuentas de cualquier tipo han sido desactivadas y menos que tengan que ver con internet donde existen los datos de las tarjetas de crédito. En este caso también hay que fijarse, si los destinatarios son muchos o Ud. solo.

4. No deben entregarse los datos personales especialmente de las cuentas a nadie y mucho menos, las claves, por más de confianza que sea.

5. Cuando se tiene duda sobre un remitente, hay que preguntarles a personas más expertas en el manejo de estas situaciones.

6. Hay que estar pendiente si la batería del teléfono dura menos o se recalienta mucho, porque pueden haber insertado un virus.

7. Si hay un comportamiento extraño cuando se usa internet, por ejemplo, con el Google Chrome y aparecen visitas en páginas web desconocidas, que incluso son pagadas o relacionados con criptomonedas, no se deben abrir porque has sido atacado por el virus denominado phishing.

8. Si se es objeto de publicidad nueva constante, estás siendo atacado de phishing.

9. Si hay aplicaciones de uso normal que muestran fallas, se cierran las sesiones del usuario, podrías tener un virus en el teléfono o la computadora.

10. Si aparecen aplicaciones que nunca se han descargado hay que eliminarlas inmediatamente.

11. Si aparecen facturas con exceso de consumo que el verdadero usuario no ha consumido, puedes tener un virus ladrón, por lo que se debe ir inmediatamente a la administración de ese servicio, para constatar que está pasando, porque posiblemente, se estén consumiendo datos del teléfono llamando o mensajeando a servicios de pago.

12. Si existen recalentamientos en el teléfono o computadora y se ralentiza, sin tener exceso de datos en los mismos, es porque tienes un virus.

13. Se hace necesario cambiar los teléfonos y demás dispositivos, por lo menos cada cinco años.

14. Si la persona es acosada por Internet, redes sociales, correos electrónicos o videojuegos, hay que pedir ayuda de inmediato para que te ayuden a debatir la situación y tomar decisiones y si sientes que el usuario está accediendo a tus datos personales o sensibles, a través del control de tus dispositivos u otra situación extraña, de inmediato hay que denunciarlo a la policía.

15. Si algo de lo expuesto anteriormente ocurre, se debe de inmediato proceder a poner el antivirus, restaurar a los valores de fábrica el dispositivo y formatear la computadora.

16. Hay que cambiar contraseñas de manera permanente.

17. Hay que configurar la privacidad y seguridad de nuestros propios perfiles en: las tarjetas de crédito, los bancos, plataformas de compra en línea y en las redes sociales.

18. Revisar la política de privacidad, seguridad y las condiciones del servicio al que queremos acceder.

19. Las personas deben asegurarse de que el sitio donde realizan transacciones y compras por internet es absolutamente seguro. Para comprobar esto, se debe revisar que la URL contenga una "s" después de http, por ejemplo, https://... , lo que significa que es un sitio de verdad seguro.

20. Utilizar sólo contraseñas fuertes, con longitud mayor a los diez (10) dígitos, con caracteres especiales.

21. No estar publicando datos en forma abierta, especialmente, en redes sociales: Facebook, Twitter, YouTube, entre otras.

22. Utilizar siempre el doble factor de autenticación en cualquiera de las plataformas que así lo requieran o lo permitan, por ejemplo, utilizar contraseña con un SMS

23. Mantener el software actualizado, además de instalar los parches de seguridad recomendados por el fabricante.

24. Utilizar un firewall para que se pueda garantizar la conexión segura a Internet, que es un programa informático destinado a controlar el acceso de la computadora a la red y a sus elementos peligrosos.

25. Cerrar la sesión en las cuentas cuando se finaliza su uso. Si el ordenador es personal no es necesario tomar esta precaución, sino cuando se presuma sepa que sus datos personales están inseguros.

26. No se deben realizar transacciones de tipo económico utilizando redes públicas, tales como el wifi, porque es seguro que los hackers podrán acceder a sus datos personales y lo que más les interesa, que son sus datos bancarios. En este caso se deben utilizar especialmente servidores VPN, de redes privadas o páginas *https.*

27. Se deben realizar copias de seguridad de la información más importante periódicamente (se recomienda por lo menos una vez a la semana).

3.2.5.2 El Estado:

1. Elaborar políticas claras para frenar el ciberdelito.
2. Capacitar y mantener actualizada a la población sobre los ciberdelitos.
3. Mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento.
4. Reforzar los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.

CONCLUSIONES

Luego de aplicar los métodos y técnicas de investigación se llegó a las siguientes conclusiones:

Los fundamentos jurídicos que tiene la prevención del delito y el derecho a la intimidad en Ecuador se consiguen en los instrumentos internacionales tales como la Declaración Universal de los derechos humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, conocida como Pacto de San José, la Convención Internacional sobre los Derechos del Niño de 1989, la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, de 1990 y la Declaración Internacional sobre los Datos Genéticos Humanos, del año 2003.

En el ámbito interno la protección la dan la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, la Ley Orgánica del Sistema Nacional de datos Públicos y la Ley Orgánica de Protección de Datos Personales, entre otros.

En el diagnóstico hecho a través de la aplicación de la encuesta en el trabajo de campo resultó, que 100% de la muestra si está informada y el 94% muy bien sobre los delitos cibernéticos o ciberdelitos, y además, tiene conocimiento y muy bueno sobre el alcance del derecho a la intimidad, lo que es altamente significativo para esta investigación, porque entonces sus respuestas gozarán de validez lo que significa, que la muestra fue altamente calificada para responder las interrogantes de la encuesta.

En lo sustantivo, el estudio de campo reveló que el descubrimiento y revelación de secretos al revisar sus documentos y el acceso no autorizado al almacenamiento de datos personales, son los delitos que más se producen, , la mayoría significativa del 64% de la muestra tiene experiencia personal sobre ciberdelitos en Ecuador, según ellos, las causas de estos ciberdelitos son entre otros: La modificación, uso o revelación de datos personales; comunicaciones o imágenes de una persona**,** Descubrimiento y revelación de secretos al revisar sus documentos**,** Acceso no autorizado al almacenamiento de datos personales, Acceso a datos sensibles necesitados de especial protección, tales como los referentes a ideología, religión y creencias, salud, origen racial o vida sexual y Difusión de grabaciones o imágenes obtenidas sin consentimiento, entre otros.

Se descubrió así mismo, que las causas que provocan los ciberdelitos contra el derecho a la intimidad personal son entre otras: la pérdida del valor respeto por el semejante, el irrespeto de algunas empresas y el aprovechamiento de la ignorancia de las personas.

En cuanto a las consecuencias son entre otras: lesiones a la dignidad personal, la baja autoestima, trastornos psicológicos y consecuencias legales y para frenar esta grave situación sugirió: elaborar políticas claras para frenar el ciberdelito; capacitar y mantener actualizada a la población sobre los ciberdelitos; mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento; reforzar los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.

Estas conclusiones dieron origen a la propuesta que se describió antes.

La comparación de los fundamentos jurídicos de la prevención del delito y el derecho a la intimidad en Ecuador, Colombia, Perú, Chile y España para el año 2021, arrojó que todos estos países tienen como fundamento legal para atacar los ciberdelitos desde hace bastante tiempo, la Constitución, los Códigos Penales y otras leyes específicas sobre la protección de la ciudadanía. El último país en promulgar una ley específica de Protección de datos personales fue Ecuador, pues en Colombia desde el año 2009 existe una ley contra los delitos informáticos, en Perú desde el año 2011, en Chile en estos momentos hay un movimiento de cambio de la Constitución, lo que provocará seguramente un nuevo legajo de leyes, entre esas la que proteja contra los delitos informáticos y en España, el Código Penal es bastante específico en cuanto a las penas para este tipo de delitos.

RECOMENDACIONES

Como producto de las conclusiones se sugiere:

Al Ministerio del Interior y Justicia del Ecuador conjuntamente con el Ministerio de Inclusión Social y el Ministerio de Educación del Ecuador.

1. Capacitar y mantener actualizada a la población sobre los ciberdelitos con urgencia a través de los órganos de policía, las Fuerzas Armadas, la Fiscalía General del Estado, el Ministerio de educación, las Universidades e Institutos Superiores Politécnicos, los medios de comunicación social, las redes sociales, entre otros.

Al Ejecutivo Nacional

1. Elaborar políticas claras de prevención para frenar el ciberdelito
2. Mantener acciones de cooperación internacional para asumir los nuevos riesgos y buscarle rápidamente su tratamiento.
3. Poner en práctica la propuesta que se hace en esta investigación al momento de capacitar a la población.

Al Ministerio de Educación del Ecuador

1. Reforzar a través de sus programas, los valores especialmente el del respeto en los estudiantes de los distintos niveles educativos.

A las Universidades

1. Instruir a sus estudiantes para que eviten los ciberdelitos poniendo en práctica las sugerencias dadas en la estructura de la propuesta de esta investigación.
2. Contribuir a través de la actividad de vinculación en la capacitación de la población para evitar los ciberdelitos.

BIBLIOGRAFÍA

Abril, L. (29 de 7 de 2021). Ecuador está entre los países con más ciberataques en América Latina. *El Comercio*. Recuperado el 3 de diciembre de 2021, de https://www.elcomercio.com/tendencias/ecuador-ciberataques-america-latina-hacker.html

Abushihab, A. (2016). *Cibercrimen: Una aproximación a la delincuencia informática.* Recuperado el 8 de enero de 2022, de Santo Tomás University: https://repository.usta.edu.co/bitstream/handle/11634/1995/Abushihabamir2016.pdf?sequence=1&isAllowed=y

Alarcón, D., & Barrera, J. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede seccional Sogamoso, 2016.* Recuperado el 8 de enero de 2022, de Universidad Norbert Wiener: http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20-%20%20Barrera%20Bar%c3%b3n%2c%20Javier%20Antonio.pdf?sequence=1&isAllowed=y

Álvarez, F. (2015). *La prevención Situacional del delito.* Madrid: Universidad Nacional de Educación a Distancia.

Chas, G. (6 de octubre de 2021). *El gran desafío de la Justicia es combatir al cibercrimen.* Recuperado el 25 de marzo de 2022, de https://www.nortecorrientes.com/172084-segun-guillermo-chas--el-gran-desafio-de-la-justicia-es-combatir-al-cibercrimen

Chicharro, A. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *Revista de Internet, Derecho y Política*(9), 1-14. Recuperado el 20 de marzo de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=3101795

Chile, Congreso Nacional. (2005). *Constitución Política de Chile.* Santiago de Chile: Decreto Supremo Número 100 del 17 de septiembre de 2005.

Chile, Ministerio del Interior y Seguridad Pública. (s.f.). *Preguntas y respuestas frecuentes*. Recuperado el 20 de mayo de 2022, de https://www.csirt.gob.cl/preguntas-y-respuestas-frecuentes/

Colombia, Congreso . (5 de enero de 2009). *Ley de delitos Informáticos. Ley 1273*. Recuperado el 24 de abril de 2022, de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Comisión Económica para América latina y El Caribe. (diciembre de 2006). *Las tecnologías de la información y la comunicación (TIC) en educación en América Latina: una exploración de indicadores*. Recuperado el 11 de abril de 2022, de cepal: https://www.cepal.org/es/publicaciones/6133-tecnologias-la-informacion-la-comunicacion-tic-educacion-america-latina

Cusson, M. (2005). *La Criminologie.* Paris: Hachette.

Dammert, L., & Lunecke, A. (2004). *La prevención del Delito en Chile. Una visión desde la comunidad.* Santiago de Chile: Cesc.

Dijk, V. (1989). *Crime Prevention Policy: Current State and Prospect.* Estados Unidos: U.S. Department of Justice.

Ecuador, Asamblea Constituyente. (2008). *Constitución de la República de Ecuador.* Quito: Registro Oficial 449 de 20-oct-2008.

Ecuador, Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial N° 180 del 10 de febrero de 2014.

Ecuador, Asamblea Nacional. (2021). *Ley Organica para la protección de Datos personales.* Quito: Suplemento del Registro Oficial No.459 del 26 de Mayo 2021.

Ecuador, Fiscalia General del Estado. (2015). *¡Tenga cuidado!, con un solo 'clic' podría caer en la red de los delitos informáticos*. Recuperado el 20 de mayo de 2022, de https://www.fiscalia.gob.ec/tenga-cuidado-con-un-solo-clic-podria-caer-en-la-red-de-los-delitos-informaticos/

Ecuador, Fiscalia General del Estado. (2019). *Fiscalía lidera operativo por presunta violación a la intimidad.* Ecuador: Boletín de prensa de la Fiscalía General del Estado Nº 381-DC-2019.

Ecuador, Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *Acuerdo Ministerial No. 012-2019.* Quito: Registro Oficial No.18 de 15 de agosto de 2019.

Ecuador, Ministerio del Interior. (2019). *Plan Nacional de seguridad ciudadana y Convivencia pacífica 2019-2030.* Recuperado el 19 de 03 de 2022, de https://www.ministeriodegobierno.gob.ec/wp-content/uploads/2019/08/PLAN-NACIONAL-DE-SEGURIDAD-CIUDADANA-Y-CONVIVENCIA-SOCIAL-PACI%CC%81FICA-2019-2030-1_compressed.pdf

EcuRed. (s.f.). *Impacto de las tecnologías en los países del Tercer Mundo*. Recuperado el 12 de Abril de 2022, de https://www.ecured.cu/Impacto_de_las_tecnolog%C3%ADas_en_los_pa%C3%ADses_del_Tercer_Mundo#Paradojas_en_la_era_de_la_informaci.C3.B3n

Emmerson, B. (26 de mayo de 2014). *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo – Misión a Chile.* Recuperado el 20 de mayo de 2022, de Naciones Unidas Derechos Humanos: https://acnudh.org/informe-del-relator-especial-sobre-la-promocion-y-proteccion-de-los-derechos-humanos-y-las-libertades-fundamentales-en-la-lucha-contra-el-terrorismo/

Equipo de comunicaciones y Escuela de Seguridad Digital. (11 de 10 de 2021). *¿Qué es una suplantación de identidad digital y cómo puede afectarte?* Obtenido de Uso estrategico de

internet para el desarrollo: https://colnodo.apc.org/es/experiencias/que-es-una-suplantacion-de-identidad-digital-y-como-puede-afectarte

España, Congreso Nacional. (1995). *Código Penal* . Madrid: Boletín Oficial del Estado (BOE), N° 281, del 24 de noviembre de 1995.

González, J. (29 de Mayo de 2017). *El derecho a la intimidad en la sociedad de la información: el caso de Mario Eduardo Guaigua Coque contra el Diario El Veci*. Recuperado el 3 de diciembre de 2021, de Dialoguemos: https://dialoguemos.ec/2017/05/el-derecho-a-la-intimidad-en-la-sociedad-de-la-informacion-el-caso-de-mario-eduardo-guaigua-coque-contra-el-diario-el-veci/#:~:text=Lamentablemente%20las%20leyes%20no%20se,de%20identidades%20virtuales%2C%20la%20continua

Herrero, C. (1997). *Criminología parte general y especial.* Madrid: Dykinson.

Larios, J., & Sánchez, R. (2014). *Ciberdelito.* Recuperado el 3 de diciembre de 2021, de Universidad Nacional Autónoma de México: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/4884/Tesis.pdf?sequence=2&isAllowed=y

Lemaitre, R. (3 de agosto de 2010). *La impunidad de los delitos informáticos en la ciber sociedad costarricence en el ámbito del derecho penal.* Recuperado el 11 de abril de 2022, de Universidad de Costa Rica: https://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/La-Impunidad-de-los-Delitos-Inform%C3%A1ticos-en-la-Ciber-sociedad-Costarricense.pdf

Martínez, J. (2016). *El derecho a la intimidad:de la configuración inicial a los últimos desarrollosen la jurisprudencia constitucional.* Recuperado el 24 de abril de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=5712518

Maza, P. (23 de febrero de 2022). *Consecuencias delitos informáticos*. Recuperado el 12 de abril de 2022, de Pablo:Maza: https://pablomazaabogado.es/penal-tecnologico/consecuencias-delitos-informaticos/

Meléndez, J. (25 de Julio de 2018). *Delito indormáticos o ciberdelitos.* Recuperado el 14 de abril de 2022, de DerechoEcuador: https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/

México, Senado de la República. (14 de agosto de 2015). *Dictámenes a Discusión y Votación.* Recuperado el 22 de marzo de 2022, de Gaceta Parlamentaria: https://www.senado.gob.mx/64/gaceta_comision_permanente/documento/56910

Ochoa, A. (2021). *Desafios globales del cibercrimen. Caso Ecuador. Período 2014-2019.* Recuperado el 8 de enero de 2022, de Universidad Andina Simón Bolivar: https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Oficina de las Naciones Unidas conre la Droga y el Delito. (junio de 2019). *Ciberespionaje*. Recuperado el 20 de abril de 2022, de Serie de Módulos Universitarios: Delitos Cibernéticos: https://www.unodc.org/e4j/es/cybercrime/module-14/key-issues/cyberespionage.html

Oficina de las Naciones Unidas contra la droga y el Delito. (2013). *El uso de internet con fines terroristas.* Recuperado el 3 de diciembre de 2021, de https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Ojeda, J., Arias, M., Rincón, F., & Daza, L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Bogotá: Cuadernos de Contabilidad.

Organización de las Naciones Unidas. (1990). *La Convención internacional sobre los trabajadores migratorios y sus familiares.* Suiza: Naciones Unidas.

Organización de Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos.* París: Naciones Unidas.

Organización de Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos.* Washington: Ediciones Legales.

Organización de Naciones Unidas. (7 de noviembre de 1969). *Convención Americana sobre Derechos Humanos (Pacto de San José)*. Recuperado el 20 de mayo de 2022, de https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Organización de Naciones Unidas. (1989). *Convención sobre los derechos del niño.* París: Unicef.

Organización de Naciones Unidas. (2003). *Declaración internacional sobre los datos genéticos humanos*. Recuperado el 20 de mayo de 2022, de Organización Mundial de la Salud: https://salud.gob.ar/dels/entradas/declaracion-internacional-sobre-los-datos-geneticos-humanos-unesco-2003#:~:text=Declaraci%C3%B3n%20internacional%20sobre%20los%20datos%20gen%C3%A9ticos%20humanos%2C%20UNESCO%202003,-Penchaszadeh%2C%20V%C3%ADctor%20B&text

Pérez, A. (2004). *Los Derechos Fundamentales.* Madrid: Tecnos.

Perú, Congreso Constituyente Democrático. (26 de Diciembre de 1993). *Constitución de la República del Perú.* Recuperado el 20 de abril de 2022, de https://www.congreso.gob.pe/Docs/constitucion/constitucion/Constitucion-Febrero2022.pdf

Perú, Congreso Nacional. (2011). *Ley proteccion datos personales.* Recuperado el 20 de abril de 2022, de Diaria Oficial del Bicentenario. El Peruano: https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Perú, Congreso Nacional. (2013). *Ley de delitos informáticos.* Lima: El Peruano.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO - Revista Latinoamericana de Estudios de Seguridad,* https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/2108.

Pons, V. (2018). *Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa nacional e internacional.* Recuperado el 3 de diciembre de 2021, de Universidad Nacional de Educación a Distancia: http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf

Quevedo, J. (2017). *Investigación y prueba del ciberdelito.* Barcelona: Universidad de Barcelona.

Riascos, L. (2007). *El derecho a la intimidad, la visión iusinformática y el delito de los datos personales.* Recuperado el 8 de enero de 2022, de Universidad de Lleida: https://www.tesisenred.net/handle/10803/8137?locale-attribute=es#page=1

Rodríguez, C. (Noviembre de 2018). *Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos legales.* Recuperado el 10 de enero de 2022, de Universidad Internacional SEK: https://repositorio.uisek.edu.ec/bitstream/123456789/3220/1/CAROL%20DE%20LAS%20MERCEDES%20RODR%c3%8dGUEZ.pdf

Rodríguez, L. (1997). *Criminología.* México: Porrua.

Ruíz, E. (1996). Responsabilidad penal en materia de informática. *Iboamericana de derecho informático, 1*, 443-460. Recuperado el 25 de marzo de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=248765

Saab, M., & Vinces, D. (10 de Febrero de 2020). *Análisis Jurídico del Derecho a la Intimidad.* Recuperado el 11 de enero de 2022, de Universidad Católica Santiago de Guayaquil: http://repositorio.ucsg.edu.ec/bitstream/3317/14534/1/T-UCSG-PRE-JUR-DER-518.pdf

Saín, G. (2012). *Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet* . Buenos Aires: Del puerto.

Saín, G. (11 de abril de 2015). *Pensamiento penal.* Recuperado el 2 de mayo de 2022, de Evolución histórica de los delitos informáticos: https://www.pensamientopenal.com.ar/doctrina/40877-evolucion-historica-delitos-informaticos

Salvatierra, L., & Cedeño, M. (2019). Medidas de prevención socialpresentes en el sector Los Cerezos de la parroquia Andrés de Vera del cantón Portoviejo. *ReHuSo: Revista de Ciencias Humanísticas y Sociales, 4*(3), 1-12. Recuperado el 3 de diciembre de 2021, de https://dialnet.unirioja.es/servlet/articulo?codigo=7047175

Sandoval, E. (s.f.). Ingenieria Social: Corrompiendo la mente humana. *Seguridad. Cultura de prevención para ti.*(10), https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana. Recuperado el 16 de abril de 2022, de Seguridad

Cultira de prevención para ti: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Serrano, A. (2009). *Oportunidad y delito.* Madrid: Dykinson.

Subijana, I. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore*, 169-187. Recuperado el 2 de mayo de 2022, de https://addi.ehu.es/handle/10810/24999

Torrente, D. (enero de 1999). *Prevención del delito y futuro de la Policía.* Recuperado el 12 de enero de 2022, de Universidad de Barcelona: https://reis.cis.es/REIS/PDF/REIS_085_071208156700477.pdf

Trávez, N. (2018). *La vulneración de los Derechos Constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación".* Recuperado el enero de 10 de 2022, de Universidad Central del Ecuador: http://www.dspace.uce.edu.ec/bitstream/25000/18733/1/T-UCE-0013-JUR-185.pdf

Vanderschueren, F. (2006.). *Modelos democráticos de seguridad ciudadana.* Santiago de Chile: Pnud.

Vásquez, C. (2012). *Combate a la delincuencia Cibernética.* México: Universidad de Xalapa.

Villabella, C. (2020). *Los Métodos en la investigación jurídica. Algunas precisiones.* México: Universidad Nacional Autónoma de México.