Universidad Nacional de Loja.

Facultad Jurídica, Social y Administrativa.

Carrera de Derecho.

“Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”.

Trabajo de Integración Curricular previo a la Obtención del Título de Abogada.

AUTORA:

Lizbeth Sofía Palacios Orellana.

DIRECTOR:

Dr. Rolando Johnatan Macas Saritama. Ph. D.

Loja - Ecuador

2023

Certificación

Loja, 16 de agosto de 2023.

Dr. Rolando Johnatan Macas Saritama. PhD.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR.

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **“Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”,** previo a la obtención del título de **Abogada**, de la autoría de la estudiante **Lizbeth Sofía Palacios Orellana**, con **cédula de ciudadanía** número **1104819485,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Firmado electrónicamente por:
ROLANDO JOHNATAN MACAS SARITAMA

Dr. Rolando Johnatan Macas Saritama. Ph.D.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR.

Autoría.

Yo, **Lizbeth Sofía Palacios Orellana,** declaro ser la autora del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Integración Curricular en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Cédula de Ciudadanía: 1104819485

Fecha: Loja, 29 de noviembre de 2023.

Correo Electrónico: lizbeth.s.palacios@unl.edu.ec

Teléfono: 0991409834

Carta de autorización por parte de la autora, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Integración Curricular.

Yo, **Lizbeth Sofía Palacios Orellana**, declaro ser la autora del Trabajo de Integración Curricular denominado: **"Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos"**, como requisito para optar al título de **Abogada**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintinueve días del mes de noviembre de dos mil veintitrés.

Firma:

Autora: Lizbeth Sofía Palacios Orellana.

Cédula de Ciudadanía: 1104819485

Dirección: Ramón Pinto y 10 de Agosto.

Correo Electrónico: lizbeth.s.palacios@unl.edu.ec

Teléfono: 0991409834

DATOS COMPLEMENTARIOS.

Director de Trabajo de Integración Curricular: Dr. Rolando Johnatan Macas Saritama. Ph.D.

Dedicatoria.

Dedico la culminación del presente Trabajo de Integración Curricular y la terminación de toda mi carrera universitaria de Derecho, en primer lugar a Dios, por guiarme en cada momento de mi vida, logrando con mucho esfuerzo, perseverancia y responsabilidad cumplir este objetivo tan anhelado que es mi formación profesional.

A mi madre, Dra. Ana Lucía Orellana Ramón, porque es la persona que me motiva a ser una mujer ejemplar, ética y justa. Por constituir mi apoyo fundamental e impulsarme a alcanzar mis metas sin importar los obstáculos que se puedan presentar en la vida.

De la misma manera, a mi Abuela María Licenia Ramón Pineda, por brindarme su sabiduría, cariño y comprensión, llenando mi vida de mucha felicidad.

Con mucho cariño para ustedes.

Lizbeth Sofía Palacios Orellana.

Agradecimiento.

Al culminar el presente Trabajo de Integración Curricular, expreso mi inmensa gratitud y agradecimiento a la Universidad Nacional de Loja, a cada uno de los docentes universitarios que impartieron sus conocimientos teóricos, prácticos y de valores, los mismos que han sido fundamentales para mi formación académica y personal.

Expreso mis sinceros agradecimientos a mi Director de Trabajo de Integración Curricular, el Dr. Rolando Johnatan Macas Saritama. Ph. D, por su asesoría en el proceso de elaboración de esta investigación, quien dirigió con sabiduría, dedicación y profesionalismo, aportando con sus conocimientos a la correcta realización del mismo.

De la misma manera, extiendo mi agradecimiento a todas las personas que emitieron su opinión en las encuestas y entrevistas realizadas para obtener información precisa sobre este tema de investigación.

Agradezco a todos mis amigos y familiares que me brindaron su apoyo para la realización de este Trabajo de Integración Curricular, a cada docente de la Carrera de Derecho que colaboró con sus criterios y conocimientos para la elaboración de esta investigación.

Lizbeth Sofía Palacios Orellana.

Índice de Contenidos.

Índice de Tablas.

Índice de Figuras.

Índice de Anexos.

1. Título.

“Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”.

2. Resumen.

El presente Trabajo de Integración Curricular se titula “Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”.

En esta investigación, se evidencia que el aumento de los delitos informáticos es ocasionado por la dependencia digital de la sociedad, la creciente sofisticación de la tecnología y su uso generalizado, donde los delincuentes informáticos, a través de ciberamenazas y ciberataques cometen el acto delictivo, vulnerando los derechos de las personas involucradas.

El crecimiento exponencial de estos delitos, es también ocasionado por la poca información, la falta de concientización y prevención en el uso de los medios electrónicos por parte del Estado, por tal razón es necesario y urgente que exista una mayor educación y difusión por parte del mismo, para propiciar una cultura de ciberseguridad en la población ecuatoriana.

En el presente Trabajo de Integración Curricular se aplicaron materiales y métodos que permitieron el desarrollo del mismo, para ello se realizaron encuestas y entrevistas a profesionales del Derecho, cuyos resultados sirvieron para la elaboración de lineamientos propositivos, con la finalidad de garantizar los derechos de las personas que utilizan los dispositivos electrónicos para realizar múltiples actividades diarias, fomentando de esta manera la confianza digital en la población ecuatoriana. Así mismo, se pretende ayudar a que el alto índice de los delitos informáticos disminuya con la información y difusión de la Política y Estrategia Nacional de Ciberseguridad del Ecuador, donde se plantea prevenir el avance de este tipo de delitos cibernéticos existentes en el ciberespacio.

2.1. Abstract.

The present Curricular Integration Work is titled "Comparative Study of National Cybersecurity Strategies and Policies to prevent cyber threats and cyber-attacks leading to cybercrimes."

In this research, it is evident that the increase in Cybercrimes is caused by society's digital dependence, the growing sophistication of technology, and its widespread use. Cybercriminals, employing cyber threats and cyber-attacks, engage in criminal acts, thereby violating the rights of the individuals affected.

The exponential growth of these crimes is further exacerbated by the government's insufficient provision of information, awareness, and preventive measures regarding the use of electronic means. Hence, it is imperative and urgent for the government to offer education and awareness initiatives to foster a cybersecurity culture among the Ecuadorian population.

In this Curricular Integration Work, various materials and methods were employed to facilitate its development. Surveys and interviews were conducted with legal professionals, and the findings were used to formulate proactive guidelines aimed at ensuring the rights of individuals using electronic devices for their daily activities. This approach seeks to cultivate digital trust within the Ecuadorian population. Moreover, the objective is to contribute to the reduction of the high incidence of Cybercrimes by disseminating information about Ecuador's National Cybersecurity Policy and Strategy, with the aim of preventing the proliferation of such cybercrimes in cyberspace.

3. Introducción.

El presente Trabajo de Integración Curricular se titula “Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”.

Al referirnos a la ciberseguridad existente en nuestro país, es preciso empezar indicando que los delitos informáticos se originaron con la aparición del Internet, donde el mundo cambió notablemente, los países trataron de imponer reglamentos para su utilización, ya que, con el crecimiento de la tecnología, se dio lugar a una serie de actos ilícitos, denominados “Delitos Informáticos”. Los mismos que han ido evolucionando a la par de la innovación de las tecnologías de la información.

El presente proyecto de investigación es de suma importancia, debido a la dependencia digital de la sociedad, la creciente sofisticación de la tecnología y su uso generalizado que ha dado lugar a amenazas más complejas; actualmente las personas tienen la necesidad de usar los medios electrónicos para realizar múltiples actividades de la vida diaria, cabe indicar que esta situación cobró más fuerza durante la pandemia COVID- 19, donde se incrementó su uso, ya que las actividades presenciales se limitaron totalmente, es aquí donde la delincuencia informática se propaga de forma acelerada y la población estuvo más expuesta a ser víctima de estos actos delictivos. También la proliferación se presenta por la poca información desplegada para poner en conocimiento estos problemas existentes, por lo tanto, creo conveniente que, para disminuir, identificar, detectar, responder o recuperarse de incidentes cibernéticos, es necesario mejorar, difundir, capacitar y enseñar la ciberseguridad, que se la puede entender como la capacidad del Estado de mejorar la resiliencia cibernética y proteger a las personas, sus bienes activos de información y servicios esenciales ante riesgos y amenazas que se identifican en el ciberespacio.

En el presente Trabajo de Integración Curricular se verifica un objetivo general que consiste en: “Realizar un estudio doctrinario, jurídico y comparado de las Estrategias y Políticas de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos”.

Además, también se pudieron verificar los objetivos específicos que se detallan a continuación:

Primer objetivo específico: “Establecer las políticas criminales implementadas por el Estado para promover en los usuarios informáticos la capacidad de prevención ante los riesgos existentes con las ciberamenazas y ciberataques”.
Segundo objetivo específico: “Detectar las formas en las que operan los antisociales al cometer Delitos Informáticos, logrando de esta manera disminuir el índice de personas perjudicadas”.
Tercer objetivo específico: “Propiciar un mayor conocimiento sobre la ciberseguridad para proteger y garantizar la correcta utilización de las Tecnologías de Información y Comunicaciones”.
Cuarto objetivo específico: “Demostrar los adecuados medios informáticos y la protección que el Estado nos brinda a través de la Estrategia y Política de Ciberseguridad”.

La hipótesis tratada es la siguiente: “La actualización del conocimiento y correcta aplicación de la ciberseguridad en el uso de los medios electrónicos servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador”.

El presente Trabajo de Integración Curricular se encuentra estructurado de la siguiente manera: en el marco teórico, se desarrollan capítulos como los Derechos Humanos, Derecho a la Seguridad Humana, Delitos Informáticos, La Ciberseguridad, Víctima, Prevención delictiva para combatir los Delitos Informáticos, Derecho Comparado de las Políticas y Estrategias Nacionales de Ciberseguridad de República Dominicana, España, Chile, Costa Rica y de la República de Argentina.

Este trabajo de investigación contiene los materiales y métodos que fueron utilizados para lograr la obtención de la información, además las técnicas de la encuesta, entrevista y el estudio de casos que sirvieron para fundamentar la presente investigación, logrando con ello verificar los objetivos, uno general y cuatro específicos anteriormente señalados, también contrastar la hipótesis planteada, cuyos resultados contribuyeron a la fundamentación de los lineamientos propositivos.

En la parte final, se describieron las conclusiones y recomendaciones de la investigación, con la finalidad de presentar los lineamientos propositivos que garanticen los derechos de las personas, empresas, instituciones públicas y privadas e incluso del mismo Estado, frente a los delitos informáticos existentes en el mundo digital.

De esta manera queda presentado el Trabajo de Integración Curricular, esperando que esta investigación sea útil y sirva como guía a los estudiantes y profesionales del Derecho como una fuente de consulta.

4. Marco Teórico.

4.1 Derechos Humanos.

4.1.1. Definiciones de Derechos Humanos.

Los Derechos Humanos nacen con el hombre, son inherentes a este por el simple hecho de existir y pertenecer a la especie humana, cada persona tiene la misma dignidad y nadie puede ser excluido del goce de sus derechos.

> Los Derechos Humanos, son todo el conjunto de principios, derechos civiles y políticos, económicos, sociales, culturales y colectivos o difusos que buscan configurar una existencia digna para todas las personas y su ejercicio o reconocimiento no dependen de las particularidades de cada una de ellas como por ejemplo su etnia, religión, nacionalidad, identidad sexual, cultura, discapacidad o cualquier otra característica o condición humana, pues su principio más importante es la Universalidad (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 11).

El Ministerio del Interior a través del Manual de Derechos Humanos para Servidoras y Servidores Públicos, nos detalla una amplia información sobre los Derechos Humanos, puedo decir al respecto que la finalidad que tienen los Derechos Humanos es alcanzar los proyectos de vida de cada una de las personas con dignidad, constituyéndose así en una prerrogativa, poder o facultad de actuar o exigir el cumplimiento de los mismos, teniendo como base la universalidad que es una característica predominante, ya que todos podemos exigir el cumplimiento de los derechos consagrados en la ley suprema.

> Los derechos humanos son facultades, libertades y atributos que tienen todas las personas por su condición humana. Los derechos humanos permiten desarrollar una vida digna y direccionar el ejercicio del poder; están en continuo desarrollo y reconocimiento. Su respeto, protección y realización, constituye el más alto deber del Estado (Defensoría del Pueblo, 2014, pág. 1).

A cerca de la definición que nos ofrece la Defensoría del Pueblo, puedo decir que los Derechos Humanos tienden a ser universales, esta característica es para todas las personas sin distinción alguna de raza, sexo, religión, nacionalidad o cualquier otra situación; por lo que, el

Estado a través de las Instituciones Públicas, tiene el más alto deber de garantizarlos, respetarlos y protegerlos.

Para comprender de mejor manera los derechos humanos y tener un panorama más claro sobre este tema, revisaré definiciones de varios autores como:

Sánchez (2006), señala que "…los derechos humanos, son derechos inalienables y pertenecientes a todos los seres humanos; necesarios para asegurar la libertad y el mantenimiento de una calidad de vida digna, y están garantizados a todas las personas en todo momento y lugar." (p. 19). Con respecto a este tema debo enfatizar, que el Estado ecuatoriano tiene el deber de garantizar a cada persona los derechos que se encuentran consagrados en la norma suprema. El ser humano no puede, sin afectar su dignidad, renunciar a sus derechos o negociarlos y nadie debe atentar, lesionar o destruir los mismos, ya que afectaría su plena autorrealización dentro de la sociedad.

> Faúndez Héctor, manifiesta que: Los derechos humanos pueden definirse como las prerrogativas que, conforme al Derecho Internacional, tiene todo individuo frente a los órganos del poder para preservar su dignidad como ser humano, y cuya función es excluir la interferencia del Estado en áreas específicas de la vida individual, o asegurar la prestación de determinados servicios por parte del Estado, para satisfacer sus necesidades básicas, y que reflejan las exigencias fundamentales que cada ser humano puede formular a la sociedad de que forma parte (Faúndez, 1996, pág. 28).

De acuerdo al pensamiento de Faúndez Héctor, puedo destacar que los derechos humanos constituyen la pieza angular del Derecho, estos han sido creados con la finalidad de reafirmar la dignidad humana, siendo esta el más grande valor que tiene el ser humano, el hombre en su vida diaria merece respeto a sus ideales, género, educación, religión, raza, orientación sexual o cualquier otra condición, por lo que el Estado como organización política, debe garantizar a todos sus ciudadanos la correcta aplicación de sus derechos, asegurando que se puedan satisfacer las necesidades básicas, la convivencia pacífica y la igualdad entre todos los integrantes de la sociedad.

> El tratadista Pedro Nikken señala que: La sociedad reconoce que todo ser humano, por el hecho de serlo, tiene derechos frente al Estado (…) estos derechos, atributos de toda persona e inherentes a su dignidad, que el Estado está en el deber de respetar y garantizar o satisfacer son los que hoy conocemos como derechos humanos (Nikken, 1994, pág. 1).

El autor resalta que el ser humano nace con derechos inherentes a su dignidad, pues los derechos humanos son fundamentales para poder vivir como seres humanos, nos permiten desarrollar nuestras capacidades, inteligencia y talento para poder llevar una vida digna y con respeto, se enfatiza que el Estado debe velar por el correcto goce de los derechos de cada persona.

4.1.2. Principios de los Derechos Humanos.

Según el Módulo Autoformativo sobre el Acceso a la justicia y derechos humanos en Ecuador del Instituto Interamericano de Derechos Humanos, aquellos atributos, facultades o prerrogativas que tienen los seres humanos por el solo hecho de existir, han sido inspirados en los siguientes principios:

- **Dignidad:** Es el valor que poseen todas las personas, cualquiera sea su origen social, cultural, económico, político o religioso.
- **Libertad:** Comprendida en el sentido de que el hombre es libre por naturaleza y que aquella libertad puede ser expresada en todos los aspectos de su vida.
- **Igualdad:** Según la cual todos los seres humanos poseemos los mismos derechos independientemente de nuestras diferencias de origen.
- **Seguridad:** Bajo la reflexión de que todos nacimos libres y tenemos iguales derechos, por lo que quien niegue esos derechos universales, debe responder ante la justicia (la justicia social sólo se alcanza a través de la igualdad entre individuos) (Instituto Interamericano de Derechos Humanos, 2020, pág. 13).

Los principios básicos en los cuales se fundamentan los Derechos Humanos son la dignidad humana, que se puede entender como la piedra angular para el desarrollo del hombre, ya que es inherente a este por su condición de individuo de la especie humana. La libertad es un atributo por el cual cada persona puede autodefinirse y decidir su actuar en la sociedad dando sentido a su propia existencia. Así mismo, la igualdad hace realce a que todos somos iguales ante la ley y debemos recibir un trato libre de discriminación, la misma que tiene por objeto menoscabar o anular el reconocimiento, goce o ejercicio de los derechos. Por último, tenemos la seguridad que nos establece que la persona que niegue, vulnere o atente contra los derechos universales de otra, debe responder ante la justicia por incumplir lo establecido en la norma jurídica suprema de nuestro país.

4.1.3. Características de los Derechos Humanos.

Los derechos humanos están reconocidos en la ley y garantizados por ella, tienen diversas características, que, en virtud de la condición intrínseca del ser humano, son de suma relevancia, entre ellas tenemos:

> **Inherentes o Innatos:** Los Derechos Humanos pertenecen a todas las personas, sin ninguna distinción, provienen de la dignidad intrínseca y el valor de todos los seres humanos. Lo inherente es todo aquello que está naturalmente unido a algo o alguien, por tanto, los Derechos Humanos son inseparables de la condición humana, determinándose como algo innato, propio de la esencia humana (Defensoría del Pueblo, 2014, pág. 1).

Para hablar de esta característica es preciso manifestar que los Derechos Humanos, son propios de cada persona por el simple hecho de nacer, por lo que se puede decir que forman parte de la condición humana, ya que desde el momento de su concepción tiene derecho a una vida digna, donde se puedan satisfacer todas sus necesidades para desenvolverse en sociedad.

Universales: "Los Derechos Humanos pertenecen a todos los seres humanos en cualquier parte del mundo, sin distinción alguna puesto que se fundamenta en la dignidad humana" (Defensoría del Pueblo, 2014, pág. 1). La universalidad, es una característica indispensable de los Derechos Humanos, donde sin distinción alguna toda persona puede gozar de los mismos, nadie puede excluir a los individuos del ejercicio y reconocimiento de sus derechos.

Inalienables: "Los Derechos Humanos son inalienables, no pueden suprimirse, son insustituibles, no negociables ni susceptibles de adaptarlos según conveniencias, no pueden ser enajenados ni negados en ninguna circunstancia. Estos derechos no pueden reemplazarse por otros de ninguna otra naturaleza" (Defensoría del Pueblo, 2014, pág. 1). Esta característica determina que los Derechos humanos no se pueden suprimir, no son susceptibles a cambios ni modificaciones, todos tienen su rol y no podrán ser reemplazados por ningún motivo, salvo en determinadas situaciones y según las debidas garantías procesales. Por ejemplo, se puede restringir el derecho a la libertad si un tribunal de justicia dictamina que una persona es culpable de haber cometido un delito.

Irrenunciables: “No se puede renunciar a los Derechos Humanos ni por voluntad propia de su titular, las personas no pueden prescindir de estos” (Defensoría del Pueblo, 2014, pág. 1). Los Derechos Humanos, son irrenunciables porque pertenecen al ser humano, no pueden ser renunciados ni transmitidos a otra persona por ninguna razón; debemos tener en cuenta que no cabe la renuncia por voluntad propia del sujeto tutelar de los mismos, por lo tanto, son indisolubles a la esencia del ser humano, protegiéndolo de los actos que atenten contra su integridad personal.

Intransmisibles: “Los Derechos Humanos no se pueden trasladar de una persona a otra pues cada persona tiene la facultad de exigir y disfrutar de sus derechos, por cuanto el goce y el disfrute es personal, individual e indelegable” (Defensoría del Pueblo, 2014, pág. 1). Cada ser humano como miembro activo de la sociedad, tiene derechos que son propios desde su nacimiento, los mismos que no pueden ser trasmitidos a otra persona, ya que son únicos; además, el goce y disfrute de ellos solamente le pertenece a su titular.

> **Indivisibles e interdependientes:** Todos los derechos humanos están relacionados entre sí, en tal razón, el avance de uno de ellos facilita el de los demás, y su privación afecta negativamente al resto de derechos. Los Derechos Humanos constituyen un todo intrínseco a la condición humana y no pueden ser ejercidos de manera parcial (Defensoría del Pueblo, 2014, pág. 1).

Esta característica destaca que los derechos son indivisibles, interrelacionados e interdependientes. El avance de uno facilita el avance de los demás. Lo mismo ocurre con la privación de un derecho, en donde este afecta negativamente el correcto desenvolvimiento de los demás, por lo tanto, si no se reconoce uno de los derechos fundamentales del ser humano, este establece un riesgo para los otros.

> **De igual jerarquía:** Todos los derechos humanos tienen el mismo valor, es decir, ningún derecho prevalece sobre otro. De la misma manera, todos tienen la misma importancia en cuanto al respeto a la dignidad humana y en la consecución de los proyectos de vida de las personas (Defensoría del Pueblo, 2014, pág. 1).

Los Derechos Humanos constituyen una base moral y ética que la sociedad considera necesaria para proteger la dignidad de las personas. Debemos tener en cuenta que los derechos

humanos están relacionados entre sí y todos tienen la misma relevancia, no podemos decir que unos tienen mayor importancia que otros.

Progresivos: "Los Derechos Humanos están en constante evolución a medida que se va ampliando su ámbito de ejercicio y protección. No pueden existir acciones de carácter regresivo que disminuyan, menoscaben o anulen injustificadamente el ejercicio de los derechos" (Defensoría del Pueblo, 2014, pág. 1). Los Derechos Humanos son progresivos, ninguna acción puede disminuir o eliminar el reconocimiento de derechos, pues el contenido de las normas legales sólo pueden mantener o aumentar el acceso y garantía de los derechos de las personas y de esta característica nace el principio constitucional de no regresividad. Además, hay que tener presente que cuando se consigue un avance en el ejercicio y la tutela de un derecho humano, ya no se puede eliminar, limitar, ni restringir posteriormente. Al contrario, este debe seguir progresando hasta alcanzar su cumplimiento.

Imprescriptibles: "Los derechos humanos son permanentes: su goce y ejercicio no dependen del tiempo" (Defensoría del Pueblo, 2014, pág. 1). Esta característica reconoce que los derechos humanos no prescriben, no tienen fecha de caducidad por ningún motivo, es decir, los derechos no se pierden, aunque haya transcurrido mucho tiempo.

Absolutos: "Su respeto se puede reclamar indistintamente ante cualquier persona o autoridad" (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 28). Todos los derechos del ser humano establecidos en la Constitución de la República del Ecuador, deben ser respetados y garantizados por el Estado a través de sus instituciones públicas; al ser lesionados cualquiera de ellos, se puede reclamar ante la autoridad competente para lograr una respuesta eficaz.

Exigibles: "Las personas podemos exigir su cumplimiento en cualquier momento de diferentes maneras, ya sea por vía legal, judicial, de participación, etc." (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 30). Cuando se vulneran los derechos humanos propios de cada persona, debemos reclamar, utilizando la vía judicial más efectiva para garantizar el reconocimiento y goce de esos derechos.

Inviolables: Nadie puede atentar, lesionar o destruir los Derechos Humanos, esto quiere decir que las personas y los gobiernos deben regirse por el respeto a los Derechos

> Humanos; las leyes dictadas, las políticas económicas y sociales que se implementan no pueden ser contrarias a éstos, por el bien común de la sociedad (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 30).

El respeto a los Derechos Humanos es de suma importancia, por esta razón todas las normas jurídicas expedidas por el órgano legislativo del país, deben estar estrechamente relacionadas entre sí, no se pueden implementar leyes que estén en contra de los mismos, por lo que se atentaría contra el bienestar de toda la sociedad, perjudicando su correcto desenvolvimiento.

Obligatorios: "La obligatoriedad es una de las características más importantes de los Derechos Humanos ya que significa que el Estado y sus instituciones deben obligatoriamente garantizar y aplicar los Derechos Humanos" (Lasluisa, 2014, pág. 28). En el Ecuador, la obligatoriedad de tutelar, proteger, respetar y promover los Derechos Humanos les corresponde a las instituciones del Estado, por medio de las políticas y leyes que dictan, las mismas que tienen como finalidad garantizar los derechos del ser humano dentro de la sociedad.

4.1.4. Clasificación de los Derechos Humanos.

Al hablar de este tema de suma importancia, puedo decir que se distinguen cuatro generaciones de los derechos humanos. Realizaré una descripción de las tres generaciones, para finalmente centrarme en el tema de mi interés que son los de cuarta generación, que involucra el acceso a las nuevas tecnologías y la cibernética. A continuación, detallaré cada una de ellas:

4.1.4.1. Derechos Humanos de Primera Generación.

> Los Derechos Civiles y Políticos se fundamentan en la libertad y surgen ante la necesidad de oponerse a los excesos de la autoridad. Se proclamaron para limitar las competencias o atribuciones del Estado y se instituyeron como garantías a la libertad. Entre los primeros se encuentran los dirigidos a proteger la libertad, seguridad e integridad física y espiritual de la persona humana. Tales derechos son el derecho a la vida; el derecho a no ser sometido a torturas o a tratos o castigos crueles, inhumanos o degradantes; el derecho a no ser tenido en estado de esclavitud o servidumbre; el derecho a la libertad y la seguridad de la persona, incluido el derecho a un juicio justo; el derecho a la intimidad e inviolabilidad en el hogar y en la correspondencia; y, el derecho a la

> libertad de pensamiento, conciencia o religión. Entre los derechos políticos están el derecho a la libertad de opinión y expresión; el derecho a la libertad de reunión y asociación; el derecho a tomar parte en la conducción de los asuntos públicos, incluido el derecho a votar y a ser elegido (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 32).

De acuerdo al Manual de Derechos Humanos, en esta generación, la libertad es de suma importancia, donde la necesidad es oponerse a los excesos de la autoridad. Se establecieron para limitar las competencias o atribuciones del Estado y se atribuyeron como garantías a la libertad, para proteger la seguridad e integridad física y espiritual de la persona humana que vive en el territorio ecuatoriano.

Los derechos humanos de primera generación son derechos individuales que corresponden a los derechos civiles y políticos, los mismos que imponen al Estado, la obligación de respetar ciertas libertades fundamentales a cada uno de los ciudadanos, como el derecho a la vida, la integridad física, la libertad, la igualdad ante la ley, la prohibición de la tortura, la libertad religiosa, entre otros.

Por lo tanto, son derechos que reconocen la autonomía y libertad frente al Estado, lo que plantean estos derechos humanos es la no interferencia del Estado en la vida de los ciudadanos y ciudadanas.

De acuerdo al problema propuesto en esta investigación, sobre la ciberseguridad como herramienta para prevenir las ciberamenazas y ciberataques que conllevan a los delitos informáticos, se debe indicar que no existe relación con los Derechos de Primera Generación, pues estos tienen su aparición antes de que exista la tecnología, los medios electrónicos y la cibernética.

4.1.4.2. Derechos Humanos de Segunda Generación.

> Los Derechos Económicos, Sociales y Culturales, se fundamentan en la igualdad y en consecuencia el ser humano le exige al Estado que cumpla con ciertas obligaciones de dar y hacer. Entre los derechos económicos, sociales y culturales figuran el derecho al trabajo, a unas condiciones de trabajo justas y favorables, a un salario justo, a la seguridad social, a una alimentación, vestuario y albergue adecuados, a un nivel de vida adecuado, a la salud, a la protección económica por discapacidad, a la protección y

> asistencia de la familia, madres e hijos, a la huelga y sindicalización, a la educación, cultura y ciencia (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 33).

En el Manual de Derechos Humanos, los derechos de segunda generación, se basan en la igualdad de condiciones, dignidad y trato, también son denominados derechos económicos, sociales y culturales, que están fundamentados en el acceso garantizado de bienes, servicios, oportunidades económicas y sociales, para procurar una mejor condición de vida de las personas. Por lo tanto, el ser humano exige al Estado el cumplimiento de ciertas obligaciones de dar y hacer, con el fin de satisfacer las necesidades de los ciudadanos, dentro de estos derechos tenemos el derecho a una adecuada calidad de vida, derecho al trabajo, el derecho de pertenecer a un sindicato, derecho a la salud, derecho a la seguridad social, derecho a la educación, entre otros.

La ciberseguridad y los delitos informáticos que son el eje de la investigación realizada, no son parte de los Derechos Humanos de Segunda Generación, estos tienen que ver con la igualdad y no con el manejo de la información a través de las redes digitales existentes en el ciberespacio.

4.1.4.3. Derechos Humanos de Tercera Generación.

> Los Derechos de los Pueblos tienen la finalidad de proteger los derechos de la humanidad, por lo que está conformado por el derecho a la paz, derecho a un medio ambiente sano, derecho al desarrollo, derecho a una vida digna, derecho a la justicia internacional, etc. Se refiere a la protección de las nacionalidades o pueblos como unidades culturales que habitan un territorio, como son los pueblos indígenas, afroecuatorianos, montubios, etc, quienes tienen el derecho a la tierra y territorio, a la identidad cultural, a la libre determinación, justicia y derecho propio, consulta y participación en la toma de decisiones, al desarrollo, propiedad intelectual, etc. (Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior, 2012, pág. 33).

Los derechos humanos de tercera generación, son considerados también derechos de los pueblos, aparecen a partir de los años 70, en la segunda mitad del siglo XX y responden a los nuevos retos a los que se enfrenta la comunidad internacional, consecuencia de la mundialización (globalización). Estos derechos surgen como respuesta a la necesidad de

cooperación entre las naciones, así como de los distintos grupos que lo integran con el objetivo de afrontar problemas globales.

Los Derechos Humanos de Tercera Generación, hacen referencia a los derechos colectivos de las personas o de la sociedad, como el derecho al desarrollo sostenible, el derecho a la paz, el derecho al medio ambiente sano, derechos de los consumidores y a la protección frente a la manipulación genética.

4.1.4.4. Derechos Humanos de Cuarta Generación.

A la tradicional clasificación de los derechos humanos en tres generaciones, algunos autores añaden una cuarta generación de derechos humanos, esto es, los derechos relacionados con el desarrollo tecnológico, las tecnologías de la información y la comunicación y el ciberespacio.

La división en generaciones de los derechos humanos para su estudio es una creación del checoslovaco ex Director de la División de Derechos Humanos y Paz de la UNESCO, Karel Vašák, que introdujo el concepto en su conferencia para el Instituto Internacional de Derechos Humanos, en Estrasburgo, en 1979.

Las tres primeras generaciones de derechos humanos, son producto de la evolución política de las sociedades nacionales e internacionales; en cambio, los derechos humanos de cuarta generación que se desarrollaron a finales del siglo XX y principios del XXI, tienen como fin proteger el acceso a las nuevas tecnologías, las innovaciones tecnológicas y la globalización.

El ciberespacio, junto a las nuevas tecnologías, dieron como resultado otros derechos, o los derechos tradicionales, tomaron una nueva dimensión. Nos referimos al derecho al acceso a la tecnología, a la libertad de expresión en las redes, a la libre distribución de la información, que se engloban dentro de la cuarta generación de derechos humanos. Así mismo, podemos mencionar el derecho de acceso a la informática; el derecho de acceso a la sociedad de la información en condiciones de igualdad y no discriminación; al uso del espectro radioeléctrico y de la infraestructura para que los servicios en línea sean satelitales o por vía de cable; el derecho a formarse en las nuevas tecnologías, el derecho a la autodeterminación informativa; el derecho al Habeas Data y a la seguridad digital (*DHpedia, los derechos humanos*, 2023, pág. 1).

Este proyecto de investigación tiene énfasis en la Cuarta Generación de los Derechos Humanos, como sabemos los derechos van evolucionando con el tiempo, actualmente la vida diaria gira en torno a las Tecnologías de la Información y la Comunicación**,** estas han sido por una parte un gran beneficio para la hiperconexión y el desarrollo del conocimiento, pero a su vez se ha generado el inadecuado y peligroso uso de las herramientas tecnológicas, ocasionando un alto índice de delitos informáticos, donde las personas que conforman la sociedad de la información se ven afectadas.

Acerca de las cuatro generaciones de los Derechos humanos, podemos decir que se basan en varios aspectos relevantes: La libertad es el valor predominante de los derechos de primera generación; la igualdad, el de los derechos de segunda generación; los derechos de tercera generación tienen que ver con los derechos de los pueblos, se relacionan con la solidaridad. Los nuevos derechos de cuarta generación se fundamentan en el desarrollo tecnológico, las tecnologías de la información y la comunicación, finalmente en el ciberespacio.

CLASIFICACIÓN DE LOS DERECHOS HUMANOS.				
Generaciones.	Primera.	Segunda.	Tercera.	Cuarta.
Denominación.	Derechos Civiles y Políticos.	Derechos Económicos, Sociales y Culturales.	Derechos de los Pueblos.	Derechos de las nuevas tecnologías de la información y la comunicación.
Fundamento.	Libertad.	Igualdad.	Solidaridad.	Acceso al Ciberespacio.
Derechos reconocidos.	**Civiles.** - Vida. - No ser sometidos a torturas o castigos crueles. - Libertad. - No estar en estado de esclavitud. - Juicio justo. - Intimidad. - Libertad de pensamiento, conciencia o religión. **Políticos.** - Libertad de opinión y expresión. - Libertad de reunión y asociación. - Ser parte de los asuntos públicos. - Votar y ser elegido.	- Trabajo. - Salario justo. - Seguridad Social. - Alimentación. - Vestuario. - Albergue. - Salud. - Protección económica por discapacidad. - Asistencia de la familia, madres e hijos. - Huelga y sindicalización. - Educación. - Cultura. - Ciencia.	- Paz. - Medio ambiente sano. - Desarrollo. - Vida digna. - Justicia. internacional. - Tierra. - Territorio. - Identidad cultural. - Libre determinación. - Justicia. - Consulta y participación en la toma de decisiones. - Propiedad intelectual.	- Acceso a la tecnología. - Libertad de expresión en las redes. - Libre distribución de información. - Acceso a la informática y a la información en condiciones de igualdad. - Uso del espectro radioeléctrico y de la infraestructura. - Formación en las nuevas tecnologías. - Autodeterminación informativa. - Habeas Data. - Seguridad digital.

Fuente: Manual de Derechos Humanos para Servidoras y Servidores Públicos del Ministerio del Interior; DHpedia, los derechos humanos.
Autora: Lizbeth Sofía Palacios Orellana.

4.1.5. Derechos Fundamentales reconocidos en la Constitución de la República del Ecuador.

La Constitución de la República del Ecuador del 2008, es la norma con mayor jerarquía de nuestro ordenamiento jurídico, por lo que las demás normas infraconstitucionales deben llevar concordancia a los derechos y garantías que establece el texto constitucional.

Nuestra Ley Suprema se encuentra dividida en: La parte dogmática que constituye el catálogo de los derechos fundamentales, principios y garantías jurisdiccionales vigentes en el nuestro país. La parte orgánica, la misma que especifica la funcionalidad, organización, estructura, funciones, instituciones y organismos del Estado, para viabilizar los derechos establecidos en la parte dogmática.

El Art. 1 de la Constitución establece que "El Ecuador es un Estado constitucional de derechos y justicia" (Constitución de la República del Ecuador, 2008, pág. 11). El presente artículo establece que Ecuador es un Estado constitucional de Derechos, por lo cual, al hablar sobre los derechos humanos en nuestra carta magna, los encontramos en el Título II Derechos, que se refiere al establecimiento y reconocimiento de los derechos de las personas por parte del Estado. Comprende desde el artículo 10 hasta el artículo 83, los cuales integran nueve capítulos. En estos capítulos tenemos un amplio catálogo, donde nos establece los principios de aplicación de los derechos; los Derechos del buen vivir; los Derechos de las personas y grupos de atención prioritaria; los Derechos de las comunidades, pueblos y nacionalidades; los Derechos de participación; los Derechos de libertad; los Derechos de la naturaleza; los Derechos de protección y las responsabilidades de las ecuatorianas y ecuatorianos.

Según el Art. 10 de la Constitución señala: "Las personas, comunidades, pueblos, nacionalidades y colectivos son titulares y gozarán de los derechos garantizados en la Constitución y en los instrumentos internacionales. La naturaleza será sujeto de aquellos derechos que le reconozca la Constitución" (Constitución de la República del Ecuador, 2008, pág. 13). Al referirnos a los derechos humanos, podemos decir que son los principios, facultades y condiciones inherentes al ser humano, es decir, que son propios de la persona desde su nacimiento, por lo que, el Estado como organización política que tutela los mismos, tiene la obligación de respetarlos, protegerlos, garantizarlos y repararlos.

El Art. 11 de la Constitución de la República del Ecuador, estipula que el ejercicio de los derechos se regirá por los siguientes principios:

2. Todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades.

Nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos. La ley sancionará toda forma de discriminación.

El Estado adoptará medidas de acción afirmativa que promuevan la igualdad real en favor de los titulares de derechos que se encuentren en situación de desigualdad.

3. 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.

7. El reconocimiento de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento.

8. El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio.

Será inconstitucional cualquier acción u omisión de carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos.

9. El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución.

El Estado, sus delegatarios, concesionarios y toda persona que actúe en ejercicio de una potestad pública, estarán obligados a reparar las violaciones a los derechos de los particulares por la falta o deficiencia en la prestación de los servicios públicos, o por las acciones u omisiones de sus funcionarias y funcionarios, y empleadas y empleados públicos en el desempeño de sus cargos.

El Estado ejercerá de forma inmediata el derecho de repetición en contra de las personas responsables del daño producido, sin perjuicio de las responsabilidades civiles, penales y administrativas.

El Estado será responsable por detención arbitraria, error judicial, retardo injustificado o inadecuada administración de justicia, violación del derecho a la tutela judicial efectiva, y por las violaciones de los principios y reglas del debido proceso.

Cuando una sentencia condenatoria sea reformada o revocada, el Estado reparará a la persona que haya sufrido pena como resultado de tal sentencia y, declarada la responsabilidad por tales actos de servidoras o servidores públicos, administrativos o judiciales, se repetirá en contra de ellos (Constitución de la República del Ecuador, 2008, pág. 13- 14).

El Art. 11 nos plantea los principios que se tomarán en cuenta para el ejercicio de los derechos, donde las autoridades competentes son las encargadas de tutelar y garantizar su cumplimiento. Ante ley todas las personas son iguales, podrán gozar de los mismos derechos, deberes y oportunidades sin distinción alguna, caso contrario la misma ley sancionará toda forma de discriminación. Para las personas que por alguna situación se encuentren en desigualdad, el Estado proporcionará medidas de acción afirmativa, con el fin de que exista la igualdad, la equidad y la justicia para todos.

Para el ejercicio de los derechos y garantías constitucionales, se aplicará la Constitución y los instrumentos internacionales, los mismos que son de directa e inmediata aplicación. Se debe tomar en cuenta que todos los derechos humanos deben ser de carácter progresivo, a través de las normas, la jurisprudencia y las políticas públicas, se podrá garantizar el pleno ejercicio

de los mismos. El Estado ecuatoriano garantizará el respeto de los derechos humanos en todas sus dimensiones, a través de las instituciones públicas, donde todas las personas que actúen en ejercicio de una potestad pública o judicial, deben prestar un servicio eficiente, caso contrario, estarán en la obligación de reparar los daños ocasionados al titular de los derechos humanos violentados.

> La Constitución de la República del Ecuador, dentro del Capítulo segundo sobre los tratados e instrumentos internacionales, el Art. 417 establece que los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en la Constitución. En el caso de los tratados y otros instrumentos internacionales de derechos humanos se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecidos en la Constitución (Constitución de la República del Ecuador, 2008, pág. 165).

El artículo 417, establece que los tratados e instrumentos internacionales se sujetarán a lo estipulado en la Constitución de la República del Ecuador, los instrumentos internacionales ratificados son de aplicación obligatoria. En materia de Derechos Humanos, los tratados e instrumentos internacionales se regirán por los principios pro ser humano, donde se establece que toda autoridad que pertenece al poder judicial, legislativo o ejecutivo debe aplicar la norma o la interpretación que sea más favorable a la persona o comunidad, en todos los casos donde se considere la protección o la limitación de los Derechos Humanos. El de no restricción de derechos, donde ninguna norma jurídica podrá restringir el contenido de los Derechos, ni las garantías constitucionales. El de aplicabilidad directa, se refiere a que los jueces y servidores públicos, podrán utilizar las normas constitucionales y las establecidas en instrumentos internacionales de derechos humanos de forma directa, siempre que sean más favorables a lo determinado en la Constitución. El de cláusula abierta, permite garantizar los Derechos Humanos, el cual debe ser sin restricciones, cuidando la esencia del ser humano en todas sus formas.

4.2 Derecho a la Seguridad Humana.

Con el fin de comprender y tener un punto de vista claro sobre el Derecho a la Seguridad Humana, observaremos varias definiciones entre ellas tenemos:

> La Comisión de la Seguridad Humana en su Informe “La Seguridad Humana Ahora”, dice que la seguridad humana “…consiste en proteger la esencia vital de todas las vidas

humanas de una forma que realce las libertades humanas y la plena realización del ser humano. Seguridad humana significa proteger las libertades fundamentales: libertades que constituyen la esencia de la vida. Significa utilizar procesos que se basan en la fortaleza y las aspiraciones del ser humano. Significa proteger al ser humano contra las situaciones y las amenazas críticas (graves) y generalizadas." (Comisión de la Seguridad Humana, 2003, pág. 3).

La Seguridad Humana es la encargada de cuidar al ser humano contra cualquier tipo de amenaza o vulneración, logrando disminuir la inseguridad que es la principal preocupación de la ciudadanía en general, a través de la creación de sistemas de diversa índole, entre ellas podemos encontrar a los políticos, sociales, medioambientales, económicos, militares y culturales que tengan como fin indispensable brindar y garantizar al ser humano una adecuada supervivencia, así como los medios de vida y dignidad más propicios donde el hombre se pueda desenvolver integralmente como parte de la sociedad.

Alkire sostiene que "el objetivo de la seguridad humana es salvaguardar el núcleo vital de todas las vidas humanas de las amenazas críticas persistentes, de un modo que sea consistente con el desarrollo humano a largo plazo" (Alkire, 2003, pág. 2). El autor hace referencia al fin que persigue la seguridad humana, que es la protección de la persona ante todo peligro o amenaza existente en la sociedad, evitando de esta manera la vulneración de los derechos humanos y poder garantizar su plena realización.

"El derecho a la seguridad es una combinación de facultades y potestades que tiene la sociedad para requerir del Estado la adopción de condiciones propicias para una convivencia pacífica exenta de todo riesgo o peligro" (Ministerio Coordinador de Seguridad Interna y Externa del Ecuador, 2012, pág. 47). Cabe mencionar que el derecho a la seguridad humana tiene como base la protección ante la inseguridad y el peligro que día a día ocasiona mayor preocupación en la población, por lo que las personas deben exigir al Estado, la implementación de políticas que ayuden a prevenir y mitigar estos problemas sociales.

4.2.1. Derecho a la Seguridad Humana en la Constitución de la República del Ecuador.

La Constitución de la República del Ecuador, siendo la norma que tiene supremacía en nuestro ordenamiento jurídico, establece dentro de la Sección undécima la Seguridad humana, la misma que detallaré a continuación:

> El Art. 393 señala que 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 (Constitución de la República del Ecuador, 2008, pág. 159).

Este artículo hace énfasis al valor que representa cuidar el bien jurídico que es la vida del ser humano, el Estado a través de la ley nos garantiza la seguridad a la misma frente a los actos de violencia y discriminación que se puedan presentar día a día, para lo cual el Estado ha elaborado distintas políticas y acciones integradoras, con el fin de que podamos tener armonía y paz en la comunidad. Entre los órganos que se encargan de la planificación y aplicación de estas políticas y acciones integradoras tenemos: en primer lugar el gobierno central, seguido de los cuatro niveles de gobiernos autónomos descentralizados que son: los gobiernos regionales autónomos, los gobiernos provinciales, los gobiernos municipales y los gobiernos de las parroquias rurales, quienes pondrán en práctica lo establecido, permitiendo que exista una seguridad eficaz ante las infracciones y delitos existentes en nuestro país.

4.2.2. Enfoques de la Seguridad Humana.

La seguridad humana como herramienta de protección del hombre, constituye tres libertades: la libertad del miedo, la libertad de la necesidad o miseria y la libertad para vivir con dignidad:

> **Libertad del miedo**, implica proteger a las personas de las amenazas directas a su seguridad y a su integridad física, se incluyen las diversas formas de violencia que pueden surgir de Estados externos, de la acción del Estado contra sus ciudadanos, de las acciones de unos grupos contra otros, y de las acciones de personas contra otras personas (Instituto Interamericano de Derechos Humanos, 2012, pág. 20).

Sobre la libertad del miedo, podemos mencionar que implica la protección de las personas ante todo tipo de amenazas y peligros que violentan la seguridad y la integridad tanto física como psicológica; cabe indicar que las amenazas constituyen una infracción donde se impone a un sujeto pasivo que realice o cumpla determinada conducta, o por el contrario deje de hacer algo contra su propia voluntad. Por lo tanto, se debe defender al ser humano y a la

comunidad de la violación de sus derechos fundamentales que causan múltiples alteraciones y afectaciones en su vida diaria.

Libertad de la necesidad o de la miseria, se refiere a "La protección de las personas para que puedan satisfacer sus necesidades básicas, su sustento y los aspectos económicos, sociales y ambientales relacionados con su vida" (Instituto Interamericano de Derechos Humanos, 2012, pág. 20). El Estado ecuatoriano garantiza a las personas una nueva forma de convivencia ciudadana, donde exista la diversidad y la armonía con la naturaleza, alcanzando con ello el buen vivir, el Sumak kawsay; una sociedad que respete la dignidad de las personas y las colectividades, logrando de esta forma la protección a la vida, al bien común y una satisfacción plena a las necesidades básicas del ser humano en el ámbito social, económico, ambiental, entre otros.

> **Libertad para vivir con dignidad**, se refiere a la protección y al empoderamiento de las personas para librarse de la violencia, la discriminación y la exclusión. La seguridad humana va más allá de la ausencia de violencia y reconoce la existencia de otras amenazas a los seres humanos, que pueden afectar su sobrevivencia, sus medios de vida o su dignidad (Instituto Interamericano de Derechos Humanos, 2012, pág. 20).

Este tipo de libertad, hace énfasis en las estrategias de la Seguridad humana, me refiero específicamente a la protección y el empoderamiento, donde las personas buscan su libertad de los actos de violencia, discriminación y exclusión, que son los problemas más comunes de la actualidad, pretendiendo con ello mitigar estas realidades que amenazan el desarrollo óptimo del ser humano, su proyecto de vida y su realización personal, que a su vez se sustenta en las opciones, que el sujeto puede tener para conducir su vida y alcanzar el destino que se propone.

4.2.3. Estrategias de la Seguridad Humana.

La seguridad humana constituye la esencia básica de la vida, se fundamenta en dos estrategias de acción que son la protección y el empoderamiento, a continuación, las detallaré a cada una de ellas:

> La protección, es definida por la Comisión sobre Seguridad Humana como las estrategias, establecidas por los Estados, los organismos internacionales, las ONG y el sector privado, para resguardar a las personas de las amenazas. Implica establecer medidas de "arriba hacia abajo", o descendentes, en reconocimiento de que las personas

> se enfrentan a amenazas que no pueden controlar (desastres naturales, crisis financieras, conflictos). La seguridad humana requiere la protección sistemática, integral y preventiva. Los Estados son los principales responsables de proveer este tipo de protección, pero también otros actores, como los organismos internacionales, la sociedad civil y las ONG- desempeñan un papel importante (Instituto Interamericano de Derechos Humanos, 2012, pág. 23).

Al hablar sobre la estrategia de protección, puedo decir que es una herramienta fundamental para implementar la seguridad humana, como se menciona anteriormente implica establecer medidas de "arriba hacia abajo" o descendentes, con la finalidad de aportar al reconocimiento de que los seres humanos constantemente se enfrentan a amenazas que muchas veces no pueden ser controladas, ocasionando afectaciones en la vida integral de las personas. La seguridad humana solamente puede ser garantizada por parte del Estado, ya que es el encargado de la protección sistemática, integral y preventiva ante la inseguridad existente, así como los organismos internacionales que también son parte fundamental del Derecho y sobre todo en este tema de suma importancia para la sociedad en general.

> El empoderamiento, son las estrategias que habilitan a las personas para sobreponerse de las situaciones difíciles. Implica establecer medidas de "abajo hacia arriba" o ascendentes, con el fin de desarrollar las capacidades en las personas y en las comunidades para que sean artífices de su propio destino. El empoderamiento no solo habilita a las personas a lograr el desarrollo de sus potencialidades, sino que también les permite participar en el diseño y ejecución de las soluciones necesarias para su seguridad humana y la de otras personas (Instituto Interamericano de Derechos Humanos, 2012, pág. 23).

Dentro de la seguridad humana, el empoderamiento, es el mecanismo que ayuda a preparar y desarrollar las capacidades de las personas y comunidades, para que conozcan cómo anticiparse y protegerse ante las posibles amenazas y peligros a los que la población está sujeta, evitando de esta forma, los altos índices de inseguridad existentes actualmente. La idea de seguridad humana tiene que ser construida y restablecida nuevamente, por medio de proyectos, políticas y estrategias de empoderamiento implementadas por el Estado, que permitan facilitar el desarrollo de una vida digna, libre de necesidades y temores, logrando con ello una sociedad justa y equilibrada.

4.2.4. Principios de la Seguridad Humana.

La seguridad humana como elemento básico del hombre para vivir en armonía, se fundamenta en varios principios básicos, entre ellos tenemos:

Centrada en las personas. "Para la seguridad humana las personas son el centro del análisis y, consecuentemente, se consideran las condiciones que amenazan la sobrevivencia, medios de vida y dignidad de las personas" (Instituto Interamericano de Derechos Humanos, 2012, pág. 27). En este principio, podemos decir que el derecho considera a las personas como las protagonistas y destinatarias de las acciones, se analizan las inseguridades que amenazan la supervivencia del ser humano y de las comunidades en general.

> **Multisectorial**. La seguridad humana se basa en la comprensión multisectorial de las inseguridades. En consecuencia, además de la seguridad nacional, la seguridad humana implica la comprensión de una gama amplia de amenazas y de sus diferentes posibles causas relacionadas con la economía, la alimentación, la salud, el medio ambiente, la seguridad personal, comunitaria y política (Instituto Interamericano de Derechos Humanos, 2012, pág. 27).

La seguridad humana se enfatiza en la interconexión entre amenazas, inseguridades, vulnerabilidades y las respuestas a las mismas, las amenazas están relacionadas entre sectores y regiones, por lo que en la actualidad se ha convertido en un problema global donde se necesita la planificación, ejecución de políticas y programas por parte del Estado, para evitar los efectos negativos en la sociedad.

Integral. "La seguridad humana implica enfoques integrales que enfatizan en la necesidad de respuestas comprensivas y multisectoriales con el fin de articular las agendas que se relacionan con seguridad, desarrollo y derechos humanos" (Instituto Interamericano de Derechos Humanos, 2012, pág. 27). El carácter multidimensional que establece este principio hace referencia a las amenazas y a la inseguridad que hoy en día es muy frecuente, afectando de manera global a un país. La seguridad, desde una perspectiva lógica, depende de las condiciones favorables en los ámbitos social, político, económico y ambiental del ser humano.

Contextualizada. "La seguridad humana reconoce que las inseguridades varían considerablemente en diferentes contextos y, por lo tanto, promueve la búsqueda de soluciones contextualizadas que respondan adecuadamente a cada situación particular" (Instituto

Interamericano de Derechos Humanos, 2012, pág. 28). La seguridad humana se basa en las inseguridades del ser humano que varían dependiendo de los contextos y de los momentos. Evalúa las percepciones donde las situaciones locales o nacionales deben contextualizarse en marcos más amplios para identificar los problemas y buscar las soluciones de acuerdo a la situación particular propia de cada contexto.

Preventiva. "Al llegar a las causas y a las manifestaciones de las inseguridades, la seguridad humana se orienta a la prevención e introduce sus estrategias de protección y empoderamiento" (Instituto Interamericano de Derechos Humanos, 2012, pág. 28). La seguridad humana al ser preventiva busca encontrar las posibles causas o raíces de las amenazas a la seguridad, analizando a las personas y las comunidades, con el fin de escoger las mejores soluciones que prevengan la inseguridad presente en la sociedad.

4. 3. Delitos Informáticos.

4.3.1. Historia de los Delitos Informáticos en Ecuador.

Al referirme sobre la historia de los delitos informáticos es indispensable hablar de los primeros computadores que existieron anteriormente, estas máquinas surgieron como medio de cálculo lógico, debido a las necesidades durante la Segunda Guerra Mundial, con el fin de decodificar las transmisiones de los bandos, que debían hacerse a través de cálculos rápidos y constantes.

La primera computadora mecánica programable del mundo fue la denominada Z1, diseñada por el ingeniero alemán Konrad Zuse entre 1935 y 1936, y se terminó de construir en 1938.

Esta computadora representó un gran avance para la época, se consideraba una calculadora de acción binaria, que leía instrucciones de cintas perforadas, cuyas funciones eran limitadas, efectuaba sumas, restas, multiplicación y división, a su vez era capaz de leer y guardar información en la memoria, que almacenaba 64 palabras de 22 bits (dígito del sistema de numeración binario, que se representa con dos valores, el 0 y el 1), era capaz de realizar sumas a una velocidad de 5 segundos y multiplicaciones en 10 segundos. La computadora fue destruida tras el bombardeo a Berlín en 1943, la réplica de aquel equipo se encuentra en el Museo de Tecnología de la misma ciudad.

Luego Zuse desarrolló, entre 1931 y 1941, las computadoras Z2 y Z3. Estos equipos antecedieron a la computadora ENIAC, que se presentó públicamente en febrero de 1946 y operó hasta 1955.

El aparecimiento de los delitos informáticos se dio a finales de la segunda guerra mundial, con las diferentes armas de guerra tanto nucleares o químicas, en donde los Estados en conflicto investigaron nuevas formas de atacar a sus contrarios. La investigación tecnológica se impuso sobre los equipos de telecomunicaciones de los países, dejándoles sin acceso a la comunicación, vulnerando sus derechos. De esta manera, se creó el primer satélite artificial llamado SPUNIK, creado por la EX UNIÓN SOVIÉTICA (04 de octubre de 1957), liderando antes que los Estados Unidos de América, quienes pretendían realizar una carrera inter espacial. Dos años más tarde se crea el departamento ADVANCED RESEARCH PROJECTS AGENCY (ARPA), traducido en español AGENCIA DE PROYECTOS DE INVESTIGACIÓN AVANZADA en los Estados Unidos de América, como respuesta a los desafíos tecnológicos y militares de la entonces URSS, una década más tarde, sería considerada la organización que asentó los fundamentos de lo que sería conocido como Internet, dando inicio al uso de las Comunicaciones Globales.

En 1983 fue el año en que nació el Internet, donde el Departamento de Defensa de los Estados Unidos decidió usar el protocolo TCP/ IP, que es la identificación del grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet, incorporándolo en su red Arpanet y creando así la red Arpa Internet que hoy conocemos.

Con la aparición del Internet, el mundo cambió notablemente, algunos países trataron de imponer reglamentos para su utilización, ya que, con el crecimiento de la tecnología, se dio lugar a una serie de actos ilícitos, denominados “Delitos Informáticos”. Los mismos que han ido evolucionando a la par de la innovación de las tecnologías de la información, el uso de los sistemas informáticos permite realizar diversas transacciones financieras, comerciales y bancarias, así como pagos por medios electrónicos y el desarrollo de las redes de comunicación que permiten la transmisión de datos.

El Delito Informático en el Ecuador, tiene su aparición en el año 2002, con la vigencia de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, conocida como Ley No. 67, publicada el 17 de abril del mismo año, en donde las Infracciones Informáticas se encontraban dentro del Título V, desde el Art. 57 al 64. Luego los delitos informáticos fueron agregados al

Código Penal Ecuatoriano vigente en aquel entonces y actualmente se encuentran ampliados en el Código Orgánico Integral Penal, publicado en el Suplemento 180 del 10 de febrero de 2014, cobrando plena vigencia el 10 de agosto del mismo año, incrementando así el catálogo de delitos. Por lo tanto, se contempla de esta forma una nueva modalidad delictiva, que es propia de la evolución de la tecnología, la utilización de la computadora, teléfonos móviles y la informática.

> Con respecto a este tema, la doctrina señala: Las infracciones informáticas son nuevas conductas delictivas que en el Ecuador se han ido perpetrando en los últimos años, en especial desde inicios del siglo XXI, es su gran mayoría realizado por los denominados crackers, que son personas que utilizan los medios informáticos para cometer infracciones con motivos de carácter económico. (Carpio, 2013, pág. 14).

Las telecomunicaciones en los últimos años han evolucionado, hoy en día todo se realiza a través de los medios digitales, con la aparición de la pandemia por el COVID-19, la vida tuvo una gran transformación, donde anteriormente la mayoría de las actividades era de manera presencial, para luego pasar a realizarse en línea, dependiendo así de los medios informáticos. En la actualidad este cambio ha quedado marcado permanentemente para las futuras generaciones.

En nuestro país los delitos informáticos no eran muy comunes, con el aumento del acceso al Internet de las personas, estos se han incrementado. En la actualidad, miles de personas han sido víctimas de estas infracciones, de manera especial cuando se efectúan compras de bienes y servicios a través del Internet.

4.3.2. Conceptos de Delitos Informáticos.

Antes de hablar sobre los delitos informáticos es preciso conceptualizar lo que es delito, Téllez (2012) lo define como: “acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas”. (Pág. 27). De acuerdo al criterio del autor, se puede decir que delito es toda aquella conducta que violenta los derechos fundamentales y las normas de convivencia establecidas en la ley, por lo tanto, es toda acción u omisión que se considera en contra del ordenamiento jurídico y como toda conducta contraria al Derecho se le debe atribuir una sanción o pena proporcional a la infracción cometida, las mismas que, en la legislación ecuatoriana se encuentran contempladas en el Código Orgánico Integral Penal, logrando de esta manera reparar el daño ocasionado a la víctima.

Para entender de mejor manera a los delitos informáticos es indispensable estudiar las definiciones que nos brindan varios tratadistas, entre ellos tenemos:

Pérez (1996) manifiesta que los Delitos Informáticos son “aquel conjunto de conductas criminales que se realizan a través de un ordenador electrónico o que afectan al funcionamiento de los sistemas informáticos”. (p. 18). Los comportamientos delictivos en el campo de la informática son cada vez más especializados, van evolucionando a medida que se incrementa el uso y el avance de la tecnología, por lo que pueden utilizar múltiples medios informáticos para cometerlos, afectando los sistemas, redes y datos informáticos.

Para el Dr. Carlos Sarzana (2012) “Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, atentando contra su integridad, confidencialidad o disponibilidad, como la propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos”. (Pág. 78). Los delitos informáticos son conductas ilícitas susceptibles de sanción, realizadas por el ser humano, utilizando como medio indispensable a la tecnología, es decir, a los dispositivos de comunicación, el fin principal es causar daño o impedir el uso de las redes informáticas, exponiendo de esta forma la integridad de las personas y el adecuado ejercicio de los derechos y garantías universales.

> 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 para realizar un delito); (b) Tienen por objeto robo de información, robo de contraseñas, fraude a cuentas bancarias, etcétera (Policía Nacional del Ecuador, 2021).

Los delitos informáticos, ciberdelitos o delitos telemáticos son actos delictivos cometidos en el entorno digital o en el Internet, a través de medios o elementos informáticos, afectando la información y los datos como bien jurídico tutelado. Actualmente la utilización de las nuevas tecnologías dentro de la vida cotidiana y el creciente número de usuarios existentes en el ciberespacio, han ocasionado conductas delictivas cada vez más perfeccionadas por los antisociales; por lo tanto, la población en general debemos tomar las precauciones debidas y estar en alerta para no ser víctimas de los delitos informáticos.

4.3.3. Características de los Delitos Informáticos.

Según la doctrina las principales características que se destacan en los delitos informáticos son las siguientes:

1. Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
3. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. Ofrecen a los menores de edad facilidades para su comisión.
10. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional (Téllez, 2012, pág. 188).

Al referirnos a las características de los delitos informáticos, señaladas por el autor antes mencionado, podemos decir, que son concretas y específicas, se pueden fácilmente diferenciar de los demás delitos existentes en el catálogo de delitos del Código Orgánico Integral Penal, su forma de ejecutarlo es clara y concisa, así como también las personas que lo realizan y los medios usados para el cometimiento de estos actos delictivos.

Con respecto a las conductas criminales de cuello blanco, podemos indicar que el delito es cometido por personas con conocimientos sobre la informática y cibernética, los mismos que están en lugares estratégicos o que presten la facilidad para acceder a la información de carácter confidencial como por ejemplo instituciones crediticias, empresas, gobierno o personas particulares, perjudicando a la víctima y a la sociedad en general.

Además, se ha podido observar que este tipo de delincuentes generan grandes pérdidas en sus víctimas. Cabe indicar que en este tipo de delitos informáticos no existe la presencia física del sujeto activo de la infracción, porque se lo realiza por uno o varios medios electrónicos, sin ser identificados por sus víctimas, dificultando su comprobación, por ser de carácter técnico. En este tipo de conductas que están en contra de la ley, se ha podido identificar que los antisociales no necesitan de una gran suma de dinero para poder ejecutarlos, solamente el acceso al Internet y a un medio electrónico de fácil adquisición.

Los altos índices de delitos informáticos que se presentan en el Ecuador, no todos son denunciados ante la Fiscalía General del Estado, siendo esto muy preocupante, por lo tanto, estos casos quedan en la más absoluta impunidad.

4.3.4. Sujeto activo y pasivo en el Delito Informático.

Como todo delito, el informático tiene un sujeto activo y otro pasivo:

Sujeto Activo: En este tipo de delitos, es aquella persona que tiene habilidades para el manejo de los sistemas informáticos, no necesariamente conocimientos técnicos de informática o un nivel de instrucción elevado, para poder manipular información o sistemas de computación.

Sujeto Pasivo: En el caso del Delito Informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin, entidades que usan sistemas automatizados de información.

4.3.5. El Delito Informático en la Constitución de la República del Ecuador.

El bien jurídico protegido de los delitos informáticos principalmente es la propiedad y la Constitución se refiere al derecho a la propiedad en la siguiente norma:

"Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley,

previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

26. El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas" (Constitución de la República del Ecuador, 2008, pág. 29-30).

La Constitución de la República del Ecuador, dentro del Art. 66 reconoce y garantiza a las personas varios derechos, en el ámbito de la informática tenemos los derechos establecidos en los numerales 19, 20, 21 y 26.

Dentro del numeral 19 se estipula el Derecho a la protección de datos de carácter personal, el correcto tratamiento de los mismos debe ser una exigencia de la dignidad de la persona, del libre desarrollo de la personalidad, de formación del carácter y de los valores personales. Cuando otros acceden a la información privada de una persona, esta se siente afectada seriamente en su normal desempeño en la sociedad. La tecnología hoy en día ha permitido su difusión masiva, situación que pone en riesgo a las personas y aumenta de forma considerable los daños a sus derechos fundamentales.

Así mismo, el numeral 20 hace énfasis en el derecho a la intimidad personal y familiar, como sabemos es un derecho fundamental; el ser humano tiene la facultad de escoger si hacer conocer o no ciertos aspectos de su vida privada, información referente al ámbito profesional, personal y familiar, donde nadie puede invadir su privacidad, de esta manera se debe garantizar su plena protección y defensa frente a la intromisión de terceros, inclusive del mismo Estado.

El numeral 21 del mismo artículo se refiere al derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, este derecho se materializa cuando la correspondencia es abierta, se da el rompimiento de las seguridades, sustracción o desviación de una carta, mensaje o información del objeto jurídico tanto de manera física como virtual, es por esto que el derecho violentado se ocasiona cuando el acto se produce sin consentimiento y conocimiento de la persona a la que va dirigida esta acción.

Por último, tenemos al numeral 26 que hace mención al derecho a la propiedad en todas sus formas, es cuando se le otorga al titular del mismo, la facultad para usar, gozar y disponer de una cosa de manera libre, por lo tanto, el propietario queda envestido para hacer lo que le

parezca pertinente sobre las cosas que se encuentran a su disposición y se consideren jurídicamente como suyas.

4.3. 6. Delitos Informáticos tipificados en el Código Orgánico Integral Penal.

En vista del alto índice de los delitos informáticos, dentro de nuestro ordenamiento jurídico se han tipificado cada uno de los mismos, con el fin de poder sancionar a las personas que cometan este tipo de conductas, a continuación, los detallaré:

> El Art. 173 del Código Orgánico Integral Penal sobre el Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, señala que la persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.
>
> Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.
>
> La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, pág. 60).

La conducta delictiva mencionada anteriormente, ha cobrado mayor fuerza con el avance tecnológico, usando medios electrónicos como el teléfono y la computadora, para mantener relaciones sexuales por vía electrónica, que se aparta del acto sexual convencional entre parejas, utilizando para su cometimiento palabras sugestivas, fotografías y hasta filmaciones donde se pide a la propia víctima, que realice actos de contacto sexual por medios electrónicos.

La característica principal de este delito es que exista el acercamiento con finalidad sexual o erótico, debemos tener en cuenta que no se requiere el contacto físico del agresor contra la víctima; sino que el medio electrónico sirve para contactarle, por vía telefónica, WhatsApp, o por cualquier red social, utilizando frases que produzcan en la víctima el engaño, sin que sea necesario ejercer la fuerza sobre ella.

También este tipo penal, se refiere al acercamiento mediante coacción o intimidación, así como la suplantación de la identidad de un tercero o mediante el uso de una identidad falsa, por medios electrónicos o telemáticos, donde se usa una apariencia distinta a la real, con nombres y edades cambiadas, en estos casos la persona es sancionada con el incremento de la pena privativa de libertad.

> El Art. 174 del Código Orgánico Integral Penal sobre la Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos, estipula que la persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años (Código Orgánico Integral Penal, 2014, pág. 60).

Los medios electrónicos hoy en día tienen gran relevancia, porque brindan múltiples servicios a las personas, facilitando la ejecución de sus actividades, así como también son medios utilizados para cometer toda clase de delitos; el Art. 174 nos habla sobre la oferta de servicios sexuales donde se utilizan a niños, niñas y adolescentes para cometer este tipo de delitos. Debemos tomar en cuenta que, en nuestro país, los niños, niñas y adolescentes forman parte de los llamados grupos de atención prioritaria; es decir, por sus condiciones son los más vulnerables, por lo tanto, el Estado, la sociedad y la familia deben brindar la protección necesaria, con el propósito de favorecer su desarrollo integral, en el marco del respeto absoluto a la libertad, dignidad y equidad.

Esta conducta antisocial, trae en los niños, niñas y adolescentes, consecuencias exteriorizadas en afecciones de por vida, no solo físicas, sino también psicológicas, que generan conmoción y alarma en la sociedad, amenazando de esta forma el principio del interés superior del niño, que es considerado como el conjunto de acciones y procesos tendentes a garantizar un desarrollo integral y una vida digna, así como las condiciones materiales y afectivas que permitan vivir plenamente y alcanzar el máximo de bienestar posible a las y los menores de edad.

> El Art. 178 del Código Orgánico Integral Penal hace referencia a la Violación a la intimidad, donde la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información

contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (Código Orgánico Integral Penal, 2014, pág. 62).

El Art. 178, nos brinda un enfoque amplio sobre la violación a la intimidad, el mismo que forma parte de los delitos informáticos, que están contenidos en el Código Orgánico Integral Penal vigente, que es producido cuando una persona, sin el consentimiento o la autorización legal del titular o propietario de la información contenida en archivos informáticos, accede, difunde o publica información confidencial de la otra persona, atentando contra el derecho a la intimidad personal y el honor de la misma. Debemos estar claros que este delito es cometido por medio de las redes sociales, donde la mayoría de personas tenemos acceso a las Tecnologías de la Información y la Comunicación, por lo que, existe el riesgo de poder ser víctimas de este tipo de conductas antisociales, afectando con ello nuestra confidencialidad.

El Art. 186 del Código Orgánico Integral Penal, hace mención al delito de Estafa, señala que la persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copiar o reproducir información de tarjetas de crédito, débito, pago o similares (Código Orgánico Integral Penal, 2014, pág. 64).

El delito de estafa es cometido por la persona que, con ánimo de lucro, utiliza algún tipo de engaño para inducir a error a otra persona, llegando a cometer un acto en perjuicio propio o ajeno. El patrimonio es el bien jurídico protegido; dentro de la ley para que el delito de estafa sea consumado, debe producirse el daño patrimonial.

También dentro del delito de estafa en el numeral 2, nos menciona que existen personas que utilizan múltiples dispositivos electrónicos, para defraudar a los cajeros automáticos, todo esto con el fin de conseguir la información de tarjetas de crédito, débito o similares, para cometer el delito informático, el mismo que perjudica el patrimonio de la víctima, generando en ella un alto grado de desconfianza, en el uso de los medios electrónicos, que difícilmente podrá superar.

> Según el Art. 190 del Código Orgánico Integral Penal, la Apropiación fraudulenta por medios electrónicos se da cuando 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 (Código Orgánico Integral Penal, 2014, pág. 66).

La apropiación fraudulenta por medios electrónicos, es un tipo de criminalidad que abarca el ámbito informático, telemático y las redes informáticas, donde se ha proliferado el uso de la informática, como por ejemplo la transferencia de dinero, el pago de salarios o de servicios básicos, la compra de todo tipo de objetos, las transferencias interbancarias, el retiro de dinero, el uso de tarjetas de crédito y débito, entre otras. Todas estas actividades que realizamos diariamente, son el medio para que la delincuencia avance, utilizando metodologías actualizadas que les ayuda a encontrar la clave de acceso a cuentas de personas naturales o jurídicas, con la finalidad de apropiarse fraudulentamente de bienes, valores o derechos de terceros.

El Estado ecuatoriano ha incorporado en el Código Orgánico Integral Penal nuevas formas de ejecución delictivas, como la apropiación fraudulenta, que se realiza mediante la utilización de sistemas informáticos, sancionando la alteración, manipulación, modificación o

inutilización fraudulenta, enfrentando esta realidad social que afecta a toda la población de nuestro país.

> De conformidad con el Art. 191 del Código Orgánico Integral Penal, la Reprogramación o modificación de información de equipos terminales móviles, establece que 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 (Código Orgánico Integral Penal, 2014, pág. 66).

Este artículo nos habla sobre el delito de reprogramación o modificación de información de equipos terminales móviles, constituye un delito informático, tipificado en el Código Orgánico Integral Penal, donde el medio de consumación son los equipos terminales móviles, entendiéndose como el dispositivo físico, destinado a ser conectado a una red pública de telecomunicaciones, con objeto de enviar, procesar o recibir información, que les servirán a los delincuentes para usarla en contra de la víctima.

> El Art. 192 del Código Orgánico Integral Penal, señala el Intercambio, comercialización o compra de información de equipos terminales móviles, donde la persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, 2014, pág. 66).

El intercambio, comercialización o compra de información de equipos terminales móviles, están amparados en el Art. 192, que es un delito que se produce en las bases de datos, que contienen la información de identificación de los equipos terminales móviles, los mismos que han sido violentados por los delincuentes informáticos, con la finalidad de obtener la información confidencial, de datos personales, laborales, empresariales u otros, que les permitirá consumar el acto delictivo ocasionando grandes pérdidas en las personas afectadas.

> De acuerdo con el Art. 193 del Código Orgánico Integral Penal el Reemplazo de identificación de terminales móviles, ocurre cuando la persona 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 (Código Orgánico Integral Penal, 2014, pág. 66).

El Art. 193, se refiere al delito que una persona comete al reemplazar las etiquetas de fabricación de los terminales móviles, que es el lugar donde se encuentra la información necesaria para identificar, reconocer o describir a estos equipos y luego proceder a etiquetarlos con información falsa o contraria a la original, afectando de forma considerable a los propietarios o fabricantes de estos equipos, causando numerosas pérdidas y desinformación.

> La Comercialización ilícita de terminales móviles, según el Art. 194 del Código Orgánico Integral Penal, 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 (Código Orgánico Integral Penal, 2014, pág. 66).

La comercialización ilícita de terminales móviles, es también un delito informático que se encuentra en el Art. 194, dentro del Código Orgánico integral Penal, la cual establece la sanción correspondiente, a quien violente las disposiciones y procedimientos establecidos, por la autoridad encargada del área de las telecomunicaciones, afectando gravemente a las tecnologías de la información y comunicación.

> La Infraestructura ilícita, según el Art. 195 del Código Orgánico Integral Penal, señala que 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 (Código Orgánico Integral Penal, 2014, pág. 66).

El Art. 195 anteriormente detallado, nos hace conocer sobre la información de la identificación de un equipo terminal móvil, que es todo dispositivo por medio del cual el usuario puede acceder a las redes de telecomunicaciones móviles, para la prestación de servicios de comunicaciones de voz y datos, que es reprogramado o alterado por los delincuentes informáticos, en la infraestructura, programas, equipos, bases de datos o etiquetas del equipo terminal móvil en el que cometen el acto ilícito.

> Dentro del Código Orgánico Integral Penal, el Art. 212, hace referencia a la Suplantación de identidad, señala que la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una

persona, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, 2014, pág. 72).

El Art. 212 del Código Orgánico Integral Penal, nos habla sobre el delito de suplantación de identidad, entendiéndose a la misma como una actividad malintencionada donde el delincuente se hace pasar por otra persona por diversos motivos, cometiendo algún tipo de fraude, obtener datos de manera ilegal, conseguir la confianza de un menor para poder abusar sexualmente de él, entre otros; la forma más típica de suplantación de identidad es que el antisocial, crea un perfil falso en las redes sociales para poder comunicarse con otras personas.

La Revelación ilegal de base de datos, según el Art. 229 del Código Orgánico Integral Penal, estipula 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 (Código Orgánico Integral Penal, 2014, pág. 78).

El delito de revelación ilegal de base de datos, constituye un ilícito que se tipifica en el Art. 229 del Código Orgánico Integral Penal, donde se sanciona a quienes en provecho propio o de un tercero, revelen información confidencial existente en archivos, bases de datos u otros, los mismo que son enviados a otro sistema telemático, para que los ciberdelincuentes alteren el derecho a la intimidad de las personas involucradas.

El servidor público y los empleados bancarios deben ejercer sus funciones con lealtad institucional, rectitud y buena fe, en el momento que estos incurren en la intermediación financiera, sin importar que hayan causado daños al Estado, la sanción de este delito se agrava.

Por lo tanto, es obligación del Estado, garantizar las condiciones necesarias para proteger la información reservada e implementar medidas acertadas, que impidan la divulgación de las bases de datos.

De acuerdo con el Art. 230 del Código Orgánico Integral Penal, la Interceptación ilegal de datos, 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, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.
2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, 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 al que quiere acceder.
3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.
4. 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.
5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Código Orgánico Integral Penal, 2014, pág. 78).

El Art. 230 antes mencionado, nos explica sobre el delito de Interceptación ilegal de datos, donde el delincuente cibernético es aquel que posee ciertas características que no presentan el denominador común de los delincuentes, estos sujetos tienen habilidades para manejar los sistemas informáticos y que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter confidencial y privada, permitiéndoles el acceso a la base de datos, sistemas informáticos o dispositivos electrónicos, entre otros; apoderándose de la información para causar daños a través de la divulgación de la misma y beneficiarse de forma ilícita. Debemos tener en cuenta que los delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, por lo que, como ciudadanos responsables debemos tener la debida precaución para que nuestros derechos fundamentales no sean lesionados.

> El Art. 231 del Código Orgánico Integral, sobre la Transferencia electrónica de activo patrimonial, establece 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 (Código Orgánico Integral Penal, 2014, pág. 78-79).

El Art. 231, nos detalla el delito de transferencia de activo patrimonial donde una persona, se apropia de los bienes, valores y derechos de otra. Con la aparición del Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. El Internet si bien es de fácil acceso para las personas, también puede ser un peligro, porque los datos del usuario inevitablemente pueden ser recogidos por terceras personas, por lo que es elemental que la población tenga una adecuada información sobre la manera más eficaz de utilizar este avance tecnológico, logrando así prevenir los daños a los sistemas informáticos.

Además, este artículo nos menciona que se castigará a la persona titular de la información que haya revelado los datos de su cuenta bancaria a otra persona, con la finalidad de obtener una apropiación ilícita por los medios electrónicos, violentando la confidencialidad, la integridad, la disponibilidad de los sistemas informáticos, redes y datos informáticos.

> Según el Art. 232 del Código Orgánico Integral Penal, el Ataque a la integridad de sistemas informáticos, sucede cuando la persona destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.
>
> Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos,

programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.

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 (Código Orgánico Integral Penal, 2014, pág. 79).

Con respecto al Art. 232, sobre el ataque a la integridad de sistemas informáticos, podemos decir, que es todo tipo de destrucción, daño, borrado, deterioro, alteración del normal funcionamiento de un sistema informático, donde debemos considerar al daño informático no por el concepto de afectación a un bien mueble o inmueble, sino al que se produce al software o al hardware, que conforman el objeto material o elementos físicos de la informática, llamados también herramientas, base de datos, instalaciones o materias primas. El daño causado afectará de manera directa a las personas que poseen un sistema informático en la realización de sus actividades cotidianas, laborales, de estudio, entre otras, perjudicando con ello la autorrealización personal. Ante este tipo de delitos la ciudadanía en general debemos tomar las debidas precauciones en nuestros equipos tecnológicos para evitar los ataques informáticos.

De acuerdo con el Art. 233 del Código Orgánico Integral Penal, los Delitos contra la información pública reservada legalmente, se producen cuando la persona 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 (Código Orgánico Integral Penal, 2014, pág. 79).

El Art. 233 citado anteriormente, hace referencia a los delitos contra la información pública reservada legalmente, donde la persona que destruya información clasificada, poniendo

en peligro la seguridad del Estado, será sancionada por la ley penal vigente, garantizando de esta manera el contenido de la información, la integridad, confidencialidad y disponibilidad de datos.

El uso indebido del sistema informático ha dado lugar al surgimiento de comportamientos lesivos de bienes jurídicos produciéndose el delito, para prevenir este delito es primordial que se difunda ampliamente en todo el territorio nacional, por los medios de comunicación tanto escrita, televisión y redes sociales como Facebook, Instagram, Twitter, WhatsApp, entre otros, para que la ciudadanía ecuatoriana conozca de este delito y su penalización, ya que el conocimiento de las leyes y los diferentes ataques de que se puede ser víctima como usuarios de Internet podrá crear una cultura de manejo adecuado y responsable de la información.

> El Art. 234 del Código Orgánico Integral Penal, sobre el Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, establece:
>
> 1. 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 sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.
> 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, pág. 79).

El acceso no consentido a un sistema informático, descrito en el Art. 234, es un delito informático que se comete mediante el uso de dispositivos de comunicación como son el computador, Tablet, celular, entre otros. El acto delictivo mencionado anteriormente, lo que intenta es causar daño a la intimidad de las personas, obteniendo información privada, sin el consentimiento de las mismas, por lo tanto, este tipo de conducta antisocial es sancionada de conformidad a lo establecido en el Código Orgánico Integral Penal en vigencia, evitando con ello que los delincuentes cibernéticos sigan violentando de manera directa la confidencialidad de la información, permitiendo que las personas puedan tener acceso a las tecnologías de la información y la comunicación de manera libre y sin temor alguno.

El Código Orgánico Integral Penal, dentro del Art. 234.1 estipula la Falsificación informática, que señala:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.
2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena (Código Orgánico Integral Penal, 2014, pág. 80).

El Art. 234.1 del Código Orgánico Integral Penal, referente al delito de Falsificación Informática, el numeral 1 nos hace hincapié a la intención que tiene el delincuente informático para provocar un engaño en las relaciones jurídicas, llegando a trastocar el procedimiento utilizado en el campo de la informática, proponiendo de esta manera otros datos o documentos falsos.

El numeral 2 nos establece de forma clara cuando una persona actúa con el propósito de perjudicar, dañar o menoscabar, logrando de esta forma obtener un beneficio para sí mismo o para otra persona, a través de un instrumento de tipo digital que introduzca, modifique, elimine o suprima la información en el tratamiento de los datos existentes dentro de un sistema informático.

El Estado ecuatoriano para evitar lo delitos informáticos debe tomar medidas determinantes y drásticas, en contra de los ciberdelincuentes, para frenar los altos índices de conductas delictivas, además debe capacitar a la ciudadanía, brindándole información pertinente para identificar y prevenir las ciberamenazas y ciberataques existentes en el espacio digital.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	**ELEMENTOS DEL TIPO PENAL**		**UBICACIÓN:** **Delito de Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.**	**UBICACIÓN:** **Delito de Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.**	**UBICACIÓN:** **Delito de Violación a la intimidad.**
1	**OBJETIVIDAD JURÍDICA**		Integridad sexual y reproductiva.	Integridad sexual y reproductiva.	Intimidad personal y familiar.
2	**SUJETO ACTIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	**SUJETO PASIVO**	**General**			Cualquier Persona.
		Especial	Persona menor de dieciocho años.	Persona menor de dieciocho años.	
4	**ASPECTO SUBJETIVO**		Dolo.	Dolo.	Dolo.
5	**ASPECTO OBJETIVO**	**Verbo Rector**	Proponer.	Ofrecer.	Acceder, interceptar, examinar, retener, grabar, reproducir, difundir y publicar.
		Otros Aspectos complementarios	Concertar un encuentro con un menor de dieciocho años.	Servicios sexuales a menores de dieciocho años.	Datos personales, mensajes de datos, voz, audio y video.
6	**RESULTADOS**		Daño.	Daño.	Daño.
7	**OBJETO DE LA ACCIÓN**		Persona menor de dieciocho años.	Persona menor de dieciocho años.	Cualquier Persona.
8	**PRECEPTO LEGAL**		Art. 173 del COIP.	Art. 174 del COIP.	Art. 178 del COIP.
9	**SANCIÓN**	**Pena**	1 a 3 años de pena privativa de libertad.	7 a 10 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.
		Formas Atenuadas			
		Formas Agravadas	3 a 5 años de pena privativa de libertad por coacción o intimidación.		
			3 a 5 años de pena privativa de libertad por identidad falsa.		
		Otras Disposiciones del Tipo Penal			No son aplicables en grabaciones de audio y video en las que interviene personalmente.

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	**ELEMENTOS DEL TIPO PENAL**		**UBICACIÓN:** **Delito de Estafa.**	**UBICACIÓN:** **Delito de Apropiación fraudulenta por medios electrónicos.**	**UBICACIÓN:** **Delito de Reprogramación o modificación de información de equipos terminales móviles.**
1	**OBJETIVIDAD JURÍDICA**		La propiedad.	La propiedad.	La propiedad.
2	**SUJETO ACTIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	**SUJETO PASIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
4	**ASPECTO SUBJETIVO**		Dolo.	Dolo.	Dolo.
5	**ASPECTO OBJETIVO**	**Verbo Rector**	Inducir.	Facilitar.	Reprogramar y Modificar.
		Otros Aspectos complementarios	A error a otra persona.	Apropiación de un bien ajeno.	Información de identificación de los equipos terminales móviles.
6	**RESULTADOS**		Daño.	Daño.	Daño.
7	**OBJETO DE LA ACCIÓN**		Patrimonio.	Patrimonio.	Persona.
8	**PRECEPTO LEGAL**		Art. 186 del COIP.	Art. 190 del COIP.	Art. 191 del COIP.
9	**SANCIÓN**	**Pena**	5 a 7 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.
		Formas Atenuadas			
		Formas Agravadas	**Pena máxima:** Defraude mediante el uso de dispositivos electrónicos.		
		Otras Disposiciones del Tipo Penal		**La misma sanción por:** La inutilización de sistemas de alarma.	

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	ELEMENTOS DEL TIPO PENAL		UBICACIÓN: **Delito de Intercambio, comercialización o compra de información de equipos terminales móviles.**	UBICACIÓN: **Delito de Reemplazo de identificación de terminales móviles.**	UBICACIÓN: **Delito de Comercialización ilícita de terminales móviles.**
1	OBJETIVIDAD JURÍDICA		La propiedad.	La propiedad.	La propiedad.
2	SUJETO ACTIVO	General	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	SUJETO PASIVO	General	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
4	ASPECTO SUBJETIVO		Dolo.	Dolo.	Dolo.
5	ASPECTO OBJETIVO	Verbo Rector	Intercambiar, comercializar y comprar.	Reemplazar y Colocar.	Comercializar.
		Otros Aspectos complementarios	Base de Datos.	Etiquetas con información falsa.	Terminales móviles.
6	RESULTADOS		Daño.	Daño.	Daño.
7	OBJETO DE LA ACCIÓN		Persona.	Persona.	Persona.
8	PRECEPTO LEGAL		Art. 192 del COIP.	Art. 193 del COIP.	Art. 194 del COIP.
9	SANCIÓN	Pena	1 a 3 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.
		Formas Atenuadas			
		Formas Agravadas			
		Otras Disposiciones del Tipo Penal			

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	**ELEMENTOS DEL TIPO PENAL**		**UBICACIÓN:** **Delito de Infraestructura ilícita.**	**UBICACIÓN:** **Delito de Suplantación de identidad.**	**UBICACIÓN:** **Delito de Revelación ilegal de base de datos.**
1	**OBJETIVIDAD JURÍDICA**		La propiedad.	La identidad.	Seguridad de los activos de los sistemas de información y comunicación.
2	**SUJETO ACTIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	**SUJETO PASIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
4	**ASPECTO SUBJETIVO**		Dolo.	Dolo.	Dolo.
5	**ASPECTO OBJETIVO**	**Verbo Rector**	Poseer.	Suplantar.	Revelar.
		Otros Aspectos complementarios	Infraestructura.	Identidad de otra persona.	Información registrada.
6	**RESULTADOS**		Daño.	Daño.	Daño.
7	**OBJETO DE LA ACCIÓN**		Persona.	Persona.	Persona.
8	**PRECEPTO LEGAL**		Art. 195 del COIP.	Art. 212 del COIP.	Art. 229 del COIP.
9	**SANCIÓN**	**Pena**	1 a 3 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.	1 a 3 años de pena privativa de libertad.
		Formas Atenuadas			
		Formas Agravadas			3 a 5 años de pena privativa de libertad si es servidor público.
		Otras Disposiciones del Tipo Penal	No constituye delito, la apertura de bandas para operación de os equipos terminales móviles.		

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	**ELEMENTOS DEL TIPO PENAL**		**UBICACIÓN:** **Delito de Interceptación ilegal de datos.**	**UBICACIÓN:** **Delito de Transferencia electrónica de activo patrimonial.**	**UBICACIÓN:** **Delito de Ataque a la integridad de sistemas informáticos.**
1	**OBJETIVIDAD JURÍDICA**		Seguridad de los activos de los sistemas de información y comunicación.	Seguridad de los activos de los sistemas de información y comunicación.	Seguridad de los activos de los sistemas de información y comunicación.
2	**SUJETO ACTIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	**SUJETO PASIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
4	**ASPECTO SUBJETIVO**		Dolo.	Dolo.	Dolo.
5	**ASPECTO OBJETIVO**	**Verbo Rector**	Interceptar.	Manipular y modificar.	Obstaculizar.
		Otros Aspectos complementarios	Datos en forma ilegal.	Funcionamiento de programa o sistema informático.	De forma grave, deliberada el funcionamiento de un sistema informático.
6	**RESULTADOS**		Daño.	Daño.	Daño.
7	**OBJETO DE LA ACCIÓN**		Persona.	Persona.	Persona.
8	**PRECEPTO LEGAL**		Art. 230 del COIP.	Art. 231 COIP.	Art. 232 del COIP.
9	**SANCIÓN**	**Pena**	3 a 5 años de pena privativa de libertad.	3 a 5 años de pena privativa de libertad.	3 a 5 años de pena privativa de libertad.
		Formas Atenuadas			
		Formas Agravadas			5 a 7 años de pena privativa de libertad, si se comete sobre bienes informáticos de servicio público.
		Otras Disposiciones del Tipo Penal	1. Sin orden judicial previa. 2. Ilegítimamente diseñe. 3. Posea, Venda, distribuya. 4. Copiar, clonar, comercializar. 5. Producir, fabricar, distribuir.	Con igual pena quien facilite o proporcione datos de su cuenta bancaria.	Con igual pena quien diseñe o programe dispositivos.

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

TABLA DE LOS ELEMENTOS DEL TIPO PENAL DE LOS DELITOS INFORMÁTICOS.					
No.	**ELEMENTOS DEL TIPO PENAL**		**UBICACIÓN:** **Delitos contra la información pública reservada legalmente.**	**UBICACIÓN:** **Delito de Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.**	**UBICACIÓN:** **Delito de Falsificación informática.**
1	**OBJETIVIDAD JURÍDICA**		Seguridad de los activos de los sistemas de información y comunicación.	Seguridad de los activos de los sistemas de información y comunicación.	Seguridad de los activos de los sistemas de información y comunicación.
2	**SUJETO ACTIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
3	**SUJETO PASIVO**	**General**	Cualquier Persona.	Cualquier Persona.	Cualquier Persona.
		Especial			
4	**ASPECTO SUBJETIVO**		Dolo.	Dolo.	Dolo.
5	**ASPECTO OBJETIVO**	**Verbo Rector**	Destruir o Inutilizar.	Acceder.	Falsificar.
		Otros Aspectos complementarios	Información clasificada.	Sin consentimiento.	Falsificación informática.
6	**RESULTADOS**		Daño.	Daño.	Daño.
7	**OBJETO DE LA ACCIÓN**		Persona.	Persona.	Persona.
8	**PRECEPTO LEGAL**		Art. 233 del COIP.	Art. 234 del COIP.	Art. 234.1 del COIP.
9	**SANCIÓN**	**Pena**	5 a 7 años de pena privativa de libertad.	3 a 5 años de pena privativa de libertad.	3 a 5 años de pena privativa de libertad.
		Formas Atenuadas	3 a 5 años de pena privativa de libertad, si es servidor público.		
		Formas Agravadas	7 a 10 años de pena privativa de libertad, si es información reservada.		
		Otras Disposiciones del Tipo Penal			Con la misma pena, si usa un documento producido a partir de contenido digital.

Fuente: Código Orgánico Integral Penal.
Autora: Lizbeth Sofía Palacios Orellana.

4.4. La Ciberseguridad.

4.4.1. Definiciones de Ciberseguridad.

La ciberseguridad en la sociedad actual tiene gran relevancia, con la difusión y acceso a las Tecnologías de la Información y la Comunicación se incrementó el uso del ciberespacio a nivel mundial, razón por la cual, todos los países deben implementar la ciberseguridad, porque mientras avanza la tecnología más son los peligros que se encuentran en el mundo digital, exponiéndose de esta manera a los ataques cibernéticos.

En vista del gran problema social existente, es preciso establecer algunas definiciones entre ellas tenemos:

"La Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio" (Leiva, 2015, p. 2). Al referirnos a este tema de gran trascendencia, podemos decir, que la ciberseguridad se basa en detectar y prevenir los ciberataques a los sistemas informáticos, para ello debe existir una planificación y preparación, donde se incluyan métodos que ayuden a encontrarlos antes de que causen graves daños y afecten la integridad de las personas que utilizan los medios electrónicos para realizar sus actividades cotidianas.

"La ciberseguridad es la colección de herramientas, políticas, conceptos de seguridad, salvaguardas, guías, enfoques de gestión de riesgos, acciones, entrenamiento, mejores prácticas, seguridad y tecnologías, que pueden ser usadas para proteger los activos de la organización y de los usuarios dentro del ciberespacio" (Global Forum on Cyber Expertise, 2016:8*).* Con relación a la ciberseguridad, podemos decir, que esta tiene como fin proteger a los usuarios que navegan y realizan sus actividades a través del ciberespacio. Los Estados crean instrumentos de ciberseguridad, que permiten construir y fortalecer el desarrollo social, económico y humano de los mismos, logrando con ello ser más competitivos y aumentar sus ingresos.

"Usualmente se acepta que el objetivo de la ciberseguridad o seguridad informática es descubrir y aclarar la naturaleza de las amenazas y proveer metodologías para mitigarlas" (Barrantes, 2010, pág. 39). La ciberseguridad usa los mecanismos necesarios para garantizar la seguridad de la tecnología de la información, contra los riesgos existentes en el ciber entorno, por lo que esta herramienta busca defender las computadoras, los servidores, dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos, por lo que las

personas deben proteger sus dispositivos, logrando así evitar que se atenten contra los derechos del ser humano.

4.4.2. Ciberamenazas y Ciberataques.

Con el auge y evolución de la informática, se incrementa el riesgo del ciberespacio a través de las ciberamenazas y ciberataques, siendo estas las formas más usadas por los delincuentes; generando así los delitos informáticos que en el Ecuador se encuentran tipificados en el Código Orgánico Integral Penal, por lo que, debemos conocer más ampliamente estos dos términos:

Podemos definir las ciberamenazas, como "Aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción" (Ruiz, 2016, pág. 3). La ciberamenaza es una acción maliciosa que se realiza en el entorno digital, generando un impacto negativo en la seguridad de la información de una persona u organización, es considerada un riesgo latente en nuestra sociedad, ya que puede ejecutarse por medio de un ordenador de sobremesa, portátil, móvil, Tablet, etcétera; la protección ante este riesgo se logra implementando herramientas de ciberseguridad, para generar confianza a la población en el momento de utilizar dichos medios.

> Los ciberataques son el principal riesgo global de origen humano, con diversas consecuencias que casi siempre se traducen en interrupción de servicios, pérdidas económicas o daños a la reputación de la víctima. La gran mayoría persigue un fin económico, pero también hay algunas, que se realizan con fines activistas para obtener información sobre un adversario, otras como acciones integradas en un plan militar para el desarrollo de las operaciones (Cubeiro, 2021, pág. 1).

Se considera un ciberataque a cualquier práctica realizada por una persona u organización con la finalidad de infiltrar, atacar y ocasionar daños a los sistemas de información, dando como resultado que los datos y la información personal se divulguen y los delincuentes puedan acceder a la misma, poniendo en peligro y causando inimaginables pérdidas para la víctima, es así que todos debemos implementar en nuestros dispositivos medidas de ciberseguridad para contrarrestar y prevenir posibles ataques.

Después de analizar los conceptos, es preciso establecer la diferencia existente entre una ciberamenaza y un ciberataque.

La ciberamenaza es la acción que puede ocasionar un ataque en los sistemas de información, el mismo que es detectado por los usuarios, permitiendo de esta forma activar las herramientas de ciberseguridad para mantenerse protegidos. En cambio, un ciberataque ocurre cuando ya hubo una acción ofensiva en contra de un sistema computarizado, vulnerando la seguridad y poniendo en riesgo la información confidencial existente dentro del dispositivo electrónico.

Usar herramientas de ciberseguridad es necesario para que una empresa, nación o persona, pueda mantener sus datos e información confidencial segura y protegida de cualquier tipo de ciberataque, los mismos que aparecen en todo momento dentro del mundo digital.

4.4.3. Política Pública

Es importante hablar de las políticas públicas implementadas por el Estado ecuatoriano, en materia de ciberseguridad, porque gracias a estas se pueden encontrar las soluciones adecuadas para impedir los daños, que se producen en los sistemas de información que afectan de manera directa a las personas, empresas, organizaciones y el propio Estado.

Vargas (1999, p. 57), describe a la Política Pública como "la serie de sucesivas iniciativas, decisiones y acciones del régimen político frente a situaciones socialmente problemáticas buscando la resolución de las mismas o llevarlas a niveles manejables". La preocupación del Estado ecuatoriano frente a la violación de los sistemas informáticos, adopta una serie de soluciones, creando políticas públicas, con la intención de eliminar y mitigar este problema social, que hoy en día vulnera los derechos de miles de personas, que han sido afectadas por los delitos informáticos.

Bañón & Castro (2007, p. 2) explican las políticas públicas como "el conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que en un momento determinado los ciudadanos y el propio gobierno consideran prioritarios". Debemos tomar en cuenta que la creación de las políticas públicas son una solución a los múltiples problemas que se evidencian en la sociedad, donde el Estado en vista del alto riesgo existente hoy en día, se responsabiliza en prestar una atención inmediata a estos inconvenientes, generando mayor confiabilidad y seguridad a los ciudadanos.

Para entender de mejor manera a las políticas públicas, debemos tomar en cuenta lo que estipula la legislación ecuatoriana. La Constitución de la República del Ecuador, en el capítulo segundo nos detalla sobre las políticas públicas, servicios públicos y participación ciudadana.

El Art. 85, establece que la formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos que garanticen los derechos reconocidos por la Constitución, se regularán de acuerdo con las siguientes disposiciones:

1. Las políticas públicas y la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y todos los derechos, y se formularán a partir del principio de solidaridad.
2. Sin perjuicio de la prevalencia del interés general sobre el interés particular, cuando los efectos de la ejecución de las políticas públicas o prestación de bienes o servicios públicos vulneren o amenacen con vulnerar derechos constitucionales, la política o prestación deberá reformularse o se adoptarán medidas alternativas que concilien los derechos en conflicto.
3. El Estado garantizará la distribución equitativa y solidaria del presupuesto para la ejecución de las políticas públicas y la prestación de bienes y servicios públicos.

   En la formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos se garantizará la participación de las personas, comunidades, pueblos y nacionalidades (Constitución de la República del Ecuador, 2008, pág. 36).

Las políticas públicas son acciones del gobierno con objetivos de interés público, que surgen de decisiones sustentadas en un proceso de diagnóstico **y** análisis de factibilidad, para la atención efectiva de problemas públicos específicos, en donde participa la ciudadanía en la definición de problemas y soluciones.

Con base en lo anterior, las políticas públicas son acciones que permiten un mejor desempeño gubernamental, a partir de cuatro supuestos: el interés público, la racionalidad, la efectividad y la inclusión. Tales premisas se logran a través del uso racional de los recursos públicos, la focalización de la gestión gubernamental a problemas públicos acotados y la incorporación de la participación ciudadana.

El Estado ha constatado la necesidad de plantear políticas públicas como una herramienta de transformación de la sociedad con la colaboración de múltiples actores sociales, estas acciones públicas ayudarán a lograr un cambio en los comportamientos de las personas, solucionando los problemas que son considerados de atención prioritaria en un momento determinado.

4.4.4. Política Criminal.

> El autor Moisés Moreno considera que la política criminal que el Estado adopta para cumplir su función en materia criminal, tiene como objetivo primordial la lucha contra el delito para lograr la vida ordenada en comunidad; lo realiza previniéndolo o reprimiendo a través de una serie de medidas, estrategias, acciones o decisiones que el Estado adopta para enfrentar el problema de la delincuencia (Moreno, 2017, pág. 64).

La criminología en nuestros días ha incursionado en los medios de comunicación, siendo estos de carácter masivo, brindando información y contenidos a la población en general, por lo que es importante crear una Política Criminal que, a través de medidas y pautas jurídicas, sociales y educativas, permitan reaccionar y prevenir los diferentes delitos informáticos utilizados por los antisociales, que cada día son más comunes y evolucionan de forma acelerada, causando daño a las personas que utilizan la tecnología de forma constante.

> El Doctor Ernesto Albán Gomes menciona que, siendo el Derecho Penal finalista y valorativo, su misión es determinar qué bienes e intereses jurídicos merecen protección penal y consecuentemente qué conductas deben ser calificadas como delitos. Y esta tarea es parte esencial de la política criminal que una sociedad debe delinear conforme a la cual se criminaliza una conducta, o se la despenaliza; se aumentan o disminuyen las penas, según sea necesario para garantizar con eficacia tales bienes e intereses. Por eso es tan directa la vinculación entre la parte especial y la política criminal (Albán, 2015, Pág. 59).

El Estado debe garantizar a los ecuatorianos una política criminal enfocada en la investigación científica del delito y de la eficacia de la pena, como una herramienta de lucha contra el crimen organizado, la delincuencia, las ciberamenazas, los ciberataques y los diferentes delitos informáticos, con el fin de controlar y prevenir los actos delictivos, utilizando estrategias, instrumentos y acciones penales que sancionen estas conductas antijurídicas, emitiendo las penas correspondientes de acuerdo a cada delito cometido, para así mitigar la creciente ola de criminalidad existente en nuestro país, que perjudica enormemente el desempeño eficaz de cada persona.

Actualmente existe una nueva reforma a la Ley de Seguridad Pública y del Estado de fecha 29 de marzo de 2023, que plantea un capítulo innumerado denominado Consejo Nacional de Política Criminal, que a continuación lo mencionaré:

> El Art. 10.1. señala que el Consejo Nacional de Política Criminal es el organismo interinstitucional encargado de aprobar la política criminal, articulada al Plan Nacional de Seguridad Integral del Estado.
>
> La política criminal es el conjunto de respuestas que el Estado adopta, de manera integral e intersectorial, para prevenir y enfrentar la delincuencia y criminalidad con el fin de garantizar la protección de los intereses esenciales del Estado y los derechos de sus habitantes (Ley de Seguridad Pública y del Estado, 2009, pág. 6-7)

La actual reforma a la Ley de Seguridad Pública y del Estado, nos hace referencia a la creación del Consejo Nacional de Política Criminal, con la finalidad que se aprueben las políticas criminales más adecuadas para manejar la delincuencia y la criminalidad existente en nuestro país, encontrando soluciones para minimizar los delitos cometidos por los antisociales, los mismos que están tipificados y sancionados en el Código Orgánico Integral Penal vigente. Con ello la población ecuatoriana podrá estar prevenida y protegida de cualquier tipo de delitos, que afectan a los Derechos Humanos fundamentales, pertenecientes a cada ser humano, donde se garantice el Buen Vivir o Sumak Kawsay, logrando de esta forma una vida digna, en armonía y equilibrio con el universo y la sociedad.

4.4.5. Política y Estrategia de Ciberseguridad en Ecuador.

La Política y Estrategia Nacional de Ciberseguridad han sido implementadas para evitar y prevenir los delitos informáticos que ahora son muy comunes, debido a la dependencia digital de la sociedad, la creciente sofisticación de la tecnología y su uso generalizado que ha dado lugar a amenazas más complejas; actualmente las personas tienen la necesidad de usar los medios electrónicos para realizar múltiples actividades de la vida diaria, es aquí donde la delincuencia informática se propaga de forma acelerada y la población está más expuesta a ser víctima de estos actos delictivos.

En el año 2021, se aprobó nuestra primera Política Nacional de Ciberseguridad, publicada mediante Acuerdo Ministerial 006-2021, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información en base a los artículos 3; 66 numeral 19 y 21; 85 numeral 1; 154 numeral 1; 226; 227; 261 numeral 10; 280; 313; 314 inciso segundo de la Constitución de la República del Ecuador, los mismos que determinan los deberes primordiales y derechos que el Estado reconoce y garantiza a las personas, así como la ejecución, evaluación y control de las políticas públicas y servicios públicos a través de las

ministras y ministros de Estado. Así mismo en base al artículo 1, 3 numeral 1, 88, 140, 141 numeral 2 de la Ley Orgánica de Telecomunicaciones, que establece el objeto y los objetivos de las telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado, que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional y del artículo 6 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos.

> La Política Nacional de Ciberseguridad en el Art. 2, estipula que el objetivo de la política es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio. La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una confianza digital que favorece el intercambio de información y, en consecuencia, de bienes y servicios en línea. La política tiene un enfoque multisectorial y multidimensional que se debe al carácter transversal de la ciberseguridad. Por tanto, la política alcanza a varios sectores y actores, públicos y privados, del país, y de manera vertical y horizontal. En esta medida, la política establece directrices para encaminar las acciones de las entidades de la Administración Pública Institucional y que dependen de la Función Ejecutiva, en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general. (Política Nacional de Ciberseguridad, 2021, pág. 4).

El Art. 2 de la Política Nacional de Ciberseguridad, nos hace hincapié en la construcción y fortalecimiento de las capacidades nacionales, cuyo fin es tener el pleno ejercicio de nuestros derechos y libertades consagradas en la Constitución de la República del Ecuador, así como también la protección de los bienes jurídicos del Estado dentro del ciberespacio, haciendo del mismo, un lugar seguro para interactuar sin limitación alguna y sin miedo a ser víctima de los delitos informáticos, permitiendo de esta manera el desarrollo social, económico y humano del Ecuador. Hoy en día el mundo digital, el trabajo, la comunicación, los negocios, las transacciones nacionales e internacionales, son cada vez más necesarias, por lo tanto, es importante tener una seguridad informática confiable, donde las políticas, estrategias y procedimientos fundamentales creados por el Estado, nos ayuden a evitar los posibles ataques y amenazas existentes en el ciberespacio. La Política de Ciberseguridad está dirigida a varios sectores y actores, públicos y privados, dentro del país, cuyas directrices están dirigidas al accionar de las entidades de la Administración Pública Institucional dependientes de la Función

Ejecutiva, y que están en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general.

La Política Nacional de Ciberseguridad fue planteada por el gobierno del Presidente Lenin Moreno, cuya línea de acción fue el fortalecimiento institucional y la articulación efectiva, de forma ordenada, con un enfoque integral y la activa presencia de múltiples actores con el fin de alcanzar un Ecuador Digital Ciberseguro, que garantice el Estado de Derecho, proteja los servicios e infraestructuras críticas del Estado y de seguridad a la población en el ciberespacio.

Con el fin de alcanzar un Ecuador Digital Ciberseguro, que garantice el Estado de Derecho, proteja los servicios e infraestructuras críticas del Estado y de seguridad a la población en el ciberespacio, el gobierno trazó su línea de acción asentada en 7 pilares: 1) Gobernanza de ciberseguridad; 2) Sistemas de información y gestión de incidentes; 3) Protección de servicios e infraestructuras críticas digitales; 4) Soberanía y defensa; 5) Seguridad pública y ciudadana; 6) Diplomacia en el ciberespacio y cooperación internacional; 7) Cultura y educación de ciberseguridad.

Los principios en los que se fundamenta esta política son la promoción y el respeto de los derechos humanos y libertades fundamentales, el fomento de la confianza, la resiliencia, la responsabilidad compartida, el desarrollo de actividades en el entorno digital y el mercado nacional de las Tecnologías de la Información y la Comunicación. En el marco de un Internet libre, abierto y seguro, donde se prioriza la comunicación de las personas, la protección de datos y el derecho a la privacidad.

La Política Nacional de Ciberseguridad solucionó en parte el problema social de la ciberdelincuencia, concientizó a la sociedad ecuatoriana sobre las vulnerabilidades que enfrentaba el entorno cibernético, sin embargo, el mayor uso de la Internet implicó un aumento en la vulnerabilidad de la ciudadanía que hace uso de esta herramienta, tanto en lo profesional como en lo cotidiano. El aprovechamiento de estas vulnerabilidades en el ciberespacio por parte de actores delictuales, se ha convertido en una nueva forma de atentar contra los derechos de las personas.

Actualmente, con el fin de mejorar la resiliencia cibernética de la sociedad ecuatoriana, se incorporó la nueva Estrategia Nacional de Ciberseguridad, que se elaboró con cooperación de actores nacionales e internacionales para los próximos tres años (2022-2025), con la

existencia de una política de ciberseguridad, que permitirá a los ciudadanos acceder a servicios digitales con mayor seguridad, fortalecer la protección de sus datos personales y de órganos nacionales pertinentes, como el Comité Nacional de Ciberseguridad, quien aprobó la Estrategia Nacional de Ciberseguridad y el EcuCERT, que es el Centro de Respuesta a Incidentes Informáticos a la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador.

Con el desarrollo de las tecnologías de comunicaciones, los ciudadanos, empresas y Estados afrontan notables retos de ciberseguridad. Las ciberamenazas y ciberataques tienen efectos directos en la seguridad de las personas, la economía y las tecnologías de la información.

El gobierno del Presidente Guillermo Lasso dentro del Plan de Creación de Oportunidades 2021-2025, establece que se debe garantizar la soberanía nacional, integridad territorial y seguridad del Estado, donde se propone entender a la seguridad desde una nueva concepción que tendrá un alcance multidimensional, ya que el mundo está sujeto a varios cambios en diversos ámbitos: por ejemplo, el tecnológico, donde se han incrementado algunas amenazas, como los ciberataques, que afectan la defensa y seguridad de un estado, por esta razón se establecen estrategias, planes y acciones para enfrentar lo que amenaza la seguridad del Ecuador.

La Estrategia Nacional de Ciberseguridad vigente en nuestro país, contempla varios principios rectores que guían el desarrollo y la aplicación de esta Estrategia, entre ellos nos referiremos a: 1. Liderazgo y responsabilidad compartida, es por el cual se garantiza una colaboración, cooperación eficaz y efectiva en la gestión de riesgos de ciberseguridad, así como también en la asignación y entrega de recursos que ayudarán a mermar los delitos informáticos. 2. Salvaguardar los derechos digitales de las personas que se relacionan con la información y la comunicación. 3. Gestión de riesgos de ciberseguridad y resiliencia cibernética, donde las personas, empresas e instituciones realicen sus actividades de forma libre, confiable, segura en las plataformas y aplicaciones digitales. 4. Visión inclusiva y colaborativa, este principio compromete a la sociedad civil, entidades públicas y privadas, para crear estrategias, políticas y soluciones con el fin de mejorar las condiciones existentes en el ciberespacio y poder actuar de manera segura en el mismo.

Por otro lado, la estrategia, se articula en torno a seis pilares de los cuales se derivan y definen los Objetivos Estratégicos de la Estrategia Nacional de Ciberseguridad del Ecuador:

1. Gobernanza y coordinación nacional: Establecer un enfoque coordinado de la ciberseguridad nacional.
2. Resiliencia cibernética: Mejorar la resiliencia cibernética a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos.
3. Prevención y lucha contra la cibercriminalidad: Fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos.
4. Ciberdefensa nacional: Reforzar las capacidades de ciberdefensa para proteger las Infraestructuras de Información Crítica nacionales y los servicios esenciales del Estado y desarrollar capacidades en ciber inteligencia que permitan obtener información útil y oportuna de las amenazas presentes en ciberespacio para la toma de decisiones
5. Habilidades y capacidades de ciberseguridad: Mejorar y ampliar las habilidades y Objetivos estratégicos capacidades cibernéticas de la nación en todos los niveles.
6. Cooperación internacional: Maximizar los beneficios de la cooperación internacional (Estrategia Nacional de Ciberseguridad del Ecuador, 2022, pág.14).

Dentro de la Estrategia Nacional de Ciberseguridad, se han planteado varios pilares, los cuales se derivan y definen los objetivos estratégicos de la misma, donde se determina la importancia de la ciberseguridad, la situación actual, los problemas y desafíos prioritarios, que hay que tomar en cuenta con los objetivos estratégicos y las líneas de acción, que acompañan a las medidas y tareas que hay que cumplir para apaliar a este tipo de delitos, que lo único que hacen es atemorizar y amedrentar a la población que utiliza los medios informáticos.

Actualmente en el Ecuador, se ha incrementado notablemente los delitos informáticos, donde las ciberamenazas y ciberataques son muy constantes y peligrosos, perjudicando la defensa y seguridad de un país. Es por ello, que el Estado ha elaborado estrategias, planes y acciones para salvaguardar los derechos de las personas y no permitir que estos delitos queden en la impunidad.

Estadísticamente Ecuador es uno de los tres países latinoamericanos con más ciberataques, luego de Brasil y México, esto según las cifras de la empresa de seguridad cibernética Kaspersky, donde más de dos millones de ataques cibernéticos han sido reportados entre agosto de 2022 y agosto de 2023, con esto podemos evidenciar que las amenazas a los dispositivos móviles, está cada vez en aumento, ocasionando grandes pérdidas en las personas afectadas, es por esto que se necesita incrementar la ciberseguridad en nuestra sociedad

ecuatoriana, a través de la difusión de información, otorgando los mejores mecanismos de prevención e identificación de las vulnerabilidades existentes en el espacio digital.

4.5. Víctima.

Hablar de víctima es muy importante dentro del Derecho Penal, por lo que es preciso entender, primeramente, cuál es su definición, para en la vida cotidiana poder identificarla, es por esto que a continuación detallaré a varios autores:

> Víctima es la persona que sufre los efectos del delito, no solo el sujeto pasivo o titular del bien jurídico, que es la víctima más directa, sino también otros perjudicados materiales o morales, directos o indirectos, como familiares, herederos, la empresa, sus integrantes y acreedores, etcétera (Diccionario panhispánico del español jurídico, 2022, pág. 1).

Del concepto de víctima podemos entender, que es la persona que sufre las consecuencias del delito, hay que considerar que no solo se refiere a quien recibe el daño de manera directa, sino también de manera general, a todas las personas que han sido perjudicadas, como consecuencia de los hechos victimizantes, limitando de esta manera el ejercicio de los derechos fundamentales propios de cada ser humano.

Se entiende por "víctima" a todo aquel que sufre un daño por acción u omisión propia o ajena, o por causa fortuita (Rodríguez, 2002, pág. 25). Como lo señala el autor es toda persona que padece el resultado de las conductas dañosas que producen un delito, las mismas que afectan al ser humano en su desarrollo personal, social, psicológico, es decir en todos los ámbitos de su vida.

> La víctima es una persona de cualquier sexo que ha sufrido una lesión ilegítima en sus bienes jurídicos tutelados. En tal sentido, es una persona que ha sufrido la desprotección del sistema de seguridad pública, debido a la imposibilidad física de la vigilancia y cuidado total por parte del aparato estatal (Moscoso, 2016, pág. 20).

Como señala el autor, víctima es aquella persona que ha sido afectada en sus bienes jurídicos tutelados, establecidos en la normativa legal, quedando de esta manera sin la protección del Estado, como ente encargado de tutelar el correcto desarrollo de los derechos del ser humano; por lo tanto, los delitos cometidos por los que infringen la norma, ocasionan graves consecuencias, convirtiéndolas a las mismas en víctimas de estas conductas punitivas.

Guillermo Cabanellas, define a la víctima como:

- Persona que sufre violencia injusta en su persona o ataque en sus derechos.
- El sujeto pasivo del delito y de la persecución indebida.
- Quien sufre un accidente casual, de que resulta su muerte u otro daño en su persona y perjuicio en sus intereses.
- Quien se expone a un grave riesgo por otro (Cabanellas, 2006, pág. 490).

El destacado jurista español, en su definición de víctima, hace referencia al individuo que recibe un daño en su persona, en sus intereses y sus derechos humanos tutelados por la normativa legal correspondiente, como es en nuestro país, la Constitución de la República del Ecuador; también concibe a la víctima como el sujeto pasivo del delito cometido, siendo el infractor sancionado de acuerdo a la conducta delictiva perpetrada.

4.5.1. Victimología.

La Victimología se originó alrededor de los años 40 del siglo XX, sus primeros precursores que iniciaron el estudio científico de la Victimología fueron: Benjamín Mendelsohn con su obra "Le Victimologie" y a Hans Von Hentig con su obra "The criminal and his victims", seguidos de Henry Ellenberger con su obra "Relations Psychologiques et la Victime". Los mismos que consideraban importante la actuación de la víctima dentro del proceso judicial y planteaban que el Estado debía interesarse por ella para encontrar la Justicia.

Benjamín Mendelsohn inició el primer estudio científico acerca de la Victimología, indicando que es una ciencia que se encarga del estudio de la víctima. Tanto Mendelsohn como Von Hentig señalaron la relación que existe entre víctima y victimario. Mencionaban el desinterés que existía por parte del Estado hacia la víctima, donde se enfocaba únicamente en el criminal y en la pena que sería impuesta.

El objetivo de Benjamín Mendelsohn al realizar sus estudios, era lograr que existan menos víctimas en los delitos, a su vez, consideraba que no se puede exigir Justicia, sin la previa participación de la víctima como principal titular del bien o derecho violentado.

Por otra parte, Henry Ellenberger, estableció características objetivas y subjetivas que poseen las víctimas, determinando de esta forma el grado de participación de las víctimas en el delito cometido, pretendía con ello enseñar a las personas a no ser víctimas.

La victimología ha ido evolucionando constantemente, ahora es considerada como una ciencia, donde se analiza las conductas, factores y circunstancias de la víctima, con el objeto de brindarle una prevención y tratamiento eficaz, que repare de alguna manera el delito cometido contra ella.

La victimología se centra principalmente en la conducta, en las características de la víctima y sus relaciones e interacciones con sus victimarios. Desde una visión más amplia, el concepto de víctima se profundiza en los daños producidos a una persona que pueden ser físicos, psicológicos, económicos o patrimoniales, es decir, en todos sus derechos humanos, estén o no jurídicamente protegidos por el Estado.

La víctima es el eje principal de la victimología, donde la víctima es el individuo o grupo que padece un daño, por acción u omisión propia o ajena, o por causa fortuita. Su estudio se centra en la persona que sufre el perjuicio en sus bienes jurídicamente protegidos, como la vida, salud, propiedad, honor, honestidad, etcétera.

4.5.2. Clasificación de víctima.

De acuerdo con el Reglamento para el Sistema de Protección a Víctimas, Testigos, dentro del Título II, Capítulo II, el Art. 8 Definiciones, el numeral 1, nos especifica las clases de víctima, como son directa e indirecta, que se detallarán a continuación:

> **Víctima directa. -** Es toda persona que haya sufrido daños, individual o colectivamente, incluidas lesiones físicas o mentales, sufrimiento emocional, pérdidas económicas o menoscabo sustancial de sus derechos fundamentales, como consecuencia de acciones u omisiones que constituyan la consumación de un delito.
>
> **Víctimas indirectas. -** En caso de familia inmediata o las personas a cargo de la víctima directa; y, las personas que hayan sufrido daños al intervenir para prestar asistencia a víctimas en peligro o para impedir la victimización, que cuenten con un riesgo potencial o real, de acuerdo a lo dispuesto en el presente Reglamento (Reglamento para el Sistema de Protección a Víctimas, Testigos, 2018, pág. 6-7).

Con respecto a la clasificación de la víctima, antes mencionada, podemos indicar que se hace una distinción, entre lo que es una víctima directa y una víctima indirecta. Se puede considerar que víctima directa es el ofendido, sujeto pasivo del delito, titular del bien jurídico

lesionado por la infracción. Por otro lado, víctima indirecta, son las personas vinculadas con la víctima por lazos familiares o afectivos.

Entonces podemos decir, que el concepto de víctima no se refiere únicamente a quien sufre de manera directa el perjuicio, daño o lesión a sus derechos fundamentales, sino también, ocasiona afectación a las víctimas indirectas, como son los familiares directos, cónyuges, los hijos, personas que dependan, convivan o se encuentren en una relación de efectividad con la víctima.

4.5.3. Víctima de acuerdo con la Constitución de la República del Ecuador.

La Constitución de la República del Ecuador en su cuerpo normativo, se refiere a la víctima en el título II Derechos, Capítulo octavo Derechos de Protección en su Art. 78, que se detalla a continuación:

> Las víctimas de infracciones penales gozarán de protección especial, se garantizará su no revictimización, particularmente en la obtención y valoración de las pruebas, y se las protegerá de cualquier amenaza u otras formas de intimidación. Se adoptarán mecanismos para una reparación integral que incluirá, sin dilaciones, el conocimiento de la verdad de los hechos y la restitución, indemnización, rehabilitación, garantía de no repetición y satisfacción del derecho violado. Se establecerá un sistema de protección y asistencia a víctimas, testigos y participantes procesales (Constitución de la República del Ecuador, 2008, pg. 34).

En la Constitución ecuatoriana, la víctima del delito es protegida por el Estado, actualmente la víctima tiene un papel fundamental en el proceso penal, que radica en la reparación integral de la misma, la restitución, indemnización, rehabilitación, garantía de no repetición y satisfacción del derecho violado, considerando que no se revictimice al sujeto pasivo del delito, logrando con ello combatir el daño causado por los delincuentes.

4.5.4. Víctima según lo establecido en el Código Orgánico Integral Penal.

En el Código Orgánico Integral Penal, en el título III denominado Derechos, encontramos en el capítulo primero los Derechos de la víctima, el Art. 11, señala que, en todo proceso penal, la víctima de las infracciones gozará de los siguientes derechos:

1. A proponer acusación particular, a no participar en el proceso o a dejar de hacerlo en cualquier momento. En ningún caso se obligará a la víctima a comparecer.
2. A la adopción de mecanismos para la reparación integral de los daños sufridos que incluye, sin dilaciones, el conocimiento de la verdad de los hechos, el restablecimiento del derecho lesionado, la indemnización, la garantía de no repetición de la infracción, la satisfacción del derecho violado y cualquier otra forma de reparación adicional que se justifique en cada caso.
3. A la reparación por las infracciones que se cometan por agentes del Estado o por quienes, sin serlo, cuenten con su autorización.
4. A la protección especial, resguardando su intimidad y seguridad, así como la de sus familiares y sus testigos.
5. A no ser revictimizada, en la obtención y valoración de las pruebas, incluida su versión. Se la protegerá de cualquier amenaza u otras formas de intimidación, se podrán utilizar medios tecnológicos.
6. A ser asistida por un defensor público o privado antes y durante la investigación, en las diferentes etapas del proceso y en lo relacionado con la reparación integral.
7. A ser asistida gratuitamente por un traductor o intérprete, si no comprende o no habla el idioma en el que se sustancia el procedimiento, así como a recibir asistencia especializada.
8. A ingresar al Sistema nacional de protección y asistencia de víctimas, testigos y otros participantes del proceso penal, de acuerdo con las disposiciones de este Código y la ley.
9. A recibir asistencia integral de profesionales adecuados de acuerdo con sus necesidades durante el proceso penal.
10. A ser informada por la o el fiscal de la investigación preprocesal y de la instrucción.
11. A ser informada, aun cuando no haya intervenido en el proceso, del resultado final, en su domicilio si se lo conoce.
12. A ser tratada en condiciones de igualdad y cuando amerite, aplicar medidas de acción afirmativa que garanticen una investigación, proceso y reparación, en relación con su dignidad humana.

    Si la víctima es de nacionalidad distinta a la ecuatoriana, se permitirá su estadía temporal o permanente dentro del territorio nacional, por razones humanitarias y personales, de acuerdo con las condiciones del Sistema nacional de protección y asistencia de víctimas,

testigos y otros participantes del proceso penal (Código Orgánico Integral Penal, 2014, pág. 10-11).

En nuestra legislación vigente no existe un concepto de víctima, de acuerdo al Código Orgánico Integral Penal, la víctima es un sujeto procesal junto con la persona procesada, la fiscalía y la defensa, esto quiere decir que tiene un papel fundamental y sin la cual no se puede realizar un proceso penal, su participación no es obligatoria y puede dejar de hacerlo en cualquier momento.

Es preciso indicar que el Código Orgánico Integral Penal, es el encargado de normar el poder punitivo del Estado, tipificar las infracciones penales, propone un procedimiento de juzgamiento de las personas procesadas, además fomenta la rehabilitación social de los sentenciados y promueve la reparación integral de las víctimas que han sufrido daños.

Al referirnos a la reparación integral, podemos indicar que es el conjunto de medidas impuestas sobre el victimario y destinadas a la víctima, para disminuir los efectos producidos o que se desencadenaron a raíz del cometimiento de una infracción penal, tratando de restituir de manera representativa y material el ilícito cometido.

En la actualidad, los delitos penales crecen de una forma exponencial, así como el derecho va evolucionando, también lo hacen las distintas conductas delictivas, donde los delincuentes con el uso de las nuevas tecnologías, buscan delinquir sin tomar en cuenta los daños que pueden ocasionar a sus víctimas, afectando de esta forma su integridad personal.

Así mismo, el Título III Sujetos Procesales, en el Capítulo Segundo del Código Orgánico Integral Penal nos hace referencia a la Víctima, dentro del Art. 441, se considera víctima, para efectos de aplicación de las normas de este Código, a las siguientes personas:

1. Las personas naturales o jurídicas y demás sujetos de derechos que individual o colectivamente han sufrido algún daño a un bien jurídico de manera directa o indirecta como consecuencia de la infracción.
2. Quien ha sufrido agresión física, psicológica, sexual o cualquier tipo de daño o perjuicio de sus derechos por el cometimiento de una infracción penal.
3. La o el cónyuge o pareja en unión libre, incluso en parejas del mismo sexo; ascendientes o descendientes dentro del segundo grado de consanguinidad o primero de afinidad de las personas señaladas en el numeral anterior.

4. Quienes compartan el hogar de la persona agresora o agredida, en casos de delitos contra la integridad sexual y reproductiva, integridad personal o de violencia contra la mujer o miembros del núcleo familiar.
5. La o el socio o accionista de una compañía legalmente constituida que haya sido afectada por infracciones cometidas por sus administradoras o administradores.
6. El Estado y las personas jurídicas del sector público o privado que resulten afectadas por una infracción.
7. Cualquier persona que tenga interés directo en caso de aquellas infracciones que afecten intereses colectivos o difusos.
8. Las comunidades, pueblos, nacionalidades y comunas indígenas en aquellas infracciones que afecten colectivamente a los miembros del grupo.

   La condición de víctima es independiente a que se identifique, aprehenda, enjuicie, sancione o condone al responsable de la infracción o a que exista un vínculo familiar con este (Código Orgánico Integral Penal, 2014, pág. 147).

Podemos indicar, que víctima es la persona que recibe un daño o perjuicio ocasionado por otra, es a quien se le vulnera un bien jurídico protegido, de manera directa o indirecta como consecuencia de la infracción. El sujeto que sufre un delito, es considerado víctima del hecho recibido; en nuestra legislación vigente, se brinda protección ante cualquier amenaza u otras formas de intimidación y se garantiza la reparación integral a la misma, con el fin de resarcir los daños ocasionados.

En el Derecho Penal, las víctimas son las personas naturales o jurídicas y demás sujetos de derechos, el socio o accionista, el Estado, así como las comunidades, pueblos, nacionalidades y comunas indígenas, entre otros; es decir es aquel que sufre un daño, el mismo que puede ser físico, moral, material o psicológico. Por lo tanto, se considera como víctima al sujeto procesal, individuo o colectividad, que padece una lesión en su integridad física, psíquica, social o económica a consecuencia del cometimiento de un delito que se encuentra tipificado en la ley.

En cuanto a la persona infractora, que ha sido sentenciada por un delito, debe resarcir los daños causados a la víctima, logrando con ello que la afectación ocasionada sea menor. Cuando no es posible revertir el daño, debe ser sustituido por una indemnización de carácter pecuniario.

4.5.5. Reparación Integral de la Víctima.

La reparación integral de la víctima establecida en el Código Orgánico Integral Penal, es una solución que el juzgador impone de acuerdo con la gravedad del daño sufrido, con la finalidad de minimizar los efectos de las violaciones cometidas por los antisociales.

En el Título III Reparación Integral, Capítulo Único denominado Reparación Integral, encontramos los siguientes artículos que hablan sobre este tema:

> El Art. 77 sobre la Reparación integral de los daños, menciona que, la reparación integral radicará en la solución que objetiva y simbólicamente restituya, en la medida de lo posible, al estado anterior de la comisión del hecho y satisfaga a la víctima, cesando los efectos de las infracciones perpetradas. Su naturaleza y monto dependen de las características del delito, bien jurídico afectado y el daño ocasionado. La restitución integral constituye un derecho y una garantía para interponer los recursos y las acciones dirigidas a recibir las restauraciones y compensaciones en proporción con el daño sufrido (Código Orgánico Integral Penal, 2014, pág. 35).

En este artículo, podemos constatar que la reparación integral, es una medida impuesta por el Estado, la cual está enfocada en dar una solución al titular del bien jurídico afectado, la cual ayudará a remediar de alguna forma, las afectaciones causadas por el cometimiento de conductas delictivas, que son contrarias a lo que establece la ley. La víctima tiene como derecho una restitución integral, donde se le entregará una restauración y compensación acorde a los daños ocasionados, logrando de esta manera que los efectos producidos por la infracción penal sean minimizados, brindándole a la víctima la tranquilidad deseada por haber encontrado justicia.

> El Art. 78 sobre los Mecanismos de reparación integral, establece las formas no excluyentes de reparación integral, individual o colectiva, que son:

1. La restitución: se aplica a casos relacionados con el restablecimiento de la libertad, de la vida familiar, de la ciudadanía o de la nacionalidad, el retorno al país de residencia anterior, la recuperación del empleo o de la propiedad, así como al restablecimiento de los derechos políticos.
2. La rehabilitación: se orienta a la recuperación de las personas mediante la atención médica y psicológica, así como a garantizar la prestación de servicios jurídicos y sociales necesarios para esos fines.

3. Las indemnizaciones de daños materiales e inmateriales: se refieren a la compensación por todo perjuicio que resulte como consecuencia de una infracción penal y que sea evaluable económicamente.
4. Las medidas de satisfacción o simbólicas: se refieren a la declaración de la decisión judicial de reparar la dignidad, la reputación, la disculpa y el reconocimiento público de los hechos y de las responsabilidades, las conmemoraciones y los homenajes a las víctimas, la enseñanza y la difusión de la verdad histórica.
5. Las garantías de no repetición: se orientan a la prevención de infracciones penales y a la creación de condiciones suficientes para evitar la repetición de las mismas. Se identifican con la adopción de las medidas necesarias para evitar que las víctimas sean afectadas con la comisión de nuevos delitos del mismo género (Código Orgánico Integral Penal, 2014, pág. 35).

El Art. 78 del Código Orgánico Integral Penal, establece los mecanismos que pueden ser aplicados por el operador de justicia con la víctima.

La reparación integral se enmarca en un contexto jurídico muy amplio, con respecto a la restitución, es aplicable para restaurar los derechos, que fueron lastimados en el momento de la ejecución de un delito, a través de elementos, instrumentos o componentes fundamentales en atención a resarcir el daño producido en una persona.

La rehabilitación es también un mecanismo de reparación, donde se garantiza que la víctima vuelva a estabilizarse y recobrar su estilo de vida que llevaba anteriormente, permitiendo que tenga una asistencia médica, psicológica, jurídica y social que beneficien su recuperación.

Se establece una compensación pecuniaria, por las afectaciones causadas por el delincuente, quien deberá entregar una indemnización proporcional al perjuicio ocasionado a la víctima, tratando de restituir de manera representativa y material lo dañado.

Con la finalidad de aliviar en la víctima, su dignidad y reputación lesionadas, la ley establece mecanismos de satisfacción, por medio de diferentes formas como los homenajes, conmemoraciones, entre otros, que ayuden a mitigar en la medida de lo posible, las consecuencias desfavorables que hayan marcado a una persona en cuanto a ser víctima del delito.

Además, la normativa penal vigente, ha creado las garantías de no repetición, para impedir que las víctimas no vuelvan a ser afectadas, por el cometimiento de una infracción penal.

La legislación ecuatoriana, establece estos mecanismos de reparación como respuesta a la búsqueda de que se repare, subsane, restablezca a la víctima su derecho violentado y los daños ocasionados por los infractores de la ley.

4.6. Prevención delictiva para combatir los Delitos Informáticos.

4.6.1. La Prevención delictiva desde el punto de vista doctrinario y jurídico.

Este tema es de suma importancia para contrarrestar los delitos informáticos, por lo cual es preciso destacar algunos puntos de vista doctrinarios, entre ello tenemos:

La prevención del delito es el "conjunto de medidas e indicadores elaborados por el Estado, las organizaciones políticas y de masas, organismos o entidades estatales para minorizar el delito, sus causas y consecuencias, neutralizando sus efectos" (Viera, M.: Ídem, p.106). La prevención delictiva comprende un complejo sistema o red de medidas, cuyo contenido varía de acuerdo a la esfera social hacia la que van dirigidas, previniendo el delito, así como sus causas y consecuencias.

La Organización de las Naciones Unidas (2013) indica que la prevención del delito supone "estrategias y medidas encaminadas a reducir el riesgo de que se produzcan delitos y sus posibles efectos perjudiciales para las personas y la sociedad, incluido el temor a la delincuencia, y a intervenir para influir en sus múltiples causas" (2013, párr. 3). El mecanismo que el Estado establece en su normativa legal para prevenir los delitos, es creado con el fin de lograr que los actos antijurídicos realizados no se vuelvan a repetir en la sociedad, minimizando de esta forma los riesgos ocasionados y el alto índice de las conductas delictivas existentes en el Ecuador.

La Constitución de la República del Ecuador, como ley suprema del ordenamiento jurídico, hace mención a la prevención del delito, de la siguiente forma:

> El Art. 163, establece que la Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional. Los

> miembros de la Policía Nacional tendrán una formación basada en derechos humanos, investigación especializada, prevención, control y prevención del delito y utilización de medios de disuasión y conciliación como alternativas al uso de la fuerza. Para el desarrollo de sus tareas la Policía Nacional coordinará sus funciones con los diferentes niveles de gobiernos autónomos descentralizados (Constitución de la República del Ecuador, 2008, pág. 80).

El Art. 163, anteriormente descrito resalta la importancia que tiene la Policía Nacional como institución que protege los derechos, libertades y garantías de los ciudadanos, a través del control y prevención de los delitos, donde existe la confianza, transparencia, credibilidad y legitimidad ante la ciudadanía, de acuerdo a los componentes de gestión preventiva como: el servicio a la comunidad, investigación de la infracción, inteligencia anti delincuencial, gestión operativa, control y evaluación. En nuestro país se ha observado un alto índice de delitos informáticos y un incremento de personas antisociales, por lo que la Policía Nacional debe promover diversos programas de prevención social del delito e incluyan estrategias y medidas que disminuyan el riesgo de que se produzcan los delitos y sus efectos que son perjudiciales para las personas y la sociedad en general.

4.6.2. La prevención como mecanismo para combatir las ciberamenazas y ciberataques.

4.6.2.1. Prevención según la Policía Nacional del Ecuador.

La Policía Nacional del Ecuador, con la finalidad de prevenir las conductas delictivas por los medios electrónicos, en su página virtual, nos brinda algunos aspectos a seguir, que son:

- Tener un antivirus (con licenciamiento) instalado, activo y actualizado.
- Navegar y descargar software sólo desde sitios web oficiales.
- Antes de enviar sus datos en una web, compruebe que ésta comience por https://. Es una Web segura.
- Ante la menor sospecha, borré el mensaje, esto es extensivo a correos, páginas web, mensajes SMS, WhatsApp, en cualquier sitio o lugar, no se fie, y menos en el trabajo.
- No publicar información personal en páginas desconocidas o redes sociales.
- No confiar en ofertas y precios muy bajos al comprar cualquier servicio.
- Crear contraseñas seguras.
- No compartir con otras personas claves de seguridad.
- No guardar contraseñas en computadores públicos para evitar las estafas.
- Verificar las cuentas bancarias en computadores personales.

- Conservar los mensajes, correos electrónicos y toda información indebida, los mismos que servirán en caso de que sea necesario denunciar ante las autoridades.
- No confiar en correos electrónicos desconocidos.
- Supervisar constantemente cuando un menor de edad se encuentra en la red.
- Revise siempre el remitente, si tiene alguna duda de quién le envía un mail, póngase en contacto con esa persona por otro canal (teléfono, por ejemplo) para verificar que es quien está enviando.
- Evitar hacer clic en ventanas, adjuntos y enlaces sin conocer su verdadero origen.
- Desestimar las advertencias sobre actualizaciones o publicidades engañosas.
- Desconfiar de mensajes de sitios web ofreciendo solucionar un virus de tu dispositivo con el mensaje “haciendo clic aquí” (Policía Nacional del Ecuador, 2019, pág. 1).

La Policía Nacional del Ecuador, en vista de la gran cantidad de conductas delictivas en el campo informático, ha elaborado mecanismos para prevenir ser víctimas de los delitos informáticos, de los ataques a los sistemas y la información; tomando en cuenta que los virus que ingresan a los sistemas informáticos, hacen daño en forma silenciosa, perjudicando al usuario y a la sociedad en general. La Policía Nacional enfrenta este acto delincuencial brindando información y recomendaciones a través de su Plan Rescate Ecuador, para evitar que las personas sean sujetos pasivos de este tipo de delitos y proteger la información personal, tomando en cuenta que es el bien jurídico protegido más preciado de todo ser humano, institución, empresa e incluso del Estado, por lo tanto, es obligación de todos aprender a cuidarla frente a los ciberdelincuentes.

4.6.2.1.1. Prevención ante los ciberdelitos en el Ecuador.

El Ing. Héctor Gonzalo García Cataña, Teniente Coronel de Policía, jefe de la Unidad Nacional de Ciberdelito, en la página del Gobierno Electrónico del Ecuador, por el Día del Internet Seguro presentó algunas alternativas para prevenir los delitos informáticos y evitar ser víctimas de estos actos delictivos, las mismas que se detallan a continuación:

- Mantén tus equipos y aplicaciones actualizadas incluyendo navegador, antivirus y sistema operativo.
- Preste especial atención si un correo electrónico te solicita información confidencial ejemplo la contraseña de tu cuenta bancaria, o datos personales.
- Ten mucho cuidado con la información que compartes en las redes sociales y en las páginas de contacto.

- No hagas clic en enlaces adjuntos o imágenes que recibas en mensajes de texto no solicitados, sin antes verificar el remitente.
- Evita compartir tu información personal como: fechas de nacimiento, dirección de domicilio y número celular.
- No aceptes contactos desconocidos en tus perfiles de las diferentes redes sociales
- Contacta personalmente con tu familiar o amigo, mediante una llamada telefónica si te piden ciertas cantidades de dinero o solicitan colaboración para retirar encomiendas.
- Si no logras contactarte con tu familiar o amigo, contáctate con un familiar cercano para verificar la información.
- No realices ningún depósito hasta no verificar que la información sea real.
- Si eres vendedor verifica que el depósito esté en tu cuenta y también consulta con tu banco de confianza que el pago esté realizado.
- Investiga antes de comprar cualquier producto mediante las diferentes plataformas.
- Verifica que exista una dirección física, correo electrónico y/o teléfonos reales para cualquier duda o problema al hacer una compra (Unidad Nacional de Ciberdelitos, 2022, pág. 15-16).

Como sabemos los delitos informáticos son actividades ilícitas, donde su medio de consumación son los dispositivos tecnológicos y de comunicación, cuyo objetivo es causar daño, provocar pérdidas o impedir el uso de los sistemas informáticos; evitarlos es tarea de todos los usuarios que poseemos un ordenador, Tablet, teléfono u otros medios informáticos. Con respecto a la prevención de los ciberdelitos, el Teniente Coronel de Policía, jefe de la Unidad Nacional de Ciberdelito, nos indica que debemos actuar con cautela, prudencia, no confiar en personas desconocidas, ni revelar información confidencial en las redes sociales, que es preciso acudir de manera inmediata a la Policía Nacional, para que sean ellos quienes intervengan y establezcan la ayuda necesaria para impedir que los antisociales realicen este tipo de conductas ilícitas y no ser víctimas de estos delitos.

4.6.2.2. Tips de Ciberseguridad de acuerdo al Ministerio de Telecomunicaciones y de la Sociedad de la Información.

4.6.2.2.1. ¿Cómo protegerse ante Cibercriminales?

El cibercrimen se ha manifestado de muchas maneras y formas, desde que existen los ordenadores y con la creciente disponibilidad de internet en los años recientes, la naturaleza del

crimen cibernético ha evolucionado. Por ello, es indispensable conocer las siguientes medidas de prevención:

- Utilizar contraseñas robustas (mayúsculas, minúsculas, números, símbolos).
- No usar contraseñas recicladas (la misma contraseña para distintos accesos).
- Utilizar preguntas de seguridad complejas.
- Si es posible, aplicar doble factor de autenticación.
- Tener conciencia de la información que se está exponiendo a Internet.
- Revisar quién está detrás de un perfil a través de confirmación de imágenes.
- Desactivar permisos de acceso no deseados de aplicaciones en dispositivos móviles (uso de cámara, ubicación, contactos, micrófono, etc.).
- Utilizar bóvedas digitales seguras para guardar contraseñas.
- Utilizar información ficticia para preguntas secretas.
- Desconfiar de todo correo que solicite información personal o contraseñas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022, pág. 3).

La prevención que debemos tener ante los cibercriminales es muy importante, para ello debemos hacer hincapié, que un cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red. La mayor parte del cibercrimen, está cometido por cibercriminales que desean ganar dinero, dañar computadoras o redes. Actualmente los cibercriminales utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas, por lo que los usuarios, debemos protegernos con técnicas de ciberseguridad para prevenir los delitos informáticos**,** con el fin de precautelar el derecho a la información y evitar pérdidas importantes de datos confidenciales. Hay que tener presente, que a medida que la tecnología avanza, surgen cada vez más formas de cometer delitos informáticos; por tal razón, tenemos que aprender a identificarlos para no ser víctimas de estas conductas antisociales.

4.6.2.2.2. Viajar Ciberseguro.

En el momento de viajar debemos tener en cuenta los principios básicos de ciberseguridad, evitando de esta forma cualquier tipo de problema, para ello el Ministerio de Telecomunicaciones y de la Sociedad de la Información, nos sugiere las siguientes medidas:

- Respaldar información crítica.
- No llevar información importante si no se va a utilizar.

- Tener en cuenta que los hackers atacan en lugares concurridos como aeropuertos, restaurantes, plazas y demás, mediante un acceso a una red inalámbrica que tiene el mismo nombre que una guardada en el dispositivo de la víctima (ejemplo: casa, familia, oficina, etc.).
- Apagar el Wifi de tu dispositivo si no lo estás utilizando.
- Revisar si se está conectando a la red inalámbrica correcta.
- Preguntar por la red inalámbrica oficial en cada localidad.
- Si se desconecta de una red inalámbrica, siempre seleccionar la opción “olvidar red” (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022, pág. 5).

Cuando una persona se encuentra en el aeropuerto, en un hotel, en un autobús o en el aire, los viajeros deben ser tan cuidadosos con su seguridad digital, como lo son con su seguridad personal. Comúnmente se ha podido observar, que las personas bajan la guardia cuando viajan y no controlan su entorno en el que se encuentran, deberían considerar que tienen información importante dentro de sus dispositivos electrónicos y que pueden ser usados por un delincuente. Por esta razón, tomar medidas de ciberseguridad, son muy necesarias para cuando viajamos, donde el objetivo primordial es que los dispositivos conectados a Internet estén seguros, esto se aplicará durante la planificación del viaje, el traslado y también cuando la persona ya se encuentra en el destino. Una ciberseguridad eficaz, servirá para ser menos vulnerables a los ciberataques existentes en el espacio digital.

4.6.2.2.3. Respaldar Información.

El respaldo de la información es un tema crucial para la protección de la información y prevención de los delitos informáticos, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, nos plantea las siguientes acciones que debemos tener en cuenta:

1. Utilizar plataformas de respaldo de información empresarial.
2. Mantener respaldo en más de un sitio o aplicativo seguro.
3. Contar con procedimientos de respaldo y planes de recuperación de información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022, pág. 6).

Otro mecanismo de prevención es el respaldo de información que consiste en realizar un duplicado de la misma, es llamado también copia de seguridad. Los respaldos permiten cierta protección contra errores en el sistema informático, virus, ciberamenazas, ciberataques,

etcétera. Cualquier persona que utilice una computadora, sea ésta personal o de oficina, un celular, Tablet u otros dispositivos informáticos, debe preguntarse si su información está realmente a salvo, para evitar que los equipos y dispositivos móviles se infecten, pues los delincuentes cibernéticos cuentan con herramientas sofisticadas para realizar sus actos delictivos y llevarse la información.

4.6.2.2.4. Recomendaciones para usar Dispositivos Electrónicos.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información, nos brinda una serie de recomendaciones para evitar los delitos informáticos, cuando usamos los dispositivos electrónicos, entre ellos tenemos:

- Actualizar el sistema operativo, antivirus.
- Activar el firewall (denominado también cortafuegos, bloquea accesos no autorizados) de windows.
- Mantener los dispositivos bloqueados y con contraseña.
- Crear un perfil de usuario para Teletrabajo.
- Respaldar la información constantemente.
- Borrar archivos innecesarios del ordenador.
- Evitar la instalación de aplicaciones sospechosas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022, pág. 6).

Hoy en día, existen muchos dispositivos digitales, incluidos teléfonos, tabletas y relojes inteligentes, que se utilizan para el tratamiento de datos digitales. Los datos digitales son información que se encuentra en formato digital, que se puede codificar y almacenar en dispositivos electrónicos como computadoras, discos duros, dispositivos de almacenamiento externos, entre otros. Estos datos pueden ser de diversos tipos, como texto, imágenes, sonido, vídeo, etcétera, los mismos que se pueden procesar, transmitir, almacenar y compartir mediante dispositivos tecnológicos y redes de comunicación, razón por la que debe existir una prevención eficiente, para evitar que se cometan los delitos informáticos y la información sea resguardada de forma confiable.

4.6.2.2.5. Recomendaciones para usar Internet y navegación.

Para usar el Internet y la navegación, en el ciberespacio, debe existir un conocimiento adecuado, para evitar los riesgos en el momento de abrir las páginas web. Para ello, es indispensable tener en cuenta las siguientes medidas de prevención:

- Verifica que la conexión a tu módem de internet no tenga adulteraciones.
- Realiza un test de velocidad y verifica que sea la contratada. Link para realizar el test: https://www.speedtest.net/es
- Si presentas lentitud en el servicio solicitar a tu proveedor de internet que revise el estado de la conexión, verifica el número de equipos conectados y actualiza la clave de tu red WI-FI.
- De preferencia conéctate mediante cable a internet.
- Evita conectarte a redes de internet que desconozcas, públicas o que te permita el acceso sin contraseña ya que pueden robar información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022, pág. 8).

Navegar por el Internet y las redes sociales pertenece a nuestro día a día, tiene ventajas y facilidades para los usuarios, pero también involucra muchos riesgos, donde la tecnología se presta para el cometimiento de delitos informáticos, por tal razón es fundamental implementar acciones que disminuyan el riesgo de ser víctimas de dichos actos. A través de la navegación segura, los usuarios pueden acceder al Internet con la certeza de que su información no será transgredida y que sus derechos serán respetados. Para prevenir los delitos informáticos se debe implementar en la ciudadanía una cultura de ciberseguridad, con el fin de identificar las distintas formas de cometimiento y buscar los mecanismos de defensa, evitando con ello, que los riesgos informáticos se propaguen.

4.7. Derecho Comparado de las Políticas y Estrategias Nacionales de Ciberseguridad.

En los últimos años se ha detectado un constante incremento de vulnerabilidades y amenazas sobre el denominado ciberespacio, este problema se extiende a todos los países del mundo por lo que se han creado Políticas y Estrategias de Ciberseguridad en cada uno de ellos, para entender de mejor manera este tema nos afianzaremos en el Derecho Comparado de:

4.7.1. Estrategia Nacional de Ciberseguridad de República Dominicana.

La Estrategia Nacional de Ciberseguridad de República Dominicana 2021-2024, proyecta los objetivos y líneas de acción que el Estado Dominicano tiene para alcanzar, desarrollar, fomentar y fortalecer el ecosistema de ciberseguridad, atendiendo a los Objetivos de Desarrollo Sostenible y a los indicadores internacionales de desarrollo y buenas prácticas en materia de ciberseguridad.

En República Dominicana, de acuerdo a las informaciones de los organismos nacionales de investigación de crímenes y delitos de alta tecnología, los delitos son cometidos a través de las infraestructuras informáticas y de telecomunicaciones, entre ellos están: robos de identidad, clonaciones de tarjetas de crédito, estafas, fraudes a través de internet, abuso sexual de niños, niñas y adolescentes, pornografía infantil, violencia contra las mujeres, difamación e injuria en redes sociales, la interrupción de servicios de las Tecnologías de la Información y las Comunicaciones, la manipulación fraudulenta de las conexiones telefónicas, el sabotaje y secuestro de centrales telefónicas privadas.

Desde el 2003, el gobierno dominicano ha desarrollado un marco legislativo con las mejores prácticas internacionales, para la penalización de la delincuencia cibernética y el manejo de evidencia electrónica, la regulación del envío de correo electrónico comercial no solicitado (SPAM) y el establecimiento de un marco de cooperación internacional. Las entidades que trabajan en ciberseguridad, están integradas en la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología, creada por la Ley 53-07.

El Estado en el año 2018, promulgó el decreto No. 230-18, creando el Centro Nacional de Ciberseguridad y estableció la Estrategia Nacional de Ciberseguridad.

El Presidente, Luis Abinader, en el marco de las políticas públicas, ha creado mediante la promulgación del decreto No. 71-21, el Gabinete de Transformación digital, cuya responsabilidad era elaborar la “Agenda Digital”, que define la Estrategia Nacional de Transformación Digital, cuyo objetivo es promover el desarrollo digital de la República Dominicana, a través del aprovechamiento de las tecnologías digitales en un marco de sostenibilidad e inclusión social, con la participación de los sectores público, privado, academia y sociedad civil.

Citando el artículo No. 1, párrafo II, de este decreto, la Agenda Digital promoverá la competitividad del país a través del desarrollo y fortalecimiento de la infraestructura digital, el desarrollo de competencias digitales en la población y el tejido productivo, la inversión, el emprendimiento e innovación tecnológica, la generación de empleos, el desarrollo de la economía digital, la eficiencia de la administración pública, el fortalecimiento de la transparencia, la rendición de cuentas y la participación de la ciudadanía, en consonancia con lo establecido por la Estrategia Nacional de Desarrollo 2030 y los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

Como eje transversal de la Agenda Digital, establece las líneas de acción para mitigar el riesgo, minimizar el impacto de las amenazas cibernéticas y proteger los sistemas de información y con atención especial las infraestructuras críticas nacionales y tecnologías de la información relevantes del Gobierno.

República Dominicana avanza en su misión y logra los objetivos de ciberseguridad, de acuerdo con los siguientes principios rectores: 1. Priorización de riesgos, 2. Rentabilidad, 3. Innovación y agilidad, 4. Colaboración, 5. Enfoque global, 6. Renta variable equilibrada y 7. Valores nacionales.

Esta Estrategia cuenta con cuatro pilares: 1) Marco Legal y Fortalecimiento Institucional, 2) Protección de Infraestructuras Críticas Nacionales e Infraestructuras de las tecnologías de la información del Gobierno, 3) Educación y Cultura Nacional de Ciberseguridad y 4) Alianzas Nacionales e Internacionales.

Cada uno de estos pilares, tiene sus respectivos objetivos que son:

1. Fortalecer el marco legal que incide en los temas relacionados con la ciberseguridad, las capacidades de las unidades especializadas y competentes para prevenir, investigar y decidir sobre crímenes y delitos de alta tecnología.
2. Asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y de la Tecnología de la Información relevantes del Gobierno y la protección de la información contenida en las mismas.
3. Fomentar la inclusión y formación en ciberseguridad en todos los niveles del sistema educativo e impulsar una cultura nacional de ciberseguridad.
4. Establecer alianzas nacionales e internacionales entre los sectores público-privado-sociedad civil y organismos e instituciones internacionales.

Después de revisar la Estrategia Nacional de Ciberseguridad de República Dominicana, podemos señalar que ha sido elaborada, por el uso masivo de las Tecnologías de la Información y la Comunicación, por las amenazas cibernéticas que han puesto en riesgo los sistemas de información y los servicios esenciales de ese país, afectando de forma grave la economía, la sociedad y la seguridad nacional.

Por tal razón, la Estrategia busca la protección de las redes y sistemas de información públicos y privados, estableciendo mecanismos de ciberseguridad que resguarden al Estado, a los ciudadanos y a los sectores productivos.

La República Dominicana pretende llegar a tener en el 2030, un ciberespacio más seguro, implementado medidas necesarias para el desarrollo confiable de las actividades productivas de la población, donde exista el respeto a los Derechos Humanos.

La Estrategia de Ciberseguridad, cuenta con principios rectores, cuyo fin es proteger el ecosistema de ciberseguridad de la República Dominicana, de los riesgos sistémicos, amenazas y vulnerabilidades de seguridad cibernética, así como la privacidad, los derechos y libertades civiles.

También plantea varios pilares, donde exista el diálogo y cooperación entre todos los sectores de la sociedad, mejorando la interacción, reconociendo los problemas existentes y solucionando las amenazas cibernéticas.

En Ecuador, la Estrategia Nacional de Ciberseguridad 2022-2025, se establece con el fin de mejorar la ciberseguridad y la resiliencia cibernética, así como minimizar los altos índices de delitos informáticos que ocurren en el país, que afectan a las personas, instituciones públicas y privadas e incluso al Estado.

En relación a los principios rectores, la Estrategia Nacional de Ciberseguridad de República Dominicana, enfatiza la priorización de riesgos, pretendiendo proteger el ecosistema de ciberseguridad de las amenazas y vulnerabilidades de la seguridad cibernética. Así mismo, propone la colaboración, donde el trabajo es colaborar con sus componentes, con otros socios federales y no federales. Ecuador tiene aspectos similares, su Estrategia Nacional de Ciberseguridad, se basa en la gestión de riesgos de ciberseguridad y resiliencia cibernética, que permite a las personas, empresas e instituciones desarrollar sus actividades de forma libre, confiable y segura en el entorno digital. De igual manera establece una visión inclusiva y colaborativa que involucra activamente a la sociedad civil, academia, entidades públicas y privadas.

Dentro de los pilares, la Estrategia Nacional de Ciberseguridad de República Dominicana, busca tener alianzas nacionales e internacionales, estableciendo marcos de cooperación técnica, operativa y de capacitación para luchar contra la ciberdelincuencia. En Diciembre de 2022, se firmó un acuerdo de cooperación interinstitucional para trabajar en favor de la Estrategia Nacional de Ciberseguridad, entre el Sistema Nacional de Atención a Emergencias y Seguridad 911 y el Centro Nacional de Ciberseguridad (CNCS), por otro lado el Centro Nacional de Ciberseguridad de República Dominicana en Agosto de 2023, firmó un memorando de entendimiento de cooperación en seguridad cibernética con el Ministerio de

Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica y con el Centro Nacional de Ciberseguridad de Panamá, para facilitar la cooperación bilateral al intercambiar información sobre Políticas de Ciberseguridad y mejores prácticas para fortalecer el ciberespacio a nivel global. La cooperación internacional ha sido un factor clave para el desarrollo digital y de ciberseguridad de este país, tiene el respaldo de múltiples países como Estonia, Unión Europea, la Red 24/7 del G8 y la Agenda Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones.

Ecuador en su Estrategia Nacional de Ciberseguridad, busca la cooperación internacional para gestionar los riesgos de ciberseguridad, fortalecer y racionalizar su participación en la respuesta bilateral, regional e internacional a incidentes cibernéticos y en la lucha contra las amenazas en el ciberespacio. Hasta el momento tenemos el apoyo del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, de la Organización de los Estados Americanos (CICTE/OEA) y del Proyecto de Resiliencia Cibernética para el Desarrollo de la Unión Europea (CYBER4DEV).

4.7.2. Estrategia Nacional de Ciberseguridad de España.

La Estrategia Nacional de Ciberseguridad 2019, establece la posición de España, frente a la nueva concepción de ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad de España, para hacer frente al desafío de la vulnerabilidad del ciberespacio y diseñar el modelo de gobernanza para la ciberseguridad nacional, contribuyendo a la promoción de un ciberespacio seguro y confiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional, su tarea es coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad.

En el 2015, se publicó la modificación del Esquema Nacional de Seguridad, para asegurar los sistemas del sector público. Con la vigencia del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La Ley 36/2015, de 28 de septiembre, se promulgó para impulsar la Seguridad Nacional.

En la Estrategia de Seguridad Nacional 2017, la ciberseguridad ocupa un espacio propio y diferencial, donde la digitalización, implica la seguridad; se basa en cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad

Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España.

La nueva ciberseguridad, se extiende más allá del campo de la protección del patrimonio tecnológico como es en las esferas política, económica y social.

La Estrategia Nacional de Ciberseguridad 2019, desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017, en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas.

La Estrategia Nacional de Ciberseguridad, se estructura en cinco capítulos:

1. "El ciberespacio, más allá de un espacio común global": Proporciona una visión del ámbito de la ciberseguridad, los avances realizados en materia de ciberseguridad desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

   La tecnología e infraestructura, que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio, uno de los principales riesgos para el desarrollo de la nación.
2. "Las amenazas y desafíos en el ciberespacio": Determina las amenazas del ciberespacio, que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad, que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: las que amenazan a activos que forman parte del ciberespacio; y aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.
3. "Propósito, principios y objetivos para la ciberseguridad": Aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia).
4. "Líneas de acción y medidas": Las líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio; impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención

de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

5. "La ciberseguridad en el Sistema de Seguridad Nacional": Define la estructura orgánica de la ciberseguridad, bajo la dirección del Presidente del Gobierno, se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas, entre estas y el sector privado y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, gestionará las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad, sobre aspectos relativos a la valoración técnica, operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes, el CSIRT (Computer Security Incident Response Team) de referencia nacional y se incorpora el Foro Nacional de Ciberseguridad.

La Estrategia Nacional de Ciberseguridad de España, frente al desafío que ha representado para el país, la vulnerabilidad del ciberespacio, ha planteado varias directrices y líneas generales de actuación, donde las autoridades buscan garantizar a la población española un ciberespacio seguro y confiable.

El Gobierno Español, considera al ciberespacio como un vector de comunicación estratégico en la opinión pública, le interesa la forma de pensar de cada uno de los ciudadanos y le preocupa la manipulación que tenga la información, los efectos causados en los sistemas digitales y las constantes amenazas informáticas existentes en el ciberespacio, ha determinado que la mejor solución es que exista una colaboración público-privada, como elemento clave para minimizar estos problemas.

Con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos, la gestión de crisis, la cultura de seguridad nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España, implementa una matriz estratégica, donde la ciberseguridad está enfocada a contrarrestar los problemas informáticos, que vulneran a la población en general.

En Ecuador, la Estrategia Nacional de Ciberseguridad, se ha planteado debido a la creciente dependencia digital de la sociedad, la sofisticación de la tecnología y el uso generalizado que la población mantiene constantemente, experimentado amenazas más especializadas, que ponen en peligro la información, la confidencialidad y el respeto a la utilización de las tecnologías de la información y las comunicaciones, por lo tanto, existe la necesidad de mejorar la ciberseguridad y la resiliencia cibernética en el país.

La Estrategia Nacional de Ciberseguridad en Ecuador, está basada en varios pilares fundamentales, en cada pilar, se identifica un resumen de la importancia de la ciberseguridad, la situación actual, los problemas y desafíos prioritarios que se deben abordar, los objetivos estratégicos y las líneas de acción que acompañan a las medidas y tareas que hay que cumplir para mejorar el ciberespacio. En cambio, la Estrategia Nacional de Ciberseguridad de España, se centra en capítulos, algunos de ellos abordan los propósitos, principios, objetivos, líneas de acción y medidas a tomarse en cuenta frente a los problemas informáticos, otros capítulos determinan la importancia del ciberespacio, las ciberamenazas y desafíos, así como la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional, todo esto con el propósito, de brindar seguridad nacional a los sistemas informativos en el ámbito público y privado.

4.7.3. Política Nacional de Ciberseguridad de Chile.

Michelle Bachelet, Presidenta de la República de Chile, en su programa de gobierno consideró el desarrollo de una Estrategia de Seguridad Digital, para proteger a usuarios privados y públicos en el ámbito digital. La idea fue refrendada en noviembre del 2015, con la Agenda Digital 2020, que consideró necesario elaborar una Estrategia de Ciberseguridad.

Esta primera Política Nacional fue construida con el diálogo público-privado, se recibió en audiencia pública a representantes de servicios públicos, de organizaciones gremiales y de la sociedad civil, además de académicos y expertos nacionales e internacionales. En el año 2015, mediante el Comité Interministerial de Ciberseguridad, se empezó a elaborar la primera

Política Nacional de Ciberseguridad del país, después se dio un proceso de consulta ciudadana que se llevó a cabo entre febrero y marzo del año 2016.

La Política Nacional 2017- 2022, planteó metas y compromisos concretos con el objetivo de promover un ciberespacio libre, abierto, seguro y resiliente, que permitió a los chilenos alcanzar el mayor desarrollo posible. En línea con la Agenda Digital y la Agenda de Productividad, Innovación y Crecimiento, permitió reducir las brechas de acceso y se llegó a concientizar sobre el uso seguro de las Tecnologías de la Información y las Comunicaciones.

Si bien la Política Nacional de Ciberseguridad aborda la persecución y sanción de los ciberdelitos, esta va más allá del ámbito punitivo, es catalogada como una variable fundamental para disminuir los riesgos asociados al ciberespacio y aprovechar sus potencialidades a través de la sensibilización, formación y difusión de ciberseguridad en la ciudadanía. Así mismo, la Política busca promover el desarrollo industrial y productivo en ciberseguridad.

Además, la Política plantea cinco objetivos estratégicos a largo plazo, para abordar los desafíos que como país enfrenta ante el ciberespacio, incorporando el ámbito de acción del Estado, el rol del sector privado, la sociedad civil y el mundo académico.

La Política Nacional de Ciberseguridad, contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2022, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente.

De acuerdo a los riesgos existentes en Chile, se creó esta Política, donde los ciberdelitos cometidos confirman el carácter transnacional de éstos, como el uso fraudulento de tarjetas de crédito y débito, estafas informáticas, los accesos o robos de información desde computadores o dispositivos infectados, entre otros.

La Política de Ciberseguridad tiene dos componentes centrales: una Política de Estado, diseñada con objetivos orientados al año 2022 y una Agenda de Medidas Específicas, que serán implementadas entre los años 2017 y 2018. El objeto es proponer una visión general a mediano y largo plazo. El Gobierno chileno en materia digital ha elaborado un conjunto de políticas como son: Agenda Digital 2020, Política Nacional de Ciberdefensa y Política Internacional para el Ciberespacio.

La Política Nacional de Ciberseguridad de Chile, cuenta con objetivos fundamentales para el año 2022, que son:

A. El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos, donde detalla: 1. Concepto. Identificación y gestión de riesgos, 2. Protección de la infraestructura de la información, 3. Identificación y jerarquización de las infraestructuras críticas de la información, 4. Contar con equipos de respuesta a incidentes de ciberseguridad, 5. Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes y 6. Exigencia de estándares diferenciados en materia de ciberseguridad.
B. El Estado velará por los derechos de las personas en el ciberespacio, donde plantea: 1. Prevención de ilícitos y generación de confianza en el ciberespacio, 2. Establecimiento de prioridades en la implementación de medidas sancionatorias, 3. Prevención multisectorial y 4. Respeto y promoción de derechos fundamentales.
C. Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales, hace énfasis en: 1. Una cultura de la ciberseguridad, 2. Sensibilización e información a la comunidad y 3. Formación para la ciberseguridad.
D. El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales, donde se tomará en cuenta: 1. Principios de política exterior chilena, 2. Cooperación y asistencia, 3. Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas y 4. Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio.
E. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos, basándose en: 1. Importancia de la innovación y desarrollo en materia de ciberseguridad, 2. Ciberseguridad como medio para contribuir al desarrollo digital de Chile, 3. Desarrollo de la industria de ciberseguridad en Chile, 4. Contribuir a la generación de oferta por parte de la industria local y 5. Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado.

En Chile la Política Nacional de Ciberseguridad, pretende garantizar plenamente los derechos del ser humano en el ciberespacio, implementar y poner en marcha las medidas que sean necesarias, para proteger la seguridad de los usuarios del espacio cibernético, considerando estrategias educativas orientadas al autocuidado y prevención en ambiente digital.

El programa de Gobierno de la Presidenta Michelle Bachelet, propuso desarrollar una Estrategia de Seguridad Digital, que proteja a los usuarios privados y públicos de las amenazas existentes por el uso de la tecnología.

La Política Nacional de Ciberseguridad se encuentra distribuida en diversos organismos y entidades, donde es necesario, la coordinación estratégica de los distintos esfuerzos, de sus roles y funciones, así como, el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia en el ámbito de la ciberseguridad, centrándose en la seguridad y libertad, en el combate a los ciberdelitos y otras amenazas en Internet.

Ecuador, ha visto la necesidad de elaborar una Política y Estrategia Nacional de Ciberseguridad, con la finalidad de hacer frente a los delitos informáticos, las ciberamenazas y ciberataques, que hoy en día se encuentran afectando la integridad de las personas, las instituciones públicas y privadas, así como del Estado.

En Ecuador, la Estrategia Nacional de Ciberseguridad 2022-2025, está articulada en base a seis pilares, de los cuales se derivan y definen los objetivos estratégicos, entre ellos tenemos: 1. Gobernanza y coordinación nacional, 2. Resiliencia cibernética, 3. Prevención y lucha contra la cibercriminalidad, 4. Ciberdefensa nacional, 5. Habilidades y capacidades de ciberseguridad y 6. Cooperación internacional, los mismos que ayudarán a contrarrestar el alto índice de los ataques cibernéticos existentes en nuestro país.

La Estrategia Nacional de Ciberseguridad de Chile, pone mayor énfasis en desarrollar una cultura de ciberseguridad en torno a la educación, con el objeto que la sociedad cuente con las herramientas y el conocimiento para entender las relaciones humanas, sus ventajas, oportunidades y riesgos, y pueda manejarlos adecuadamente. Actualmente se ha realizado propuestas por parte del equipo de especialistas que conforman la Mesa de Ciberseguridad de Chile, para que exista educación básica, media, superior y continua en el campo de la ciberseguridad, para generar conciencia nacional sobre las vulnerabilidades, a las que se encuentra expuesto el ser humano con el uso de los medios digitales.

En la Estrategia Nacional de Ciberseguridad del Ecuador, en el Pilar 5, dentro de sus objetivos y líneas de acción referentes a las habilidades y capacidades de ciberseguridad, se plantea la creación sistemática de planes de estudios en todos los niveles de educación, así como el fortalecimiento de la cultura de ciberseguridad, que empiece desde los ciudadanos hasta las organizaciones públicas y privadas, generando con ello una conciencia compartida de los riesgos de ciberseguridad y las amenazas en el ciberespacio. Actualmente en nuestro país no

existen propuestas concretas con respecto a la implementación de la ciberseguridad en los distintos niveles de educación existentes en el Ecuador.

4.7.4. Estrategia Nacional de Ciberseguridad de Costa Rica.

La Estrategia Nacional de Ciberseguridad de Costa Rica 2017, proporcionó un marco estratégico, para lograr los objetivos socioeconómicos que dependían de la seguridad del ciberespacio. Con la necesidad de proteger el espacio digital, se diseñó e implementó políticas frente a los riesgos emergentes, que amenazaban el funcionamiento básico de la sociedad.

Costa Rica ha presentado un proceso de acciones para mejorar la ciberseguridad nacional, lo cual llevó al país en el año 2017, a generar su primera Estrategia Nacional de Ciberseguridad, con una visión nacional en respuesta a las amenazas cibernéticas.

Es importante destacar que en el año 2012, el Decreto 37.052 creó el CSIRT Nacional bajo el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, para coordinar la seguridad cibernética y de información, formando un equipo de expertos destinado a prevenir y responder tanto amenazas como ataques cibernéticos contra las instituciones gubernamentales. Su trabajo empezó en el 2018, en los temas de ciberseguridad a nivel nacional y coordinó con el resto de organismos del país, constituyéndose como la institución responsable de mejorar las capacidades en ciberseguridad.

En general, Costa Rica está dispuesto a invertir el capital político, tiempo, dinero y recursos para contar con un ciberespacio más seguro en beneficio de sus ciudadanos. Este trabajo, impulsado desde el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, también ha contado con socios internacionales, como la propia Organización de los Estados Americanos, el Banco Interamericano de Desarrollo, los gobiernos de Israel y Corea del Sur.

En la Estrategia Nacional de 2017, su objetivo específico 8, fue seguir mejorando las capacidades en ciberseguridad del país, a partir de la implementación, seguimiento y evaluación de las líneas de acción y proponer los ajustes según se requiera.

La línea estratégica 8.2, estableció realizar una revisión y actualización de la Estrategia Nacional de Ciberseguridad. Siguiendo este mandato, en septiembre de 2020, el Gobierno de Costa Rica solicitó formalmente, la asistencia técnica especializada del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los

Estados Americanos, para llevar a cabo una revisión y elaboración oportuna de la Estrategia Nacional de 2017, en vista de renovar el marco de ciberseguridad.

Para aprovechar los beneficios y gestionar los desafíos de la digitalización, el gobierno de Costa Rica, confirma su compromiso para mantener un ciberespacio seguro, a partir de la actualización de la Estrategia, creándose así la Estrategia Nacional de Ciberseguridad de Costa Rica 2022, que pretende crear una hoja de ruta de trabajo común que permita, generar nuevos ejes de desarrollo como educación, oportunidad de actividades económicas, desarrollo seguro del turismo y fortalecimiento de la ciberseguridad del país.

El objetivo de esta Estrategia Nacional 2022, es crear una visión de un ciberespacio abierto, libre y seguro, que responda a las ciberamenazas potenciales a las que se enfrenta o puede enfrentar Costa Rica, generando un pensamiento estratégico, que permite continuar apoyando a las autoridades del país y formuladores de políticas en el desarrollo, establecimiento e implementación de un marco holístico e integral, que englobe todas las iniciativas que tienen que ver con la ciberseguridad en el país, para evitar la duplicidad de esfuerzos que puede derivarse de intervenciones aisladas y no coordinadas, partiendo de la base que la ciberseguridad es una responsabilidad de todos.

La Estrategia presenta los siguientes principios rectores: 1. Las personas son la prioridad, 2. Respeto a los Derechos Humanos y la Privacidad, 3. Coordinación y corresponsabilidad de múltiples partes interesadas y 4. Cooperación Internacional.

Actualmente el gobierno de Costa Rica, cuenta con políticas públicas e iniciativas en materia de las Tecnologías de la Información y las Comunicaciones, como son: 1. Estrategia De Transformación Digital, 2. Estrategia Nacional de Bioeconomía Costa Rica 2020-2030, 3. Plan Nacional de Desarrollo de Telecomunicaciones, 4. Política Nacional de Sociedad y Economía basada en el Conocimiento y 5. Estrategia de Prevención y Atención del Abuso y Explotación Sexual de Niños, Niñas y Adolescentes en Línea (2021-2027).

Las amenazas a la ciberseguridad de Costa Rica, afectan al desarrollo socioeconómico, político y humano, que se ve alterado por diversos factores dentro del contexto nacional; es por esta razón que se han identificado una serie de ejes transversales que agrupan distintos ámbitos, entre ellos existen: 1. Coordinación Nacional, 2. Fortalecimiento del Ecosistema de Ciberseguridad, 3. Habilitar un ciberespacio más seguro, 4. Fortalecimiento de la cooperación cibernética internacional, 5. Gestión del riesgo, 6. Protección de Servicios Esenciales, 7.

Fortalecimiento del marco legal en Ciberseguridad y las Tecnologías de la Información y las Comunicaciones y 8. Gestión de la comunicación en crisis de ciberseguridad.

Teniendo en cuenta la implementación de la Estrategia Nacional de Ciberseguridad 2017, así como la revisión de la misma que se realizó en el 2021 en Costa Rica, se han considerado los siguientes objetivos auxiliares: 1. Desarrollo de capacidades en ciberseguridad empresarial, 2. Desarrollo de capacidades de ciberseguridad del turismo, 3. Alfabetización digital, 4. Desarrollo de Planes de Acción, 5. Desarrollo de ciberseguridad con el sector financiero, 6. Infraestructura resiliente y 7. Ciberseguridad Industrial.

En Costa Rica la Estrategia Nacional de Ciberseguridad, tiene como eje principal a las personas, al respeto de los derechos humanos, especialmente los relacionados con el acceso a las Tecnologías de la Información y la Comunicación, a la información y a la privacidad. Además, toma en consideración el apoyo de todos los sectores en el ámbito público-público, público-privado y público-sociedad civil. La construcción de alianzas, acuerdos y estrechamiento de lazos con otras entidades públicas y privadas, que atienden las temáticas relacionadas a la ciberseguridad, tanto a nivel regional e internacional, son elementos clave dentro de esta Estrategia.

Dentro de los principios rectores, en los que se basa la Estrategia Nacional de Ciberseguridad de Costa Rica, se destaca la cooperación internacional, para la atención de las amenazas, la transferencia de conocimiento y el desarrollo de acciones locales y globales que ayuden a incrementar la confianza y la seguridad global. Este país cuenta con el apoyo del Convenio de Budapest sobre la ciberdelincuencia, siendo uno de los 68 Estados miembros de este convenio. En Ecuador, su Estrategia Nacional de Ciberseguridad, busca la cooperación internacional, debido a que el ciberespacio es transnacional y requiere un diálogo eficaz para aprovechar las oportunidades y gestionar los riesgos de ciberseguridad. Actualmente nuestro país, se encuentra en proceso de adhesión al Convenio de Budapest sobre la ciberdelincuencia, que permitirá armonizar las leyes nacionales, mejorar las técnicas de investigación y el aumento de la cooperación con otras naciones firmantes.

Por otro lado, la Estrategia Nacional de Ciberseguridad de Costa Rica, establece la alfabetización digital, como un objetivo auxiliar, donde se propone la elaboración de un Plan Nacional de Alfabetización Digital de sectores vulnerables, con el fin de formar una cultura digital, mejorando el conocimiento en ciberseguridad, en delitos informáticos y su prevención. En Ecuador, la alfabetización digital es muy limitada y la falta de concientización de la

población en materia de ciberseguridad, inducen a la población a ser víctima de la ciberdelincuencia. Además, las víctimas de delitos cibernéticos, no siempre se percatan de que sus activos se han visto comprometidos; y aunque lo hagan, existe un desconocimiento generalizado sobre cómo denunciar este tipo de delitos.

4.7.5. Estrategia Nacional de Ciberseguridad de la República de Argentina.

La Estrategia Nacional de Ciberseguridad 2019 de Argentina, establecida por el Poder Ejecutivo Nacional y la sociedad en forma multidisciplinaria y multisectorial, sienta los principios básicos y desarrolla los objetivos fundamentales, que permitirán fijar las previsiones nacionales en materia de protección del ciberespacio. Su finalidad es brindar un contexto seguro para el aprovechamiento de las personas, organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo acorde.

El Comité de Ciberseguridad creado por el Decreto N° 577 del 28 de julio de 2017, desarrolló la Estrategia Nacional de Ciberseguridad, donde se desplegaron las acciones para el uso seguro del ciberespacio en la República de Argentina, que impulsó una visión integradora que garantice la seguridad y el progreso de la nación. Luego, a través de la Resolución de la ex Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros N° 829 del 24 de mayo de 2019, se aprobó la primera Estrategia Nacional de Ciberseguridad.

La Estrategia se llevó a cabo con la coordinación y cooperación entre la Administración Pública Nacional, poderes de las jurisdicciones provinciales, municipales, el sector privado, las organizaciones no gubernamentales y las entidades académicas de la Ciudad Autónoma de Buenos Aires. Todo ello se hizo efectivo, en el marco del respeto a los principios recogidos en la Constitución Nacional, a las disposiciones de los tratados y acuerdos internacionales, a los que la República de Argentina se ha adherido.

La República de Argentina, adoptó medidas idóneas para proteger la privacidad de los datos de las personas y organizaciones, por medio de la prevención, detección, análisis, investigación, recuperación, defensa y respuesta, que constituyen elementos esenciales para alcanzar todos los beneficios del uso seguro del ciberespacio.

La Estrategia Nacional de Ciberseguridad 2019, promovió una serie de objetivos centrales, sustentados por principios rectores, que se encargaban del desarrollo de planes, políticas y acciones concretas para beneficio de la nación, entre ellos tenemos: Respeto por los

derechos y libertades individuales; Liderazgo, construcción de capacidades y fortalecimiento federal; Integración internacional; Cultura de ciberseguridad y responsabilidad compartida y Fortalecimiento del desarrollo socioeconómico.

Dentro de los Objetivos de la Estrategia Nacional de Ciberseguridad se destacan: 1) Concientización del uso seguro del Ciberespacio; 2) Capacitación y educación en el uso seguro del Ciberespacio; 3) Desarrollo del marco normativo; 4) Fortalecimiento de capacidades de prevención, detección y respuesta; 5) Protección y recuperación de los sistemas de información del Sector Público; 6) Fomento de la industria de la ciberseguridad; 7) Cooperación Internacional y 8) Protección de las Infraestructuras Críticas Nacionales de Información.

Las complejidades que exhibe el ciberespacio y los desafíos que se presentan en la protección del entorno digital frente al avance de nuevas tecnologías, llevó a actualizar la referida Estrategia, dada la relevancia que adquiere la ciberseguridad, en el uso e implementación de las tecnologías de la información y la comunicación, se sometió a consulta pública a la Segunda Estrategia Nacional de Ciberseguridad, para contar con el aporte y participación de la ciudadanía, del sector público, privado, de la academia, la sociedad civil y cualquier interesado en la materia.

La Estrategia Nacional de Ciberseguridad 2022, plantea la necesidad de continuar desplegando acciones para el uso seguro del ciberespacio, impulsando una visión integradora, cuya aplicación ayude a garantizar la seguridad y el progreso de la nación.

La vigencia de las tecnologías de procesamiento masivo de datos, la computación en la nube, Internet de las cosas, el desarrollo de 5G y los avances en la inteligencia artificial, tanto, así como la utilización de redes sociales y plataformas para la comunicación interpersonal, resulta determinante para los Estados, incorporar la problemática de la ciberseguridad a la agenda gubernamental.

La ciberseguridad es abordada en la Estrategia 2022, como el conjunto de políticas y acciones, orientadas a elevar los niveles de seguridad de las personas y las organizaciones, frente a amenazas, incidentes y delitos, entre otros, que utilicen como medio y/o fin un dispositivo informático.

La República de Argentina, indica que promoverá el uso pacífico del ciberespacio y apoyará toda iniciativa que tenga por fin la instauración de valores como la justicia, el respeto al Derecho Internacional, el equilibrio y la reducción de la brecha digital entre las naciones,

impulsando el diálogo y la cooperación. En este sentido, el ciberespacio debe constituirse en un dominio en el que impere la paz, impidiendo el desarrollo de posibles conflictos armados o aquellos que puedan poner en riesgo la seguridad de la nación y de su población.

La Estrategia Nacional de Ciberseguridad 2022, se sustenta en los siguientes principios rectores: Paz y seguridad en el ciberespacio; Respeto por los derechos humanos, los derechos y libertades individuales; Construcción de capacidades y fortalecimiento federal; Cooperación internacional; Respeto por la soberanía nacional; Cultura de ciberseguridad y responsabilidad compartida y Fortalecimiento del desarrollo socioeconómico.

Los objetivos de esta Estrategia se centran en: 1. Concientización, Capacitación y Educación en el uso responsable del ciberespacio y promoción para la formación de especialistas en ciberseguridad; 2. Desarrollo del marco normativo; 3. Fortalecimiento de capacidades de prevención, detección y respuesta; 4. Protección y recuperación de los sistemas de información del Sector Público; 5. Fomento de la industria de la ciberseguridad; 6. Cooperación Internacional; 7. Protección de las Infraestructuras Críticas Nacionales y 8. Fortalecimiento del sistema institucional para el abordaje de la problemática de la ciberseguridad a nivel federal.

Luego de analizar las Estrategias de Ciberseguridad de la República de Argentina, podemos deducir, que es fundamental la protección, el respeto por los derechos y libertades individuales consagrados en la Constitución Nacional y en los Tratados Internacionales de los cuales la República de Argentina es miembro activo. Además, su fin es promover políticas públicas y construir capacidades de detección, prevención y respuesta a incidentes cibernéticos. Esta Estrategia pretende desarrollar una cultura de ciberseguridad, para concientizar el uso seguro y responsable del ciberespacio, brindando seguridad al Estado y a la sociedad.

Actualmente, en la Guía Estratégica del Panorama Nacional de Argentina 2023, se establece un Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones, dentro de la segunda dimensión denominada Cultura y Sociedad Cibernética, se revisan aspectos importantes sobre la adquisición de una cultura de ciberseguridad responsable, donde su principal fin es ayudar a entender los riesgos relacionados con la ciberseguridad en la sociedad, el nivel de confianza en los servicios de Internet, del gobierno y comercio electrónico, así como la comprensión de los usuarios sobre la protección de la información personal en línea. Con estos conocimientos la ciudadanía puede estar alerta a las ciberamenazas y ciberataques

existentes en el espacio digital, evitando ser víctimas de los delitos informáticos producto de la mala utilización de las tecnologías de la información y la comunicación.

Las nuevas Tecnologías de la Información y la Comunicación han significado un cambio en la historia de este país, donde los aspectos de la vida humana están relacionados con este fenómeno, las personas se comunican, expresan, educan, crean, comercian, investigan y desarrollan gran parte de su vida social y laboral en el ciberespacio. Por lo tanto, el entorno virtual es una fuerte dependencia de las redes informáticas, donde los servicios esenciales para la vida de las personas y la economía, deben ser protegidos, con la coordinación de esfuerzos de múltiples actores públicos y privados.

En Ecuador, el uso de las Tecnologías de la Información y la Comunicación tiene una relación directa entre las personas, la interacción del Estado con el ciudadano, el surgimiento de la economía digital, entre otras actividades, las mismas que ayudan al crecimiento exponencial en el uso del ciberespacio, aumentando consecuentemente los riesgos a los que se encuentran expuestas las personas y las organizaciones.

En Ecuador como en Argentina, observamos que mientras mayor es el desarrollo, mayor es la vulnerabilidad, todo esto gracias a la masividad en el uso del ciberespacio; es decir, a medida que la sociedad avanza, mayor es la cantidad de personas, organizaciones públicas y privadas que se conectan a las redes informáticas, siendo así, mayores los riesgos y desafíos que enfrentan. Actualmente el bienestar y el progreso de la sociedad, están ligados al desarrollo digital, cuya expansión es imposible detener. Por ello, las Estrategias de Ciberseguridad, son necesarias e indispensables para que los beneficios de estas innovaciones se distribuyan con justicia, equidad y con pleno respeto de los derechos humanos; por lo tanto, todos los países del mundo, deben centrar sus esfuerzos en prevenir actos que afecten los derechos de las personas, entre ellos su libertad, integridad física, privacidad de sus datos y propiedad privada.

5. Metodología.

5.1. Materiales Utilizados.

El presente Trabajo de Integración Curricular, ha sido desarrollado con la ayuda de diversos materiales, los mismos que aportaron para que los objetivos planteados se puedan cumplir, entre las fuentes bibliográficas tenemos: Libros, Diccionarios Jurídicos, Manuales, Obras jurídicas, Páginas web, Revistas jurídicas, Leyes y Códigos.

Los materiales que hemos utilizado para la realización de la presente investigación son: Computador portátil, teléfono celular, grabadora, proyector, cámara, impresora, conexión a Internet, fichas, cuaderno de apuntes, hojas de papel bond, fotocopias, entre otros materiales adicionales.

5.2. Métodos.

En la realización del presente Trabajo de Integración Curricular, se aplicaron múltiples métodos, los mismos que han servido para sustentar esta investigación, a continuación, los detallaré a cada uno de ellos:

Método Inductivo: Este método va de lo particular a lo general. En la presente investigación nos permitió analizar el alto índice de los delitos informáticos, a través de noticias actualizadas en diferentes medios como la prensa digital ecuatoriana, con la finalidad de encontrar los datos más relevantes a este problema social y plantear alternativas adecuadas para la aplicación, ejecución y fortalecimiento de la Política y Estrategia Nacional de Ciberseguridad vigentes en el Ecuador, siendo las herramientas más eficaces para minimizar el cometimiento de estas conductas antijurídicas.

Método Deductivo: Método que va de lo general a lo particular, se lo aplicó en la formulación del problema de investigación, en la presentación de conceptos y normas jurídicas que tienen relación con el problema planteado que es el aumento de los delitos informáticos a causa de las ciberamenazas y ciberataques existentes en el Ecuador. Este método nos ayudó a realizar un estudio de la Política y Estrategia Nacional de Ciberseguridad existente en nuestro país con el fin de contrastar la hipótesis, obtener resultados y posibles soluciones.

Método Analítico: Se analizan las partes de un todo, este método posibilita descomponerlo en partes, elementos y cualidades, pudiendo estudiar el problema social de forma detallada, estableciendo nuevas teorías. Dentro de la investigación se lo utilizó para realizar los análisis y comentarios a los respectivos conceptos, definiciones y demás aspectos doctrinarios tomados de diversos autores, además de las normas jurídicas que sustentan el presente trabajo de

investigación como la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, el Reglamento para el Sistema de Protección a Víctimas y Testigos, la Política y Estrategia Nacional de Ciberseguridad del Ecuador, así como también en el análisis de los resultados obtenidos de las encuestas y entrevistas aplicadas en la investigación.

Método Comparativo: Con la ayuda de este método, se ha podido contrastar realidades y perspectivas de varios países en cuanto a las Políticas y Estrategias Nacionales de Ciberseguridad. El Derecho Comparado es un gran aporte en la presente investigación, ya que nos proporciona nuevos conocimientos y visiones legales sobre el tema antes planteado, para lo cual hemos tomado algunos países como: República Dominicana, España, Chile, Costa Rica y Argentina, con el fin de plantear alternativas y soluciones que contribuyan a disminuir y contrarrestar los delitos informáticos existentes en nuestro país.

Método Estadístico: En la presente investigación, se utilizó este método para recolectar información cuantitativa y cualitativa, mediante las técnicas de encuestas y entrevistas, para luego proceder a la tabulación de resultados, la elaboración de tablas y figuras que nos permitirán conocer las opiniones de varios profesionales en relación al tema planteado. Para la aplicación de este método se realizó la recolección, recuento, presentación, síntesis y análisis de los datos obtenidos en el estudio de campo.

5.3. Técnicas.

Las técnicas que utilizamos en la presente investigación, son las siguientes:

Encuesta: Cuestionario de preguntas que se realizó para obtener la opinión de 30 profesionales con conocimientos pertinentes sobre la problemática planteada, la misma que fue contestada adecuadamente por los encuestados.

Entrevista: Diálogo establecido entre la persona entrevistadora y el entrevistado, con la finalidad de recabar y adquirir una opinión más acertada sobre el problema social investigado, en el presente Trabajo de Integración Curricular, se la aplicó a 10 profesionales del Derecho especialistas en la materia de estudio.

5.4. Observación Documental.

Este procedimiento me permitió realizar el estudio de casos judiciales, determinando la conducta antisocial utilizada por los delincuentes informáticos que hoy en día es muy sofisticada, la misma que ha evolucionado a la par de la innovación de la tecnología. Además,

se analizó los datos estadísticos más actualizados y relevantes sobre el problema de investigación planteado.

6. Resultados.

6.1. Resultados de las Encuestas.

La presente técnica de encuesta, fue aplicada a treinta profesionales del Cantón de Loja. Este cuestionario está conformado por cinco preguntas, que serán presentadas a continuación y de las cuales se han obtenido los siguientes resultados.

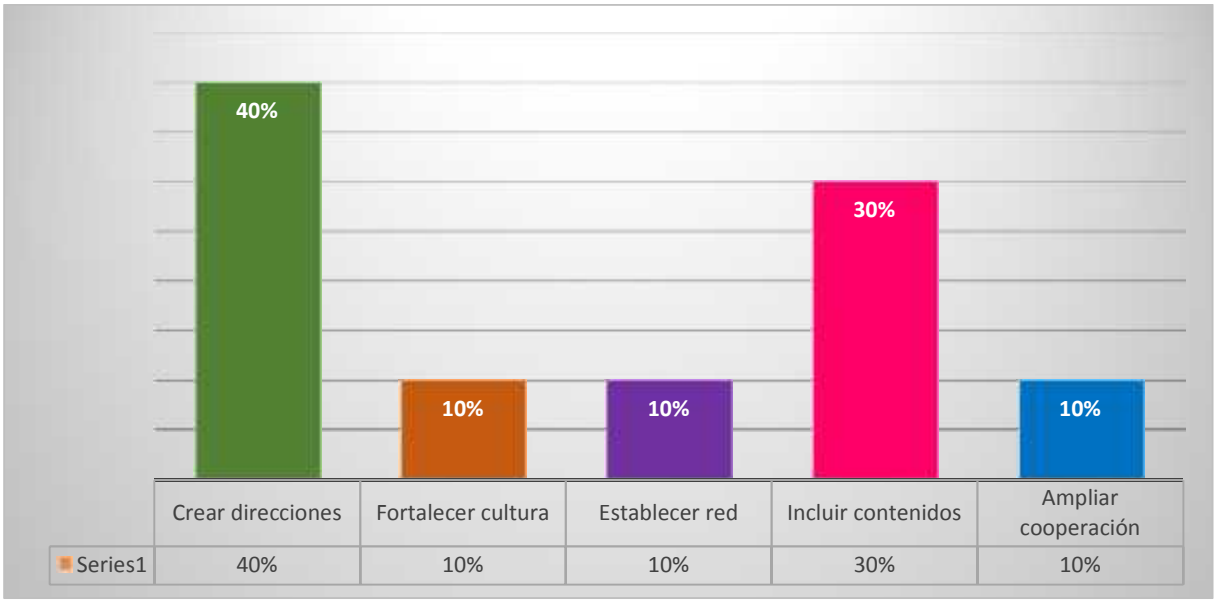
Primera Pregunta: De las siguientes líneas de acción, dígnese seleccionar una: ¿Cuál cree usted, que es un aporte a las políticas criminales implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos de ciberamenazas y ciberataques?

Tabla Estadística No. 1

Indicadores	Variables	Porcentaje
Crear direcciones	12	40 %
Fortalecer cultura	3	10 %
Establecer red	3	10 %
Incluir contenidos	9	30 %
Ampliar cooperación	3	10 %
Total	**30**	**100%**

Fuente: Profesionales del Cantón Loja.
Autora: Lizbeth Sofía Palacios Orellana.

Figura No. 1



Interpretación:

En la presente pregunta los treinta encuestados respondieron de la siguiente manera: Doce encuestados que representan el 40% seleccionan la opción crear Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional calificado en el campo de la informática y el Derecho; mientras que tres personas que equivalen al 10% escogen la opción fortalecer la cultura sobre el uso del ciberespacio, mejorando las habilidades y la conciencia de ciberseguridad de las múltiples partes interesadas, a través de capacitaciones técnicas especializadas, de acuerdo con el desarrollo tecnológico acelerado y el panorama de riesgos y amenazas; en cambio tres profesionales que figuran el 10% eligieron la opción de establecer una red de puntos de contacto nacionales, para la educación en ciberseguridad en diferentes sectores, instituciones educativas y agencias gubernamentales; por otro lado nueve investigados que representan el 30% optaron por la opción incluir contenidos educativos complementarios de ciberseguridad, dirigidos a docentes y estudiantes de educación primaria, secundaria y superior; finalmente tres personas que corresponden al 10 % decidieron la opción de ampliar y formalizar la cooperación con otros organismos nacionales e internacionales de respuesta a incidentes cibernéticos.

Análisis:

De acuerdo a los resultados obtenidos en la presente encuesta, comparto la opinión de la mayoría porque al Crear Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional calificado en el campo de la informática y el Derecho, nos permitirá estar mejor preparados para identificar las ciberamenazas y ciberataques que son muy recurrentes hoy en día, por la dependencia digital en la que nos encontramos, tomando en cuenta que la mayoría de las actividades que realizamos son por los medios electrónicos. Además, es muy importante fortalecer la cultura de ciberseguridad a través de la concientización, capacitación y enseñanza de la Política y Estrategia Nacional de Ciberseguridad en nuestro país, con el objetivo de que la población ecuatoriana no sea víctima de los delincuentes informáticos.

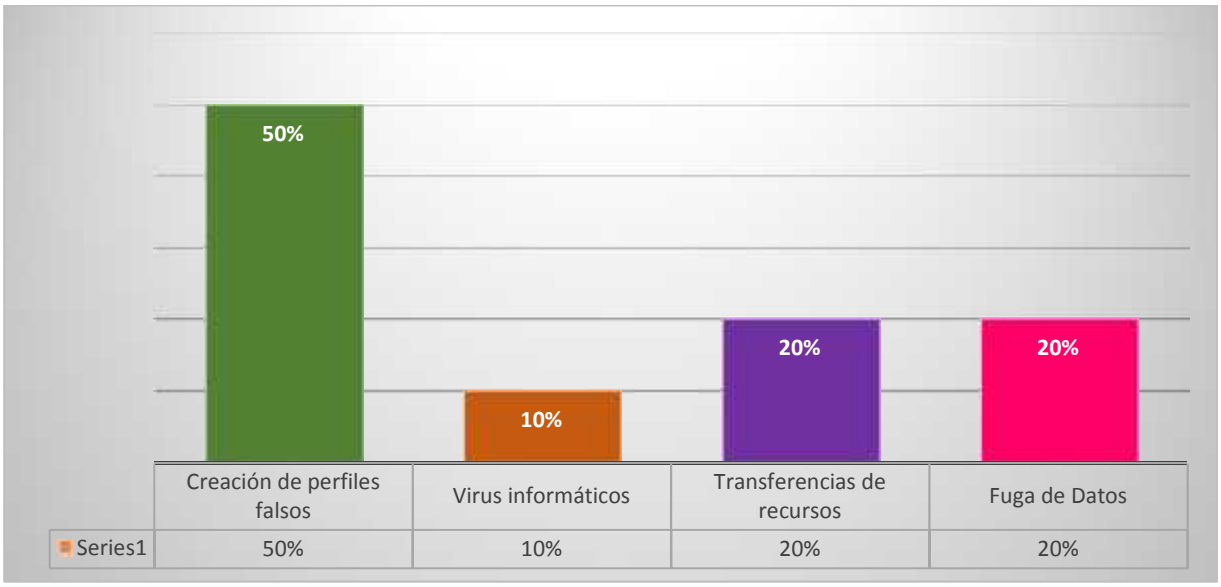
Segunda Pregunta: Seleccione una opción: ¿Cuál es la forma más común en la que operan los antisociales al cometer los Delitos Informáticos?

Tabla Estadística No. 2

Indicadores	Variables	Porcentaje
Creación de perfiles falsos	15	50 %
Virus informáticos	3	10 %
Transferencias de recursos	6	20 %
Fuga de Datos	6	20 %
Total	**30**	**100%**

Fuente: Profesionales del Cantón Loja.
Autora: Lizbeth Sofía Palacios Orellana.

Figura No. 2



Interpretación:

En la presente pregunta los treinta encuestados respondieron de la siguiente manera: Quince personas que representan el 50% seleccionan la opción de la creación de perfiles falsos sobre la base de la información consignada en redes sociales; mientras que tres encuestados que equivalen al 10% escogen la opción sobre los virus informáticos y malware, que son programas maliciosos que tienden a reproducirse y extenderse dentro del sistema; en cambio seis profesionales que figuran el 20% eligieron la opción de las transferencias de recursos de entidades financieras a varias cuentas; por último, seis personas que corresponden al 20% optaron por la opción de la fuga de datos, que consiste en la divulgación o publicación de información confidencial.

Análisis:

Con respecto a los resultados alcanzados en esta pregunta, estoy de acuerdo con la mayoría de los encuestados, que indican que la forma más común que utilizan los antisociales para cometer

los delitos informáticos, es la creación de perfiles falsos sobre la base de la información consignada en redes sociales, teniendo en cuenta que actualmente el cometimiento de los delitos informáticos en el Ecuador han crecido ampliamente por medio de las plataformas digitales, causando que la información sea falsificada o alterada, ocasionado grandes daños en el ámbito social, psicológico y económico en los individuos, grupos y a la sociedad en general.

Por lo tanto, es necesario que el Estado busque los mecanismos más adecuados para desarticular las bandas delincuenciales existentes en nuestro país. Es pertinente indicar que una eficiente educación, capacitación, información y concientización en el manejo adecuado de las redes sociales y el Internet, permitirán que el ser humano pueda ejercer el derecho a las tecnologías de la información y la comunicación sin temor alguno; así como también, desarrollarse en un ambiente libre de actos ilícitos, contribuyendo al goce efectivo de los derechos humanos de todas las personas.

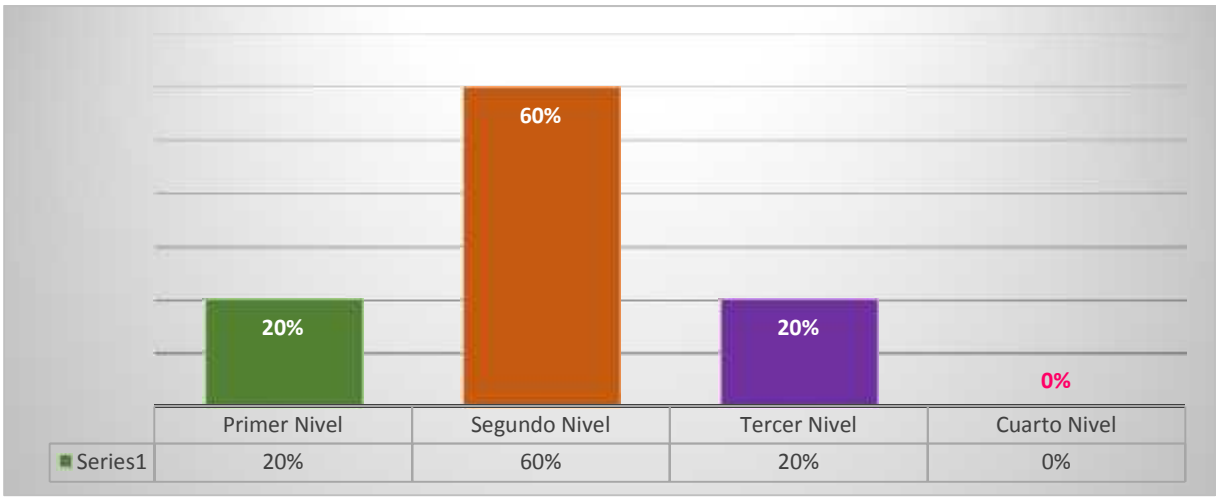
Tercera Pregunta: Señalar la opción pertinente: ¿En qué nivel de educación estima usted, que sería favorable impartir conocimientos sobre Ciberseguridad, para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?

Tabla Estadística No. 3

Indicadores	Variables	Porcentaje
Primer Nivel	6	20 %
Segundo Nivel	18	60 %
Tercer Nivel	6	20 %
Cuarto Nivel	0	0 %
Total	**30**	**100%**

Fuente: Profesionales del Cantón Loja.
Autora: Lizbeth Sofía Palacios Orellana.

Figura No. 3



Interpretación:

En la presente pregunta los treinta encuestados respondieron de la siguiente manera: Seis encuestados que representan el 20 % seleccionan la opción primer nivel o nivel inicial; mientras que dieciocho personas que equivalen al 60% escogen la opción segundo nivel de educación general básica y bachillerato; en cambio seis profesionales que corresponden al 20% eligieron la opción de tercer nivel técnico – tecnológico de grado; para finalizar ninguna persona, decidió la opción cuarto nivel o de posgrado.

Análisis:

En relación a los resultados conseguidos, puedo mencionar que comparto la opinión de la mayoría de los encuestados que mencionan que es favorable impartir conocimientos de ciberseguridad en el segundo nivel de educación general básico y bachillerato, porque los niños, niñas y adolescentes son las personas que mayormente usan los medios informáticos para realizar múltiples actividades como la investigación, el estudio, es decir, todo lo relacionado al aprendizaje, así como también las actividades de ocio y distracción como son los juegos en línea, la música, videos, redes sociales, etcétera.

Además, podemos observar que las niñas, niños y adolescentes viven en un mundo globalizado y tecnológico, donde la mayoría de ellos tienen acceso a la web y poseen cuentas en las diferentes redes sociales como WhatsApp, Facebook, YouTube, Instagram, Twitter, Linkedln, TikTok, Telegram, Pinterest, entre otros; siendo estos sitios el medio por el cual se expone la información personal, que es utilizada por los delincuentes informáticos para cometer actos ilícitos. Por tal razón, es necesario que exista una educación basada en ciberseguridad, tomando en cuenta que los menores de edad no tienen la madurez, capacidad y conocimientos suficientes para enfrentar las ciberamenazas y ciberataques.

Por lo tanto, la ciberseguridad debe ser implementada en todos los niveles de educación y a la sociedad en general, porque es una herramienta indispensable para prevenir, identificar y proteger la información personal, logrando de esta manera disminuir el alto índice de los delitos informáticos en el Ecuador.

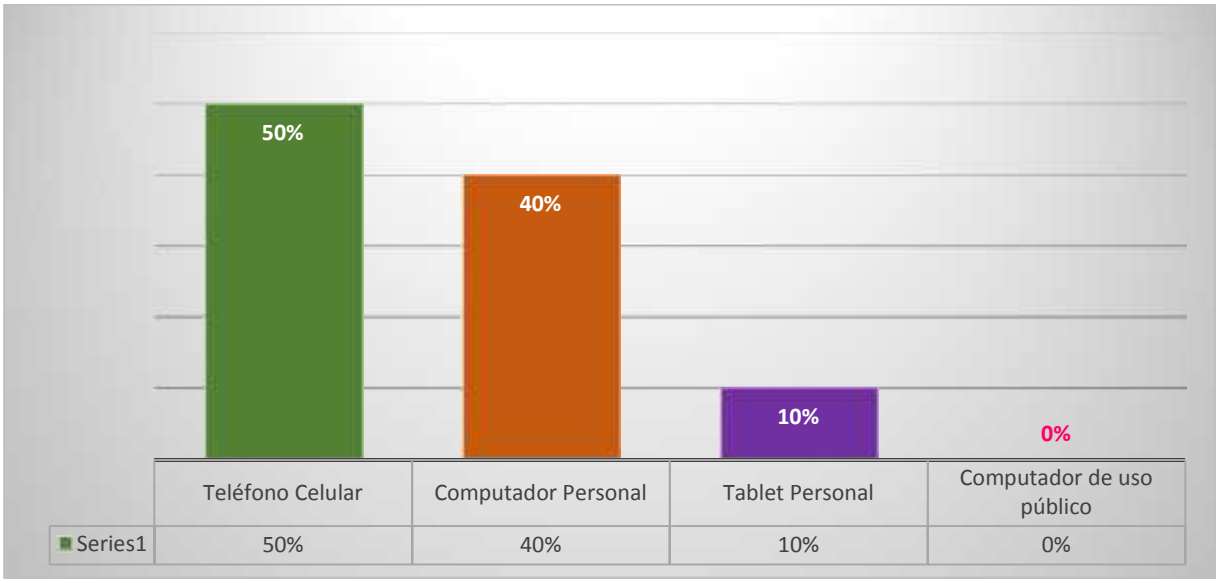
Cuarta Pregunta: Escoja la opción pertinente: ¿Según su criterio, qué medio tecnológico es el más adecuado para evitar los perjuicios ocasionados por los Delitos Informáticos?

Tabla Estadística No. 4

Indicadores	Variables	Porcentaje
Teléfono Celular	15	50 %
Computador Personal	12	40 %
Tablet Personal	3	10 %
Computador de uso público	0	0 %
Total	**30**	**100%**

Fuente: Profesionales del Cantón Loja.
Autora: Lizbeth Sofía Palacios Orellana.

Figura No. 4



Interpretación:

En la presente pregunta los treinta encuestados respondieron de la siguiente manera: Quince encuestados que representan el 50% seleccionan la opción Teléfono Celular; mientras que doce personas que equivalen al 40% escogen la opción Computador Personal; en cambio tres profesionales que figuran el 10 % eligieron la opción de Tablet Personal; por último, ningún encuestado prefirió la opción Computador de uso público.

Análisis:

Después de obtener los resultados de esta pregunta, referente a que medio tecnológico es el más adecuado para evitar los perjuicios ocasionados por los delitos informáticos, la mayoría de las personas expusieron que es el teléfono celular, personalmente no comparto esta opinión porque, el móvil o teléfono celular no se diseñó para ser seguro, sino para ser más abierto y compatible, por lo que está más expuesto a todo tipo de ciberamenazas y ciberataques. Los teléfonos celulares pueden estar protegidos por huella dactilar, reconocimiento facial, contraseña, entre

otras formas, pero estas son ineficientes cuando el dispositivo electrónico es vulnerado. Además, considero que este medio tecnológico es fácil de trasladar, por lo que es más susceptible a ser olvidado, robado o hurtado y nuestra información registrada puede ser usada por los antisociales, accediendo a los datos, redes sociales, cuentas bancarias, etcétera.

Por lo tanto, todos como usuarios debemos conocer los peligros a los que se nos exponemos, por el mal uso de las tecnologías de la información y la comunicación, lo conveniente sería utilizar nuestro computador personal, ya que posee mejores garantías para su uso, instalando cortafuegos, un antivirus con licencia activa y nuestra propia red de Internet, manteniendo con una mayor protección en las actividades diarias que realizamos con este dispositivo, evitando los perjuicios ocasionados por los delitos informáticos.

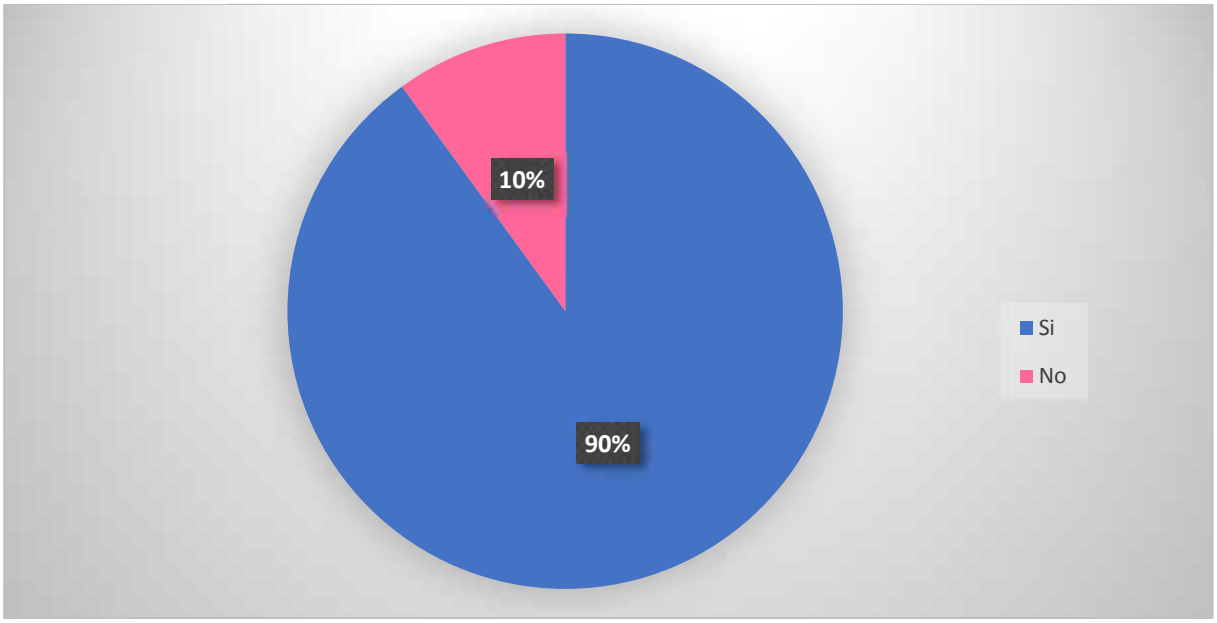
Quinta Pregunta: ¿Cree usted, que la actualización de conocimiento y correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos, servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador?

Tabla Estadística No. 5

Indicadores	Variables	Porcentaje
Si	27	90 %
No	3	10 %
Total	**30**	**100%**

Fuente: Profesionales del Cantón Loja.
Autora: Lizbeth Sofía Palacios Orellana.

Figura No. 5



Interpretación:

En la presente pregunta los treinta encuestados respondieron de la siguiente manera: veintisiete profesionales que representan el 90% seleccionaron la opción Si; mencionan que la actualización de conocimientos y correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos, servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador, porque la actualización de conocimientos de Ciberseguridad, permitirá que la ciudadanía en general, aprenda las técnicas y alternativas de protección al momento de utilizar los dispositivos informáticos evitando que la delincuencia atente contra la privacidad e información personal; en cambio, tres personas que equivalen al 10% escogen la opción No; consideran que la actualización de conocimientos y la correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos, no servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador, porque creen que el Estado debería ampliar las directrices y el control en el sistema penal, para sancionar de forma más drástica a los delincuentes informáticos, que buscan apropiarse de la información de carácter personal de los usuarios en beneficio de sus intereses.

Análisis:

Después de analizar las respuestas a esta pregunta, confirmo la opinión de la mayoría de los encuestados, donde nos indican que es importante que exista una actualización de conocimientos, para ampliar la cultura de ciberseguridad en el manejo de los medios digitales, permitiendo con ello que cada usuario tenga una mayor cautela sobre la información que suministra y comparte en las distintas aplicaciones, sistemas, redes sociales, etcétera; tomando en cuenta que actualmente los delincuentes informáticos, están muy preparados frente a los avances tecnológicos existentes en el mundo digital y del cual todos formamos parte.

Además, la ciberseguridad es necesaria porque nos permite tener un conocimiento amplio sobre los peligros que asechan al ciberespacio, ocasionados por personas inescrupulosas que incurren en conductas delictivas sin importarle su accionar, que sin mostrar su identidad vulneran los derechos de los individuos, las instituciones públicas y privadas, las empresas e incluso al Estado ocasionando grandes perjuicios a los mismos.

El Estado ecuatoriano para contrarrestar las ciberamenazas y ciberataques ha creado instrumentos de ciberseguridad con el objeto de construir y fortalecer el desarrollo social, económico y humano del país, utilizando técnicas y alternativas de protección, ante cualquier

atentado que violente la privacidad y la información, logrando con ello minimizar el cometimiento de los delitos informáticos en el Ecuador.

6.2. Resultados de las Entrevistas.

La técnica de la entrevista fue aplicada a diez profesionales del Derecho especializados, entre ellos, Magister de Ciberseguridad, Oficial de Seguridad de la Información, Analista de Seguridad de la Información, Programador de Sistemas Informáticos, Director de Tecnología de la Información, los mismos que pertenecen a la Cooperativa de Ahorro y Crédito Manuel Esteban Godoy Ortega; Asesor Jurídico del Banco de Loja; Agente Fiscal de la Unidad de Delincuencia Organizada Transnacional e Internacional (FEDOTI) del Cantón Loja, Abogados especializados en Derecho Penal e Informático.

La entrevista aplicada a cada uno de los especialistas, consta de 6 preguntas, las cuales las detallaré a continuación:

Primera pregunta: **Podría indicar usted, ¿Cuáles son las Políticas de Ciberseguridad implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos existentes con las ciberamenazas y ciberataques?**

Respuestas:

Primer entrevistado: La Política Nacional de Ciberseguridad establece lineamientos para la coordinación de actividades de todas las partes interesadas relevantes en la seguridad informática, los mismos que tendrán funciones y responsabilidades frente a las ciberamenazas y ciberataques existentes en el ciberespacio.

Segundo entrevistado: Para promover en los usuarios informáticos la capacidad de prevención, el Estado ecuatoriano ha presentado varias políticas, que servirán como herramientas para alertar sobre los riesgos que la tecnología ha traído con su evolución, despertando el interés de la ciudadanía para combatir la delincuencia informática.

Tercer entrevistado: Existen algunas políticas implementadas por el Estado para el tema de ciberseguridad, entre ellas tenemos:

- La Política Nacional de Ciberseguridad realizada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, la cual es general y debe ser implementada por las instituciones públicas y privadas, así como por la ciudadanía en general.

- La Estrategia Nacional de Ciberseguridad que involucra proteger la información de todas las empresas, organismos del Estado, para que trabajen de forma conjunta en contrarrestar los delitos informáticos.

Estas políticas ayudan al Estado ecuatoriano a proteger la información confidencial de todas las personas y entidades existentes en nuestro país.

Cuarto entrevistado: Las Políticas de Ciberseguridad implementadas por el Estado para prevenir los riesgos existentes en el mundo digital son:

- Construir y fortalecer las capacidades nacionales, que permitan garantizar el ejercicio de los derechos y libertades de la población, además la protección de los bienes jurídicos del Estado en el ciberespacio, para garantizar un espacio digital seguro.
- Contribuir al desarrollo social, económico y humano del país, creando una confianza digital en toda la población, fortaleciendo el intercambio de información de manera libre y segura.

Quinto entrevistado: La ciberseguridad como mecanismo de prevención de los ataques cibernéticos, tiene como fin enseñar a la ciudadanía a proteger la información y los datos personales, así como también la información comercial a nivel local e internacional, logrando con ello que los delincuentes informáticos no lleguen a cometer el acto delictivo.

Sexto entrevistado: Para la prevención de los riesgos existentes en el ciberespacio, como son las ciberamenazas y ciberataques, la Política de Ciberseguridad se ha enfocado en concientizar a la sociedad ecuatoriana sobre las formas de delinquir que utilizan los antisociales, para que puedan identificarlas correctamente, evitando con ello que la información que se encuentra en los dispositivos sea comprometida.

Séptimo entrevistado: Esta Política plantea que la información es de carácter personalísima, porque no se puede proporcionar a terceras personas, al hacerlo permite el uso indebido de estos datos. Creo que falta mayor difusión y concientización de las políticas públicas que el Estado ha implementado para prevenir los ciberdelitos en nuestro país.

Octavo entrevistado: El Estado ha implementado la Política de Ciberseguridad para resguardar la información personal, porque la tecnología va avanzando y se necesita mayor privacidad y seguridad al momento de utilizar la tecnología.

Esta Política se la realizó en base a la Constitución de la República del Ecuador, donde se protegen los derechos a la información, a la seguridad y la intimidad.

Noveno entrevistado: Esta Política pretende controlar el manejo de información personal en las entidades públicas y privadas. Además protege los datos mejorando las capacidades de defensa y seguridad informática.

Refuerza los mecanismos de ciberseguridad y aumenta la confianza en el ciudadano garantizando la seguridad y protección de los datos confidenciales.

Crean una confianza digital, fomentando el uso adecuado del ciberespacio.

Décimo entrevistado: La Política de Ciberseguridad ha sido creada para evitar las ciberamenazas y ciberataques a la población ecuatoriana, por parte de la delincuencia informática, enseñando métodos de prevención para que los usuarios utilicen correctamente sus dispositivos electrónicos.

Comentario de la autora: De las respuestas vertidas por los profesionales en la presente pregunta, puedo decir que las respuestas son adecuadas, indican que tanto la Política como la Estrategia Nacional de Ciberseguridad, tienen como objetivo proteger la información personal de los usuarios, empresas, instituciones públicas y privadas e incluso del mismo Estado, velando por el correcto ejercicio de los derechos fundamentales de toda la población ecuatoriana.

La Política de Ciberseguridad se realizó con el objeto de conseguir que el Ecuador sea un país digital y ciberseguro, que garantice el Estado de Derechos y justicia que nos plantea en el Art. 1 de la Constitución de la República del Ecuador, que es la ley suprema de nuestro ordenamiento jurídico, protegiendo los servicios en infraestructuras críticas del Estado y la seguridad de la población ecuatoriana en el ciberespacio digital; por lo tanto, es de suma importancia que todos los usuarios obtén por la prevención, cuidando sus dispositivos informáticos, para proteger sus derechos digitales, así como las actividades sociales y económicas que realizan diariamente, contribuyendo con ello a enfrentar la ciberdelincuencia.

Segunda pregunta: ¿Podría usted señalar, cuáles son las formas en las que operan los antisociales para cometer los Delitos Informáticos?

Respuestas:

Primer entrevistado: Las formas que los ciberdelincuentes utilizan para cometer delitos informáticos son:

- Ataques a contraseñas.
- Ataques por ingeniería social.
- Ataques direccionados a las conexiones de las empresas y personas.
- Ataques mediante el uso de malware.

Segundo entrevistado: La principal forma que los delincuentes informáticos usan para vulnerar a los usuarios, es el phishing, porque no existe una concientización a nivel general de la seguridad informática.

Tercer entrevistado: Las formas más concurrentes de cometer delitos informáticos es por medio del phishing, grooming, sexting, stalking, sextorción, vishing, whaling, etcétera, los mismos que afectan considerablemente a las víctimas.

Cuarto entrevistado: Las formas en las que operan los antisociales para cometer los delitos informáticos son:

- Ataques a las contraseñas de las víctimas, pudiendo acceder a su información.
- Ataques por medio de la ingeniería social, entre los principales tenemos el phishing, smishing, qrishing, etcétera.
- Ataques donde se vulneran las conexiones como las wifis falsas, la suplantación de identidad, etcétera.
- Ataques mediante el uso de malware como son los virus, troyanos, gusanos, aplicaciones maliciosas, etcétera.

Quinto entrevistado: La ingeniería social es la modalidad más utilizada, los delincuentes informáticos aplican técnicas en donde investigan y conocen los hábitos de sus posibles víctimas, logrando que las personas proporcionen su información personal, cometiéndose fraudes que ocasionan grandes pérdidas.

Sexto entrevistado: Existen muchas formas, la más aplicada por los antisociales es la ingeniería social, donde el usuario es el eslabón más débil para obtener más beneficios.

Séptimo entrevistado: De los casos receptados en la Unidad de Delincuencia Organizada Transnacional e Internacional, se ha podido determinar que los antisociales cometen los delitos informáticos a través de:

- Suplantación de identidad de personas naturales o jurídicas difundiendo información a través de redes sociales y plataformas de Internet.
- Prestar créditos por las entidades crediticias privadas, para inducir al error a la víctima y aprovecharse de la información, realizando hackeos de dichas cuentas.
- Hackeo de cuentas personales de correo electrónico por las redes sociales (Facebook), desbloqueando las claves de ingreso y acceso obteniendo información confidencial.
- La transferencia electrónica de dinero, desde la cuenta de la víctima a cuentas de terceras personas.
- La introducción de software y virus maliciosos, a través de los correos electrónicos, donde al momento de abrir y descargar el mensaje, se cumple la función delictiva.

Octavo entrevistado: Los delincuentes informáticos son personas con conocimientos avanzados, es decir son hackers, los mismos que buscan entrar en los sistemas de los medios

electrónicos. Entre las formas que utilizan para cometer estos delitos está la suplantación de identidad, hackear claves de cuentas bancarias, estafa de dinero, creación de perfiles falsos, virus informáticos y malware.

Noveno entrevistado: Los delincuentes informáticos tienen muchos mecanismos como el acceso a plataformas, redes sociales, la creación de perfiles falsos, apropiarse de información de terceros, hackeo de correos electrónicos, notificaciones que no son reales y la suplantación de identidad, entre otros, con estos actos logran obtener la información personal de las víctimas, cometiendo los delitos informáticos.

Décimo entrevistado: Los antisociales operan hackeando la información del usuario por los medios electrónicos, debido a que se coloca mucha información en las redes sociales, además la transferencia de recursos o fondos de entidades financieras a otras cuentas para luego ser retiradas, también realizan hackeos en los cajeros automáticos donde colocan dispositivos para grabar la clave de acceso de las tarjetas de crédito y poder sustraer dinero afectando la economía.

Comentario de la autora: De acuerdo con las respuestas proporcionadas por los entrevistados en esta pregunta, comparto la opinión de cada uno de ellos, porque los ciberataques y ciberamenazas, que se realizan a los dispositivos electrónicos, son por medio de la ingeniería social donde los delincuentes informáticos gracias a su gran conocimiento del manejo de las tecnologías de la información y la comunicación, pueden obtener la información personal de sus víctimas sin necesidad de mostrar su identidad.

Los delitos informáticos son todas aquellas acciones ilegales que se cometen por los sistemas informáticos u otros dispositivos de comunicación, los mismos que han evolucionado a la par de la innovación de la tecnología, se encuentran reconocidos y tipificados en el Código Orgánico Integral Penal, donde se estipula las sanciones correspondientes a las personas que cometan estas actividades ilícitas.

Por lo expuesto anteriormente es importante que el Estado brinde la protección ante los riesgos del ciberespacio, implementando herramientas de ciberseguridad, para generar confianza a la población en el momento de utilizar sus dispositivos electrónicos.

Tercera pregunta: **¿En qué nivel de educación, cree usted, que es recomendable propiciar el conocimiento sobre la Ciberseguridad para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?**

Respuestas:

Primer entrevistado: Se debe empezar a impartir conocimientos sobre ciberseguridad o seguridad de la información, desde la primaria de manera progresiva, debido al incremento en el uso de la tecnología en los niños y a las ciberamenazas existentes en Internet.

Segundo entrevistado: El conocimiento sobre el uso de la tecnología y la ciberseguridad debe ser desde la edad más temprana, ya que actualmente somos muy dependientes a la tecnología y un mal uso de esta, ocasiona grandes consecuencias.

Tercer entrevistado: La educación en ciberseguridad y delitos informáticos debería empezar muy temprano en la escuela, puesto que los niños desde muy pequeños utilizan dispositivos electrónicos como Tablet, computadores, celulares, etcétera, siendo muy susceptibles de recibir ataques informáticos.

Cuarto entrevistado: Se debe empezar a impartir conocimientos sobre ciberseguridad, de manera progresiva desde la primaria, porque los niños y niñas crecen en un espacio donde el uso de la tecnología es generalizado y avanzado.

Quinto entrevistado: Para propiciar las buenas prácticas de las Tecnologías de la Información y la Comunicación, se debe proporcionar la educación desde la primaria, porque desde ese momento los niños se exponen a diferentes riesgos con el uso de la tecnología.

Sexto entrevistado: La educación sobre ciberseguridad debe empezar desde que el ser humano es un niño, porque actualmente ya utilizan la tecnología en su diario vivir, pudiendo ser víctimas de los cibercriminales.

Séptimo entrevistado: La ciberseguridad debería formar parte de la malla curricular obligatoria desde el segundo nivel de educación. Actualmente los niños, niñas y adolescentes se encuentran constantemente interactuando en los sistemas informáticos, siendo más susceptibles de ser víctimas de delitos informáticos.

Octavo entrevistado: La educación sobre ciberseguridad debe implementarse en todos los niveles, empezando en el hogar con los niños, porque ellos ya usan la tecnología. Todos necesitamos tener conocimientos amplios porque podemos ser engañados por los delincuentes informáticos.

Noveno entrevistado: La ciberseguridad debe aplicarse en todos los niveles de educación, empezando desde los más pequeños, que son nativos informáticos, es decir, que nacen con la tecnología en sus manos. Todos tenemos la corresponsabilidad de cuidar nuestra información personal en el ciberespacio, que es el sitio donde se desarrollan los delitos informáticos.

Décimo entrevistado: Se debe implementar la educación sobre ciberseguridad desde el nivel básico, porque los niños antes de ir a la escuela ya utilizan los medios electrónicos, evitando de esta forma que se cometan los delitos informáticos.

Comentario de la autora: En cuanto a esta pregunta y los comentarios obtenidos por los entrevistados, estoy en total acuerdo, como sabemos hoy en día la creciente sofisticación de la tecnología ha provocado la existencia de una dependencia digital, donde su uso es generalizado, por tal razón es pertinente que se imparta una educación sobre ciberseguridad en todos los niveles educativos, empezando desde el hogar, ya que los niños y niñas son nativos informáticos, es decir, que nacieron con la tecnología y desde muy pequeños tienen acceso al Internet, siendo este el medio por el cual los delincuentes informáticos cometen sus actos delictivos, a través de ciberamenazas y ciberataques, vulnerando los derechos de todas las personas involucradas.

Cuarta pregunta: ¿Podría usted indicar, cuáles son los medios tecnológicos más adecuados y la protección que el Estado brinda a través de la Política y Estrategia de Ciberseguridad?

Respuestas:

Primer entrevistado: Todos los medios tecnológicos o dispositivos conectados a la red de datos pueden ser vulnerados por los ciberdelincuentes, con la finalidad de obtener algún beneficio personal o económico. El Estado ecuatoriano mediante la Política y Estrategia de Ciberseguridad busca resguardar la seguridad pública y ciudadana en el ciberespacio, para detectar y prevenir los incidentes informáticos.

Segundo entrevistado: Considero que todos son un peligro inminente, debido a que los delincuentes informáticos a través de sus amplios conocimientos, pueden vulnerar cualquier medio electrónico existente.

La Política y la Estrategia Nacional de Ciberseguridad, es la protección que el Estado brinda a la población en general para disminuir los delitos informáticos, es la herramienta para fortalecer la seguridad informática de todos los sectores, a través de la difusión, propiciando el conocimiento y correcta aplicación de la misma.

Tercer entrevistado: El Estado brinda protección a la población ecuatoriana, a través de la Política y Estrategia de Ciberseguridad existente en nuestro país, con estos lineamientos se pretende reducir las ciberamenazas y ciberataques en el ciberespacio.

Los medios tecnológicos existentes no son adecuados; para que exista una mayor efectividad de los mismos se debe implementar los sistemas antifraudes. Así mismo, se debe incrementar la educación a los usuarios de los sistemas informáticos.

Cuarto entrevistado: Todos los medios tecnológicos o dispositivos conectados a la red de Internet, pueden ser vulnerados por los delincuentes informáticos. La correcta utilización por parte de los usuarios, la instalación de software oficial, escaneo de virus, instalación de parches de seguridad y el conocimiento sobre la ciberseguridad o seguridad digital, permitirá reducir el riesgo de ser víctimas de ataques informáticos.

El Estado busca cuidar la seguridad informática de todos los ecuatorianos, incrementando la detección, prevención y gestión de los riesgos existentes en el espacio digital, empleando la ciberseguridad de manera oportuna, efectiva, eficiente y coordinada.

Quinto entrevistado: Cada uno de los medios tecnológicos existentes no son seguros, por lo tanto, a través de la Política y Estrategia de Ciberseguridad se buscan los procedimientos más adecuados, implementando herramientas de seguridad. Se debe capacitar y concientizar a las personas sobre los riesgos del uso de la tecnología.

Sexto entrevistado: Creo que ningún medio tecnológico es el más seguro. El Estado por medio de la Política y Estrategia de Ciberseguridad protege a la población ecuatoriana de los delitos informáticos, por lo que debe propiciar el conocimiento sobre las formas de prevenir y mitigar las ciberamenazas y ciberataques, que vulneran la información que es el activo más valioso de cada persona en la actualidad.

Séptimo entrevistado: Todos los medios tecnológicos, pueden ser utilizados por los antisociales para realizar conductas delictivas, por lo que ninguno es seguro.

La Política y Estrategia poseen las normas de prevención y control ante las conductas delictivas de tipo informático, protegiendo los bienes jurídicos de las personas, instituciones públicas y privadas e incluso del Estado, que se encuentran afectados por estos actos antijurídicos.

Octavo entrevistado: Ningún medio tecnológico es seguro, todos tienen el riesgo de ser comprometidos por las ciberamenazas y ciberataques producidas por los antisociales.

El Estado debe proteger las plataformas institucionales del sector público y privado, las mismas que poseen la información reservada. Además, contratar personal capacitado en temas de ciberseguridad, es decir profesionales éticos que protejan los sitios web, interfiriendo, monitoreando y combatiendo los ataques maliciosos de los cibercriminales.

Noveno entrevistado: Todos los medios tecnológicos son adecuados, cuando tienen acceso a varios filtros de seguridad como la huella dactilar, la confirmación del correo electrónico, verificación facial, entre otros.

El Estado a través de la Política y Estrategia de Ciberseguridad, pretende asegurar la información de los ciudadanos a nivel nacional, para impedir que se incrementen los delitos informáticos.

Décimo entrevistado: Los medios tecnológicos son la computadora, Tablet, teléfonos celulares, etcétera, todos pueden ser vulnerados, no son seguros.
No debemos utilizar lugares públicos para realizar nuestras actividades personales, hay que hacerlo en un espacio privado, con nuestra propia red de Internet.
Por medio de la Política y Estrategia de Ciberseguridad, el Estado garantizará un mayor control de la información confidencial existente en el ciberespacio de las personas naturales y jurídicas.
Comentario de la autora: Del comentario emitido por los entrevistados, comparto la opinión, donde mencionan que ningún medio tecnológico es seguro, porque los dispositivos al estar conectados a Internet, pueden ser utilizados por los delincuentes informáticos, apropiándose de la información de los usuarios para cometer los delitos informáticos.

Para que estos medios tecnológicos sean confiables se debe colocar antivirus efectivos, además instalar un firewall o cortafuegos, el mismo que protege los equipos individuales, servidores o equipos conectados en red, contra accesos no deseados de intrusos que pueden obtener datos confidenciales.

El Estado ecuatoriano ha planteado la Política y Estrategia Nacional de Ciberseguridad para proteger a los usuarios que navegan y realizan sus actividades a través del ciberespacio, con la finalidad que exista una confianza digital al momento de utilizar las tecnologías de la información y la comunicación.

Quinta pregunta: **¿Podría usted indicar, en qué consiste la Política y Estrategia Nacional de Ciberseguridad implementada en el Ecuador, para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos?**

Respuestas:

Primer entrevistado: La Estrategia Nacional de Ciberseguridad, se articula en torno a seis pilares, de los cuales se derivan y definen los Objetivos Estratégicos:

1. Gobernanza y coordinación nacional: Establece un enfoque coordinado de la ciberseguridad nacional.
2. Resiliencia cibernética: Pretende mejorar la resiliencia cibernética a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos.
3. Prevención y lucha contra la cibercriminalidad: Fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos.
4. Ciberdefensa nacional: Reforzar las capacidades de ciberdefensa para proteger las Infraestructuras de Información Crítica nacionales, los servicios esenciales del Estado

y desarrollar capacidades en ciber inteligencia que permitan obtener información útil y oportuna de las amenazas en el ciberespacio para la toma de decisiones.

5. Habilidades y capacidades de ciberseguridad: Mejorar las habilidades y capacidades cibernéticas de la nación en todos los niveles.
6. Cooperación internacional: Maximizar los beneficios de la cooperación internacional.

Segundo entrevistado: La Política y Estrategia de Ciberseguridad, se planteó para proteger a los usuarios que realizan sus actividades a través del ciberespacio, es por ello que el Estado creó este instrumento para construir y fortalecer el desarrollo social, económico y humano del Ecuador.

Tercer entrevistado: La Estrategia Nacional de Ciberseguridad fue presentada en junio del año 2022, por el Gobierno Nacional del Ecuador, es una herramienta que fija lineamientos para proteger a los ciudadanos, fortaleciendo la ciberseguridad del sector público y privado.

Esta Estrategia se realizó en conjunto con el sector privado, académico, público y expertos tanto internacionales como nacionales en ciberseguridad.

Consta de seis ejes o pilares:

1. Gobernanza y coordinación nacional.
2. Resiliencia cibernética.
3. Prevención y lucha contra la cibercriminalidad.
4. Ciberdefensa nacional.
5. Habilidades y capacidades de ciberseguridad.
6. Cooperación internacional.

Cuarto entrevistado: La Estrategia Nacional de Ciberseguridad del Ecuador, se articula en seis pilares, que se detallan a continuación:

1. Gobernanza y coordinación nacional: Consiste en establecer un enfoque coordinado de la ciberseguridad nacional.
2. Resiliencia cibernética: Mejorar la resiliencia cibernética a nivel nacional para prepararse, responder y recuperarse de los incidentes cibernéticos.
3. Prevención y lucha contra la cibercriminalidad: Fortalecer las capacidades para prevenir, investigar y perseguir los delitos informáticos.
4. Ciberdefensa nacional: Mejorar las capacidades de ciberdefensa para proteger las Infraestructuras de Información Crítica nacionales y los servicios esenciales del Estado.
5. Habilidades y capacidades de ciberseguridad: Estas deben ser ampliadas en todos los niveles con relación a la ciberseguridad en Ecuador.
6. Cooperación internacional: Debe existir la cooperación internacional con otros Estados.

Quinto entrevistado: La Política y Estrategia Nacional de Ciberseguridad, son lineamientos que establece el Estado en relación a las políticas, procedimientos y buenas prácticas que deben aplicar las empresas, instituciones públicas y privadas, la ciudadanía y el Estado, con el objetivo de construir y fortalecer las capacidades nacionales que permitan garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La Política establece directrices que buscan afianzar el ciberespacio y la Estrategia tiene como fin mejorar la resiliencia cibernética de la sociedad ecuatoriana.

Sexto entrevistado: La Política Nacional de Ciberseguridad está enfocada en prevenir, gestionar, mitigar, monitorear, evaluar e identificar los riesgos y amenazas que están expuestas las personas, empresas, instituciones públicas y privadas, incluso el propio Estado ecuatoriano. La Estrategia Nacional de Ciberseguridad se realizó con la finalidad de mejorar la resiliencia cibernética de la sociedad ecuatoriana.

Séptimo entrevistado: La Estrategia Nacional de Ciberseguridad vigente desde el año 2022 al 2025, presentada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, es una herramienta que fija lineamientos para fortalecer la ciberseguridad del país. Pretende generar conciencia al titular de la información, a efecto de evitar que la misma se transfiera a terceras personas y se realice el uso indebido de la información personal, evitando el aumento de los delitos informáticos en el Ecuador.

Octavo entrevistado: La Política y Estrategia de Ciberseguridad tiene como fin resguardar la información del Estado y de la sociedad en general, con la ayuda de varias leyes como la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, la Ley de Protección de Datos, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, logrando que los derechos de todas las personas sean respetados.

Noveno entrevistado: La Política y Estrategia de Ciberseguridad que el Estado ha implementado, sirve para prevenir y erradicar las ciberamenazas y ciberataques producidos por los delincuentes informáticos, garantizando que los derechos de las personas y la información se encuentren resguardados.

Décimo entrevistado: La Política y Estrategia de Ciberseguridad del Ecuador son directrices que el Estado proporciona para evitar las conductas delictivas contra la ciudadanía.

El Estado se ampara en la ley como medio coercitivo, además se apoya de las instituciones como la Policía Nacional, el Ejército y las Secretarías de Inteligencia encargadas de detectar a las organizaciones delictivas.

Comentario de la autora: De la información emitida por los entrevistados, puedo manifestar que estoy de acuerdo, considerando que la Política y Estrategia Nacional de Ciberseguridad fue

realizada por el Estado con el objetivo de construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población ecuatoriana y la protección de los bienes jurídicos del Estado en el ciberespacio.

Nuestras actividades diarias las realizamos a través del mundo digital, el trabajo, la comunicación, los negocios, las transacciones, es decir interactuamos en línea, por lo que es propicio que el Estado cree medidas acertadas, para impedir la delincuencia informática que nos asecha en todo momento, vulnerando así nuestros derechos fundamentales consagrados en la Constitución de la República del Ecuador.

Sexta pregunta: ¿Qué sugerencia daría usted ante la problemática planteada?

Respuestas:

Primer entrevistado: En los últimos años, a partir de la pandemia del COVID-19, se vivió una transformación digital a nivel global, las organizaciones y personas en general tuvieron la necesidad de hacer uso de las nuevas tecnologías, incrementándose las ciberamenazas y ciberataques y con ello los delitos informáticos. Ante esta problemática se plantea lo siguiente:

- A nivel de empresas públicas y privadas, educar a las personas y personal en seguridad informática, ciberseguridad y seguridad de la información.
- Endurecer las leyes y condenas en caso de delitos informáticos en el Ecuador.
- Fortalecer la cooperación a nivel internacional.
- Incluir en la malla curricular para los distintos niveles y subniveles de educación la materia de ciberseguridad.

Segundo entrevistado: El estudio con respecto a la Estrategia y Política de Ciberseguridad debe ser más enfocado en el Pentesting, que es la base para cuidar que no existan ataques a nivel de infraestructura. Con relación a las ciberamenazas debe propiciarse una capacitación a nivel público sobre cómo identificar y prevenir las ciberamenazas ayudando de esta forma a minimizar los delitos informáticos.

Tercer entrevistado: Se requiere:

- Implementar la Política y la Estrategia Nacional de Ciberseguridad a nivel de educación, empezando desde la escuela, colegio y universidad, es decir, en todos los niveles.
- Educación en casa sobre el uso correcto de las tecnologías de la información y la comunicación.
- Fortalecer los controles en las empresas públicas y privadas para evitar ciberataques y ciberamenazas que conllevan a los delitos informáticos.

- Capacitar a las personas y personal encargado de los sistemas informáticos para que implementen la Política y Estrategia Nacional de Ciberseguridad.

Cuarto entrevistado: La sugerencia sería realizar la búsqueda de Políticas y Estrategias implementadas a nivel de Latinoamérica, Estados Unidos, Europa, Asia y realizar un análisis comparativo para lograr identificar que tan efectiva y eficiente es nuestra Política y Estrategia Nacional de Ciberseguridad frente a otros países para enfrentar, prevenir y actuar ante las ciberamenazas, ciberataques y los delitos informáticos, logrando con ello mejorar las políticas vigentes en nuestro país.

Quinto entrevistado: La ciberseguridad se debe encontrar en todo lugar, por lo que, la Estrategia y Política vigentes en el Ecuador se deberían aplicar tanto en el sector público como privado y en la sociedad en general, esto nos permitirá fortalecerla, evitando de esta forma los altos índices de delitos informáticos.

Sexto entrevistado: El Estado debe difundir a todas las personas a través de la prensa, radio, televisión y demás medios de comunicación, sobre la Política y Estrategia de Ciberseguridad, debido a que el 80% de la población ecuatoriana, no tiene conocimiento de cómo aplicar la seguridad para proteger la información confidencial de cada uno de ellos.

Séptimo entrevistado: Se debe analizar si las políticas públicas implementadas por el Estado son las propicias y adecuadas, de serlo así, difundirlas a nivel de toda la ciudadanía e incluir en la malla curricular de estudio desde el segundo nivel de educación, con la finalidad de que toda la población ecuatoriana tome conciencia de los riesgos existentes en el ciberespacio y adopte una cultura de ciberseguridad.

Octavo entrevistado: Establecer una cultura de ciberseguridad, implementando la educación en todos los niveles, para concientizar los riesgos que genera el mal uso de las tecnologías de la información y la comunicación.

Además, no se debe divulgar información personal por las redes sociales, porque los delincuentes utilizan estos datos para comprometer los sistemas informáticos de los dispositivos y cometer sus actos delictivos.

Noveno entrevistado: Realizar la difusión de la Política y Estrategia de Ciberseguridad para todas las personas del país, con la finalidad de proporcionar la información precisa sobre cómo identificar, prevenir y resguardar la información confidencial, logrando que disminuyan los altos índices de delitos informáticos.

Décimo entrevistado: Se debe mantener tipificadas y sancionadas las conductas delictivas en el Código Orgánico Integral Penal. Además, se informe y prepare a la ciudadanía con

conocimientos de ciberseguridad, para evitar que sean sujetos pasivos de los delitos informáticos, con el apoyo de las instituciones de seguridad pública.

La información personal de cada ciudadano debe ser reservada, porque si la exponemos puede ser un peligro que ocasiona pérdidas considerables.

Comentario de la autora: Las respuestas proporcionadas por los profesionales entrevistados, son de gran aporte al presente Trabajo de Integración Curricular, porque sus sugerencias permiten entender que el uso inadecuado de la tecnología y sus medios electrónicos, ocasiona graves perjuicios que vulneran, menoscaban o dañan a las personas y entidades del Estado poniendo en riesgo la estabilidad del país.

La protección ante este peligro que son los delitos informáticos, se consigue con la correcta aplicación y ejecución de las medidas de ciberseguridad, para generar confianza en la población en el momento de utilizar dichos medios, garantizando los derechos de las personas y evitar que se cometan este tipo de conductas delictivas que comprometen la información personal y confidencial.

6.3. Estudio de Casos.

Caso No. 1

1. **Datos Referenciales:**

Juicio No 09292201800176

Actor/ Ofendido: Ab. L. M.

Procesado: O. O. H. D.

Juzgado: UNIDAD JUDICIAL PENAL SUR CON COMPETENCIA EN DELITOS FLAGRANTES CON SEDE EN EL CANTÓN GUAYAQUIL, PROVINCIA DEL GUAYAS.

Delito: ART. 195 INFRAESTRUCTURA ILÍCITA.

Fecha: 13/06/2018

2. **Antecedentes:**

El viernes 6 de julio de 2018 a las 15h18, el Juez de la Unidad Judicial Penal con Competencias en Delitos Flagrantes de Guayaquil, avocó conocimiento del parte de detención de la ciudadana O. O. H. D, a quien en audiencia del 13 de Junio del 2018 a las 18h15, en virtud de lo dispuesto en los artículos 527 y 529 del Código Orgánico Integral Penal, se le declaró como legal su detención y el de flagrante la infracción. El señor Fiscal en uso de sus competencias, formuló cargos en contra de O. O. H. D, imputándola como posible responsable del delito de

Receptación inciso primero conforme lo dispone el Art. 202 y del Artículo 195 por Infraestructura Ilícita mediante una concurrencia real de infracciones tipificada en el Art. 20 del Código Orgánico Integral Penal, a partir de la noticia hecha a conocer a través del parte policial informativo suscrito por los señores policías CAPIT. G. V. A. H; TENIENTE G. V. M; TENIENTE G. M. H. R; SGTO N. S. R. A; CBOP. G. F. D. G; CBOP. R.T. H.; CBOP. C. L. W. N.; CBOP. S. A. D. O; CBOS. G. Q. P. F; CBOS. G. G. G. G. Quienes dan conocer los hechos investigativos y delictual según el expediente de fojas 1 a la 10 que indican que mediante una orden de allanamiento concedida por esta misma autoridad comparecieron hasta el local ubicado en las calles Eloy Alfaro Delgado entre Manabí y Ayacucho local N.- 04-0102-00294 y al identificarse como policías tomaron contacto con la ciudadana O. O. H. D, quien se identificó como la propietaria a quien se le pidió autorización para proceder a un registro y verificación del mismo, encontrando sobre una vitrina una computadora Portátil color Negro marca Sony modelo SVE14AA12U Serie 00194-402-962-811 y en el escritorio de la misma se encontraba abierta una ventana o herramienta con el nombre de ODIN encontrándose conectados a varios cables, por lo que la ciudadana O. O. H. D, desconecto el disco duro, una herramienta de flasheo y un celular pequeño color blanco procediendo a guardar en sus partes íntimas, por tal razón fiscalía solicito el registro corporal de la ciudadana, encontrando en su poder un equipo terminal marca Samsung color blanco Modelo Gt.I8160L, Gama media, Imei 352053051131814 en regular estado sin tapa posterior, sin chip, sin memoria con batería reportado como robado, perdido o hurtado en la página de la Arcotel en la fecha 25 de febrero de 2018, así mismo un disco duro externo, un lector de chips con cámara de flasheo sin numeración y posterior a la verificación y registro del local procediendo a solicitarle la respectiva documentación o contratos que justifiquen su titularidad de tales equipos, la cual indicó que no poseía facturas, ordenes de trabajo, etc., se procedió así mismo a la verificación de los imeis de los diferentes terminales móviles existentes en el lugar en la página web Arcotel incautando varios equipos terminales que se describen en el parte policial esto es 9 celulares, una Tablet, un disco duro marca Toshiba, un USB marca GPG, un USB Marca Huawey, Dos chip de la Operadora Claro, un chip de la operadora TMOBILE, un chip de la operado Movistar, un chip de la operadora SPRINT, Ocho tarjetas de memoria micro SD de 1, 2 y 4 Gigabyte; Dos adaptadores Lectores Micro Sd, una computadora Portátil color negro marca Sony y una mochila Totto. Por lo que al ser puesto en consideración al señor fiscal el mismo que dispuso la aprehensión de la ciudadana O. O. H. D, acogiéndose a lo que determina el Art. 444 numeral 9 del Código Orgánico Integral Penal, así mismo siendo respetados sus derechos y garantías básicas dispuestas en el Art. 77 numeral 2, 3, 4 de la Constitución de la República. Para posterior

ser ingresada en aseguramiento Transitorio de la policía judicial para su respectiva audiencia; el señor Fiscal, por estarle permitido al tenor de lo dispuesto en el numeral 2 del artículo 635 del Código Orgánico Integral Penal, manifestó la propuesta de un procedimiento abreviado el cual fue acogido por la defensa técnica de la Procesada, de lo cual el Abogado de la Defensa puso en conocimiento de la parte Procesada, la misma que manifestó su consentimiento. Habiendo las partes procesales llegado a un acuerdo en la pena, que es de es de DOCE meses de privación de la libertad. El Suscrito Juez admitió tramitar en procedimiento abreviado de conformidad con los artículos 635, 636 y 637 del Código Orgánico Integral Penal. Con respecto a la existencia material de la infracción y la responsabilidad penal de la Procesada que se encuentra comprobada conforme a derecho; con el contenido del parte de detención de la ciudadana O. O. H. D. suscrito por los señores policías antes mencionados; el INFORME DE RECONOCIMIENTO DEL LUGAR DE LOS HECHOS N.- 127-2018-UDF-PORTETE SUSCRITO POR EL AGENTE POLICIAL J. G. P; INFORME INVESTIGATIVO N.- 4876-2018-PJ-Z8 SUCRITO POR EL AGENTE INVESTIGADOR CBOP. C. P. S; INFORME DE RECONOCIMIENTO Y AVALUO DE EVIDENCIAS N.- DCGIT1803624 SUSCRITO POR EL PERITO POLICIAL J. D. G. Y; INFORME PERICIAL DE INFORMÁTICA FORENCE SUSCRITO POR EL TENIENTE DE POLICÍA J. E. Z. P y, la propia aceptación de la participación de la procesada O. O. H. D.

3. Resolución:

Por lo antes expuesto, el Doctor Marco Eduardo Guerra Guerrero, Juez de Garantías Penales del Guayas, en funciones de Juez de la Unidad Judicial Penal con Competencias en Delitos Flagrantes de Guayaquil, por considerar justificada la existencia del delito y la responsabilidad penal de la Procesada, de conformidad con lo dispuesto por el primer inciso del artículo 621 del Código Orgánico Integral Penal ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, declara a la señora O. O. H. D, RESPONSABLE en el grado de AUTOR del delito tipificado y reprimido en el primer inciso del artículo 202 del Código Orgánico Integral Penal y el Articulo 195 por Infraestructura Ilícita, mediante una concurrencia real de infracciones tipificada en el Art. 20 del Código Orgánico Integral Penal, imponiéndose la pena de DOCE MESES DE PRIVACIÓN DE LA LIBERTAD Y MULTA DE TRES SALARIOS BÁSICOS UNIFICADOS DEL TRABAJADOR EN GENERAL, en aplicación de los principios de proporcionalidad y razonabilidad, y en atención a lo dispuesto en el tercer inciso del artículo 636 del Código Orgánico Integral Penal y la regla determinada

en el numeral 4 del artículo 70.- La multa deberá ser satisfecha mediante depósito en la cuenta corriente número 750006-8 sublínea 170499 del Banco del Pacifico a nombre del Consejo de la Judicatura.- La Sentenciada cumplirá la pena en el Centro de Privación de Libertad de Personas Adultas en Conflicto con la Ley Guayaquil Nº 1, Hágase conocer al Director del Centro de Privación de Libertad de Personas Adultas en Conflicto con la Ley Guayaquil Nº 1. Dispongo que se obtengan copias de esta sentencia en el Libro respectivo. Se dispone el comiso de la evidencia materia de esta infracción.

4. **Comentario de la Autora:**

En el presente caso, se evidencia el cometimiento de la infracción tipificada en el Art. 202 y el Art. 195 del Código Orgánico Integral Penal, donde se hace referencia al delito de receptación y al de infraestructura ilícita. Es importante indicar que este último delito está contemplando como una de las infracciones informáticas, teniendo en cuenta que la infraestructura ilícita se produce cuando una persona posee infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil; de acuerdo con el Código Orgánico Integral Penal vigente en nuestra normativa ecuatoriana, este delito tiene una sanción de uno a tres años de pena privativa de libertad.

En los delitos antes mencionados, el objeto material de la infracción, lo encontramos en los equipos terminales móviles que estuvieron en posesión de la procesada, algunos de ellos reportados como robados, perdidos o hurtados en la página web de la Arcotel, así como también la ventana o herramienta denominada ODIN, la cual le servía para la realización del acto delictivo, obteniendo datos importantes para alterar la información de un equipo terminal móvil, que es un dispositivo tecnológico que permite la comunicación entre personas, utilizando la telefonía móvil y la mensajería instantánea a tiempo real, sin importar la distancia existente entre dos o más dispositivo conectados a una red de Internet o datos móviles.

El daño causado es la alteración o modificación de la información de identificación de los equipos terminales móviles existentes, además, el no poseer la respectiva documentación o contratos, que justifiquen a la procesada como la titular de los equipos encontrados en el local comercial, en el momento del allanamiento realizado por la Policía Nacional bajo la orden de la autoridad competente.

Caso No. 2

1. **Datos Referenciales:**

Juicio No 01283201502767

Actor/ Ofendido: C. B. R. G.

Procesado: G. G. M. M.

Juzgado: UNIDAD JUDICIAL PENAL CUENCA

Delito: 231 TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL

Fecha: 12/05/2015

2. **Antecedentes:**

El 29 de junio del 2015, a las 07h40. De conformidad con el Art. 609 del Código Orgánico Integral Penal, la etapa de juicio se sustancia sobre la base de la acusación fiscal, se tramitó por el Procedimiento Directo previsto en el Art. 640 en relación con el artículo 610 y siguientes del Código Orgánico Integral Penal para resolver la situación jurídica de M. M. G. G, a quien Fiscalía acusó por el delito de Transferencia electrónica de activo patrimonial, tipificado y sancionado en el primer inciso del artículo 231 del Código Orgánico Integral Penal. Una vez concluida la audiencia de juicio, en cumplimiento a lo que dispone el Art. 619 del Código Orgánico Integral Penal, se anunció en forma oral la decisión judicial, dictando sentencia condenatoria, por la existencia de la infracción y de la culpabilidad penal de la procesada.

El Fiscal P. M. M, indica que el día 12 de mayo del 2015, a eso de las 11h00, se recibe en la cooperativa JEP un reclamo de R. G. C, que informa a los directivos de la misma que ha recibido mensajes de texto de transferencias electrónicas no autorizadas, ingresando al sistema on line, constando como si hubiese realizado una trasferencia desde su cuenta hasta la de M. G. G, por usd. 4820,oo y otras transferencias más, por lo que ese día a eso de las 12h00, presentó la denuncia en el cantón Durán, provincia del Guayas, una vez emitida una alerta sobre este particular a las 12h15 en la sucursal de Balzay en la ciudad de Cuenca, se acercó la procesada G. G. M. M, para retirar dinero en efectivo, procediendo a su detención, se le acusa por el delito de transferencia electrónica tipificado y sancionado en el artículo 231 COIP en relación con el artículo 42.3 del Código Orgánico Integral Penal. El Abg. de la defensa M. B. indica que M. G. G, no ha cometido ningún delito de transferencia, que un día anterior el 11 de mayo del 2015, a las 15h00, cuando estaba en su local se acercó el señor R. G. G, indicando que desea adquirir un vehículo en usd. 5.800,oo, luego de conversar con el hermano de la procesada, acuerdan que

el pago lo haga con un depósito en la JEP por usd. 5000,oo y los restantes 800 en efectivo al día siguiente, el 12 de mayo recibe la llamada de G. indicando que ya está la transferencia, la procesada se acercó a la Cooperativa JEP a verificar el depósito, esta no estaba en su totalidad sino usd. 4.800,oo; ella sale de la cooperativa para reclamar los 200 que faltan; G. le dice que le entregará cuando le de las llaves y la matrícula del vehículo. Ella posee un taller de mecánica y necesitaba repuestos, quiso sacar dinero y en la ventanilla le dijeron que por ser un valor elevado necesita autorización, o le daban un cheque, saca 4.000,oo para pagar una deuda que era emergente y luego le detienen sin haber ningún tipo de delito.

Las pruebas aportadas por la fiscalía son la recepción de los testimonios de R. G. C. B; I. M. Z. G., A. C. F. P; L. A. T. V; K. G. L. Q; C. R. C, como prueba documental presenta Denuncia del Señor I. Z, denuncia presentada por R. G. C. B, estados de cuenta ocasionales de M. M. G. G., y de R. G. C, documentación de apertura de ambas cuentas, el parte policial informativo, videos de cámaras, informe de reconocimiento del lugar de los hechos, documentación remitida por la Cooperativa JEP que da a conocer los movimientos de la procesada y la víctima en horas exactas de las transferencias de las cuentas de éstos. En la prueba de la defensa técnica de la procesada se reciben los testimonios de L. M. A. C; J. J. L. Y; C. A. M. T; L. F. G. G; como prueba documental presenta certificados de antecedentes penales, honorabilidad y de trabajo.

Fiscalía expresó que el día martes 12 de mayo del presente año, se había realizado una transferencia a la cuenta de G. G. M. M., desde la cuenta del señor C. B. R. G, esta transferencia jamás fue autorizada. La Fiscalía indica que se ha justificado la acusación, existencia de la infracción y responsabilidad. Con la documentación se certifica que efectivamente se realizó una transferencia por la suma de Usd. 4.200,oo a las 10h35 y a las 11h00 ya es detenida G. G. M. M.L, los testimonios son contundentes, y la prueba documental entregada justifica, que existió un delito de Transferencia Electrónica Patrimonial tipificada y sancionada en el artículo 231, segundo inciso del Código Orgánico Integral Penal, por lo que acusa a G. G. M. M. en calidad de autora de esta infracción, pide se dicte sentencia condenatoria, y solicita que el valor de usd. 4820,oo se devuelta a la víctima y se aplique la multa respectiva.

La defensa técnica de la procesada expresa que la acusación fiscal es por el artículo 231 del Código Orgánico Integral Penal, sustenta que no existe informe pericial que establezca la dirección IP desde la que se hizo la transferencia, que la señora G. hubiese accedido a la base de datos, no existe ningún documento que pruebe la existencia del delito. El señor C. dice que ingresó en internet sus datos, claves; que no se conocen la procesada y la víctima, que hubo la

negociación de un vehículo, por eso fue la transferencia, el único inconveniente que tuvo fue facilitar la cuenta para depositar el dinero de esa negociación.

3. **Resolución:**

Por lo expuesto, el Juez, en uso de sus atribuciones legales, "ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR, Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA", declaró a la ciudadana M. M. G. G, como autora y responsable de la infracción tipificada y sancionada en el segundo inciso del artículo 231 del Código Orgánico Integral Penal, imponiéndose la pena privativa de libertad de 3 años, que la cumplirá en el Centro de Privación de Libertad de Personas Adultas en Conflicto con la Ley Regional Centro Sur Turi, y la pena restrictiva del derecho de propiedad, de multa de 10 remuneraciones básicas unificadas del trabajador de conformidad con lo dispuesto en el artículo 70 numeral 7 del Código Orgánico Integral Penal. Dando cumplimiento al principio establecido en el artículo 78 de la Constitución de la República del Ecuador, se fija en atención a la realidad de los hechos, el perjuicio ocasionado a la víctima por la transferencia realizada, teniendo en cuenta que la misma no tiene su domicilio en esta ciudad de Cuenca, en donde se sustancio esta causa, y a donde acudió a fin de colaborar con el sistema de administración de justicia penal, se fija dos remuneraciones básicas unificadas del trabajador, la indemnización por daños y perjuicios que cancelará M. M. G. G, en favor de R. G. C. B. La defensa de la sentenciada dentro del plazo establecido en el artículo 630 del Código Orgánico Integral Penal solicitó la SUSPENSIÓN CONDICIONAL DE LA PENA, y se señaló día y hora para la audiencia, en la misma la defensa justificó que se cumplen con todos los requisitos del Art. 630 del Código Orgánico Integral Penal. En base al principio de contradicción se corrió traslado con la documentación presentada por la defensa y su petición al señor Fiscal, al Dr. I. Z, Abogado de la Cooperativa JEP y a la víctima R. G. C. B, quienes se allanaron al pedido. Por lo tanto, la sentenciada durante los TRES AÑOS que dura su pena CUMPLIRÁ las condiciones establecidas en el Art. 631 del Código Orgánico Integral Penal: 1.- Residir en un lugar determinado, informará cualquier cambio de domicilio al Juez de Garantías Penitenciarias, para tal efecto el domicilio de M. M. G. G, está ubicado en el barrio Buenos Aires, de la parroquia Sayausí de la ciudad de Cuenca, provincia del Azuay. 2.- No frecuentar al señor R. G. C. B, 3.- No salir del país sin previa autorización del señor Juez. 4.- Cada 6 meses se justificará con documentos que se encuentra trabajando. 5.- Acreditará con la periodicidad de 6 meses documentación que acredite que está estudiando, justificará cuando egrese de la carrera para cumplir esta condición. 6.- Como trabajo comunitario la Cooperativa de Ahorro y Crédito

Juventud Ecuatoriana Progresista en el plazo de 10 días luego de ejecutoriada esta sentencia, presentará el diseño de una publicidad tipo volante donde constará una breve descripción de estos delitos informáticos, las penas con las que están sancionadas las infracciones y la advertencia de que también es responsable de estas infracciones la persona que facilite su cuenta para realizar los depósitos de valores indebidamente transferidos. El volante será entregado a la sentenciada, quien bajo su responsabilidad costeará la impresión de 3000 ejemplares, que los distribuirá 1000 cada 3 meses, en los sectores más concurridos de la ciudad de Cuenca, a partir de los 90 días siguientes a la ejecutoría de esta sentencia, justificará al Juez el cumplimiento de esta condición. 7.- En el plazo de 60 días luego de ejecutoriada la sentencia donará a la Fundación Luis Vargas Torres, a cargo del Lcdo. F. A, la cantidad de 10 inhaladores para niños con fibrosis quística. 8.- Cancelará el valor de 2 remuneraciones básicas unificadas del trabajador a la Víctima R. G. C. B, mediante depósito en su cuenta, en dos partes, la primera en el mes de julio y la siguiente en el mes de agosto del 2015. 9.- La Cooperativa de Ahorro y Crédito Juventud Ecuatoriano Progresista, dentro del plazo de 3 días posteriores a la ejecutoría de esta sentencia procederá a verificar la reversión de los valores indebidamente transferidos de la cuenta de la víctima R. G. C. B. Nro. 406046222705 a la cuenta de la sentenciada M. M. G. G. Nro. 406007529500, por usd. 4820,oo. Verificada esta transferencia se hará conocer a la sentenciada el cierre de la cuenta, hasta dentro de los 3 días siguientes a la notificación de que los dineros fueron restituidos a su propietario. 10.- Se presentará periódicamente cada 3 meses, el primer lunes de cada mes en horas hábiles en el Juzgado de Garantías Penitenciarias para el control de estas condiciones. 11.- Pagará la multa dispuesta mediante depósito al Consejo de la Judicatura en un plazo no mayor a 8 meses, sin que esto interfiera con el proceso de coactiva, el que será independiente de esta condición cuyo objetivo, es verificar que la sentenciada cumpla con el pago impuesto como pena restrictiva de la propiedad, pudiendo iniciar los procedimientos coactivos a fin de lograr el cobro referido. 12.- No tener sentencia condenatoria por este delito y 13.- No tener nueva instrucción fiscal. La sentenciada fue informada de estas condiciones, así como advertida de que en caso de incumplimiento de cualquiera de ellas se ordenará la ejecución de la sentencia. Aceptada la suspensión condicional de la pena se ordenó la inmediata libertad de M. M. G. G. Ejecutoriada esta sentencia remítase copia certificada de la misma a la Oficina de Sorteos de la Función Judicial de Cuenca, para que mediante sorteo radique la competencia en uno de los señores Jueces o Juezas de Garantías Penitenciarias a fin de que se dé cumplimiento a lo dispuesto en los artículos 632 y 633 del Código Orgánico Integral Penal. Hágase conocer de esta sentencia a la Víctima y a la Cooperativa de Ahorro y Crédito Juventud Ecuatoriano Progresista.

4. **Comentario de la Autora:**

En este caso judicial se demostró que existió el delito informático denominado transferencia electrónica de activo patrimonial, reconocido y tipificado en el Código Orgánico Integral Penal en el artículo 231, que ocurre cuando una persona, con la intención de obtener un beneficio, altera y manipula el funcionamiento de un sistema informático, procurando la apropiación no consentida de un activo patrimonial que son los bienes, valores y derechos, perjudicando a la víctima con este acto ilícito, cuya sanción es de tres a cinco años de pena privativa de libertad.

Así mismo, es sancionada la persona que proporcione datos personales de su propia cuenta bancaria, con la finalidad de recibir ilegítimamente estos activos patrimoniales mediante transferencia electrónica, ocasionando graves daños en el patrimonio de la persona involucrada.

Se configura el delito de transferencia electrónica de activo patrimonial, cuando una persona accede a los recursos del usuario de un banco, sin la autorización del mismo, extrayendo grandes cantidades de dinero, provocando perjuicios en su economía. Para evitar ser víctima de este tipo de delitos informáticos, no se debe compartir con otras personas claves de seguridad, contraseñas, ni información personal en páginas desconocidas o redes sociales, además revisar periódicamente las cuentas bancarias, percatándose de que no existan transferencias de dinero sin su consentimiento.

Caso No. 3

1. **Datos Referenciales:**

Juicio No 09281201900506
Actor/ Ofendido: Fiscalía General Del Estado, C. M. V. M.
Procesados: C. O. C. J, E. M. J. C.
Juzgado: UNIDAD JUDICIAL DE GARANTÍAS PENALES CON COMPETENCIA EN DELITOS FLAGRANTES DE GUAYAQUIL PROVINCIA DE GUAYAS.
Delito: Art. 190 APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS, INC.1
Fecha: 02/02/2019

2. **Antecedentes:**

El 01 de febrero del 2019 a partir de las 11h30 a 17h:45, son detenidos los ciudadanos E. M. J. C y C. O. C. J. en la vía a Daule Calle 24 N-O, y Av. Carlos Julio Arosemena a la altura de la parada de la Metrovía (Colegio 28 de Mayo) de la ciudad de Guayaquil, por lo cual de

conformidad a lo dispuesto en el artículo 529 del Código Orgánico Integral Penal, realizó la audiencia de calificación de flagrancia, en la cual el Fiscal de Turno Ab. P. J. A, por existir presunciones graves y fundadas sobre la existencia del delito y la participación de los entonces aprehendidos hoy procesados, formuló cargos por el delito tipificado en el Art. 190 del Código Orgánico Integral Penal, (DELITO DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS), solicitando las medidas cautelares dispuestas en los numerales 1 y 2 del Art. 522 del COIP, para J. C. E. M; y, la medida cautelar de prisión preventiva (numeral 6) para C. J. C. O. (peruano). En este estado el suscrito Juez aceptó la petición fiscal, disponiendo que se presente cada semana ante la Fiscalía y la prohibición de ausentarse del país, para E; y, prisión preventiva en contra de C. Tomando como antecedentes el Parte de aprehensión suscrito por el Capt. P. C. L. R; Sbte. F. Y. W. G; CboP. Q. R. J. A; CboS. R. V. L. G. y CboS. J. A. J. C. El día 11 de febrero del 2019, a las 08h30 se instaló la audiencia de procedimiento directo en la que el Dr. L. P. M, Fiscal de lo Penal del Guayas, de la Fiscalía N° 2 de la Unidad de Delitos de Flagrancia, a quien le correspondió el conocimiento de esta causa, llegó a un acuerdo con la defensa del procesado C. O. C. J. con respecto a la aplicación de un PROCEDIMIENTO ABREVIADO, suspendiéndose la audiencia a las 09h30 quedando pendiente la situación jurídica del procesado E. J.

Con fecha 20 de marzo del 2019 a las 15h30 se resolvería la situación jurídica del procesado E. M. J. C; por lo que siendo el estado del proceso el de dictar SENTENCIA, para hacerlo se considera los siguientes antecedentes: Según el contenido del Parte de aprehensión de fecha 01 de febrero del 2019 a partir de las 11h30 elaborado por Capt. P. C. L. R; Sbte. F. Y. W. G; CboP. Q. R. J. A; CboS. R. V. L. G y CboS. J. A. J. C, en el que hacen saber: "…Pongo en su conocimiento mi Mayor, que encontrándonos de servicio como BAC Nacional, el día de hoy 1 de febrero del 2019 siendo aproximadamente las 11h30 recibimos la llamada telefónica de parte del señor Jefe de Seguridad del Banco de Machala, señor F. B. M. M, quien manifestó que en la agencia de este Banco, en el Parque California se encontraba una persona que realizó transacciones presuntamente fraudulentas, por lo que nos trasladamos a verificar lo sucedido, tomando contacto con la señora Ma. B. T. E, Gerente de la agencia, que manifestó que el ciudadano de nombres J. C. E. M, se había acercado a dicha entidad a retirar una tarjeta de débito de su cuenta de ahorros No. 138-0037617, y al momento de realizarle un registro corporal entre sus pertenencias se le encontró lo siguiente: 4 papeletas del Banco de Machala, las cuales son tres de retiro por distintas cantidades como son la papeleta con serie No. 42431415; No. 42431413 y 43276586 y una papeleta de depósito con serie No. 55443648

debiendo recalcar que todas las papeletas se encuentran con número de cuenta 1380037617, además un comprobante de transacción a la cuenta No. 1380037617, una cédula de identidad No. 092632553-1, y papeleta de votación, así como además un teléfono Samsung en regular estado de color azul oscuro, y dos billetes de la denominación 20 dólares americanos; de igual manera se tuvo conocimiento por el Jefe de Seguridad que un ciudadano de nombres V. M. C. M, se había acercado a la agencia del Banco de Machala en el cantón El Guabo (provincia de El Oro), donde al intentar retirar el dinero en la cuenta de ahorros No. 1010106865 no poseía los fondos disponibles, acudiendo a la gerencia indicando dicha novedad por lo cual se ha puesto una alerta a nivel nacional, ya que los fondos de cuenta, esto es 978 dólares habían sido transferidos sin su consentimiento y de manera fraudulenta vía electrónica a la cuenta No. 130-0037617, perteneciente al ciudadano J. C. E. M, el día 31 de enero del 2019 a las 10:28 y minutos siguientes fue retirado con libreta, la suma de 975 dólares por parte del mencionado ciudadano. Inmediatamente se le comunicó al señor C. M. V. que había un detenido en la ciudad de Guayaquil y que se traslade hasta esta ciudad al Albán Borja a poner la respectiva denuncia. Que mediante entrevista con el señor E. M. J. (detenido), este manifestó de manera voluntaria que C. O. C. le facilitó el dinero para la apertura de la cuenta de ahorros en el Banco de Machala y posteriormente le había pedido el número para las transacciones bancarias y que el 31 de enero de 2019 le había llamado C. C. indicando que ya estaba hecho el depósito de 975 dólares y que en la tarde pasaría retirando el dinero y que por ello ha retirado la cantidad señalada en la agencia del Banco de Machala ubicado en las calles Calicuchima y Eloy Alfaro y que aproximadamente a las 18h00 le había entregado la cantidad de 975 dólares al señor C. C, quien como reconocimiento de prestarle la cuenta le había entregado la cantidad de 140 dólares americanos. Con estos antecedentes, en persecución ininterrumpida del delito y mediante operaciones básicas de inteligencia (OBI) siendo las 17h45 del (1 de febrero del 2019) se logró detener al ciudadano C. O. C. J. con número de pasaporte peruano 44855889, de nacionalidad peruana, en la avenida Carlos Julio Arosemena a la altura del Colegio 28 de mayo, a quien al hacerle un registro corporal entre sus pertenencias se le encontró en su poder 3 tarjetas de débitos del Banco del Pichincha de diferentes personas; dos billetes de denominación 20 dólares americanos, un baucher de depósito del Banco del Pichincha a nombre de L. L. J. A, con el valor de 6 dólares americanos de fecha 29-01-2019; un celular marca Samsung, regular estado color rosa con blanco. Con estos antecedentes nos trasladamos hasta la fiscalía del Albán Borja en donde se toma contacto con el señor Fiscal de Turno Ab. V. L. T, quien dispuso la aprehensión de C. O. C. J. (peruano) y J. C. E. M. (ecuatoriano), y que se dé cumplimiento a lo que dispone el Art. 444 numeral 9 del Código Orgánico Integral Penal…"; así mismo consta la

denuncia presentada por parte del Sr. V. M. C. M. (víctima), en la que señaló: "…el día de hoy 01 de febrero del 2019 a eso de las 09h30 me acerqué a la agencia bancaria del Banco de Machala ubicada en El Guabo para retirar un dinero, en eso me indican que yo había hecho un trasferencia de mi cuenta No 111010106865 a la cuenta de ahorros del mismo banco No 138-0037617 a nombre del señor J. C. E. M. por la cantidad de $ 978 dólares, por lo que le indique a los señores del Banco que en ningún momento había hecho transferencia alguna denunciando el hecho en el Banco, cuando ya en la tarde del 01 de febrero del 2019 a las 11h30 recibí una llamada por parte del gerente del Banco de Machala indicándome que la policía había detenido a la persona que había hecho la transferencia, posterior me llamó un miembro de la policía y me dijo del por menor, luego me trasladé hasta la Unidad Judicial Albán Borja, donde me indicaron lo sucedido y presenté la respectiva denuncia contra los señores J. C. E. M. y C. O. C. Y…". La denuncia presentada por el ciudadano R. O. W. H. en la que señaló: "…el día de viernes 01 de febrero del 2019 a eso de las 16h00, me acerqué a retirar de la matriz del Banco de Machala ubicado en las calles 9 de mayo y Rocafuerte, a fin de retirar la cantidad de US $ 865.00 de mi cuenta corriente No. 1010522958; pero me encontré con la novedad de que no había fondos, revisé mi otra cuenta de ahorros No. 130283039, pero tampoco había fondos, preocupado por la situación me acerqué a hablar con la Gerente del Banco y me comentó que yo supuestamente he realizado una transferencia de mi cuenta corriente No. 1010522958 a mi cuenta de ahorros No. 130283039 y de esa cuenta a la cuenta No. 1380037617 del mismo Banco a nombre del señor E. M. J. C. por la cantidad de US $865.00; por lo que les indiqué que en ningún momento había hecho ninguna transferencia y alarmé al Banco a fin de que investigue; a eso de las 18h00 recibo una llamada de un capitán de la policía indicándome que habían cogido a dos señores que responden a los nombres de E. M. J. C. y C. O. C. J. Según tengo entendido ellos habían cogido mi número celular y mi correo electrónico creando cuentas digitales de forma fraudulenta y sin mi autorización. Cabe indicar que yo jamás había conocido a estas personas, es así que presento esta denuncia contra los señores E. M. J. C. y C. O.C, J…"; En la foja 92 a 94 de los autos consta por escrito la sentencia condenatoria emitida por este juzgador con fecha 24 de marzo del 2019 a las 09h09, dictada en contra de C. O. C. J., mismo que se acogió a un "procedimiento abreviado". En la parte resolutiva de dicha sentencia se indica lo que sigue: "…Por estas consideraciones ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, se dicta SENTENCIA CONDENATORIA en contra de C. J. C. O, al haberse establecido que es AUTOR responsable de la comisión del delito previsto y sancionado en el Art. 190 inciso primero del Código

Orgánico Integral Penal y en cuanto a la pena previamente acordada entre las partes, considerando que se trata de su primera detención, su confesión espontánea y la reparación a la víctima, se le impone (08) OCHO MESES de privación de libertad, que deberá cumplir en el Centro de Privación de Personas Adultas en Conflicto con la Ley, Guayaquil No. 1, sección varones, debiendo descontarse todo el tiempo que el sentenciado haya estado detenido por esta causa. Al amparo del Art. 69 numeral 1 literal b) del Código Orgánico Integral Penal, se le impone la multa proporcional de (01) Un Salario Básico Unificado del Trabajador en General".

En la audiencia de Procedimiento Directo llevada a cabo el 20 de marzo de 2019 a las 15h30, para juzgar la conducta de J. E. M, el Dr. L. P. M, Fiscal, en cumplimiento de lo dispuesto por el Art. 454 No. 1, y Art. 640 No. 3 del COIP, solicitó como prueba de cargo se recepte el testimonio de varios testigos, de conformidad a las reglas establecidas en los artículos 609 y siguientes del citado cuerpo de ley, es así que: Comparece a rendir su testimonio CBOP. M. A. M. J, Perito reconocedor de objetos y evidencias, quien realizó el Informe de reconocimiento de Objetos N° DCGIT1900657; el testimonio del Testigo V. M. C. M., (víctima); el testimonio del Capitán P. C. L. R, (APREHENSOR); el testimonio del Sargento A. A. L, L, agente investigador, quien realizó el Informe Investigativo N° 112-2019-SCF-DF-PJ-Z-8; el testimonio el CBOP. D. F. C S, perito reconocedor del lugar de los hechos, quien realizó el Informe de reconocimiento del lugar de los hechos N° 240-2019-PJ-DMG-Z8; el testimonio de la ciudadana M. B. T. E, Jefe de Agencia del Banco de Machala.

En el turno de la DEFENSA DEL ENCARTADO, se le concede la palabra al Ab. W. I, en calidad de defensor privado, quien procede a realizar su anuncio de prueba y llama a rendir testimonio al procesado J. C. E. M.

3. Resolución:

Por lo precedentemente expuesto, ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, dicto SENTENCIA CONDENATORIA en contra de J. C. E. M, por considerarlo AUTOR responsable del delito de APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS, previsto y sancionado en el Art. 190 inciso primero del Código Orgánico Integral Penal, conforme el Art. 42 del citado cuerpo de ley, imponiéndose la pena de (01) UN AÑO de Privación de Libertad. Que cumplirá en el Centro de privación de personas adultas en conflictos con la Ley No. 1, sección Varones, de Guayaquil. De conformidad a lo dispuesto en el Art. 70 en concordancia con el Art. 69 numeral 1 literal b) del

Código Orgánico Integral Penal, se le impone la multa de (01) un salario básico unificado del trabajador en general, el cual será cancelado en cuotas durante el tiempo que cumpla la sentencia, cantidad que será depositada en la Cuenta Corriente No. 750006-8 del Banco del Pacífico, Sublínea 170499 a nombre de la Dirección Provincial del Consejo de la Judicatura Guayas. Así mismo se le impone como reparación integral (01) un salario básico unificado del trabajador en general, debiendo cancelar la suma impuesta en el plazo de 30 días, una vez ejecutoriado el presente fallo.

El 29 de marzo de 2019, a las 16h30, se llevó a cabo la Audiencia, en la que el suscrito Juez le concedió la palabra al Ab. V. I. I, en calidad de defensor privado del procesado, quien indicó lo siguiente: Se ha presentado solicitud de suspensión de la pena, a favor de mi defendido E. M. J. C, por lo que se cumplen requisitos de los 4 numerales del Art. 630 COIP, es una persona honesta, trabajadora no tiene otra causa pendiente, presentó la documentación necesaria, certificado del sistema SATJE, certificado de entorno familiar, declaración juramentada de su nexo domiciliario. En audiencia estipulo el pago de reparación integral a la víctima, lo que se va hacer en esta audiencia. Solicito se conceda la suspensión condicional de la pena, se impongan las condiciones del Art. 631 del COIP. La fiscalía considera que se han presentado los requisitos del Art. 630 COIP, pudiéndose conceder la suspensión condicional de la pena, imponiéndole las condiciones del Art. 631.

Escuchadas las partes se considera, que esta causa se inició por el delito tipificado en el Art. 190, Inc. 1 del COIP, en audiencia de juzgamiento efectuada el 20 de marzo del 2019 la fiscalía pudo determinar que efectivamente había los componentes del quebrantamiento de una norma, se verificó que E. M. J.C. era autor del delito que tipifica el Art. 190, Inc. 1, del COIP, se le impuso la sentencia de 12 meses de pena privativa de libertad, y el pago de la reparación integral a la víctima de 01 salario. Este juzgador considera que la documentación presentada cumple parámetros legales por lo tanto concede la suspensión condicional de la pena, a favor de E. M. J. C, quien se encuentra en goce de su libertad con medida alternativa. Se le impone las condiciones del Art. 631 COIP, numerales 1 y 2 abstenerse de concurrir a cualquier agencia del banco de Machala, 3, 5, 7, la reparación integral a la víctima ya ha sido cancelada, 8, debiendo presentarse ante el fiscal de la causa, todos los días 01 y 15 de cada mes, en día y horas laborables durante el plazo de 12 meses; 9) no ser reincidente; y, 10) no tener otra causa por nuevo delito.- El control de estas condiciones la cumplirá el juez de garantías penitenciarias que avoque conocimiento mediante sorteo.

4. Comentario de la Autora:

En este último caso, se sentenciaron a dos personas, por el delito de apropiación fraudulenta por medios electrónicos, según el Art 190 inc.1, que se refiere a la persona que utiliza fraudulentamente un sistema informático, 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.

En este caso podemos observar que el objeto material de la infracción es la transferencia o transacción de dinero, de manera fraudulenta por vía electrónica, sin el consentimiento del titular de la cuenta de ahorros, el mismo que fue depositado en otra cuenta que se encontraba a nombre de las personas procesadas. El daño causado es la pérdida del activo patrimonial (dinero), que se encontraba en la cuenta de ahorros del Banco de Machala, perjudicando notablemente a la víctima con este acto ilícito.

La apropiación fraudulenta por medios electrónicos, es uno de los delitos informáticos más utilizados para obtener información confidencial de forma ilícita de contraseñas, información detallada sobre tarjetas de crédito y otra información bancaria de la víctima.

Hoy en día es muy común que recibamos correos donde muchas veces, solicitan ingresar información o sus propios códigos de seguridad, es aquí cuando los delincuentes se aprovechan para realizar grandes transacciones, que conllevan al perjuicio patrimonial del usuario.

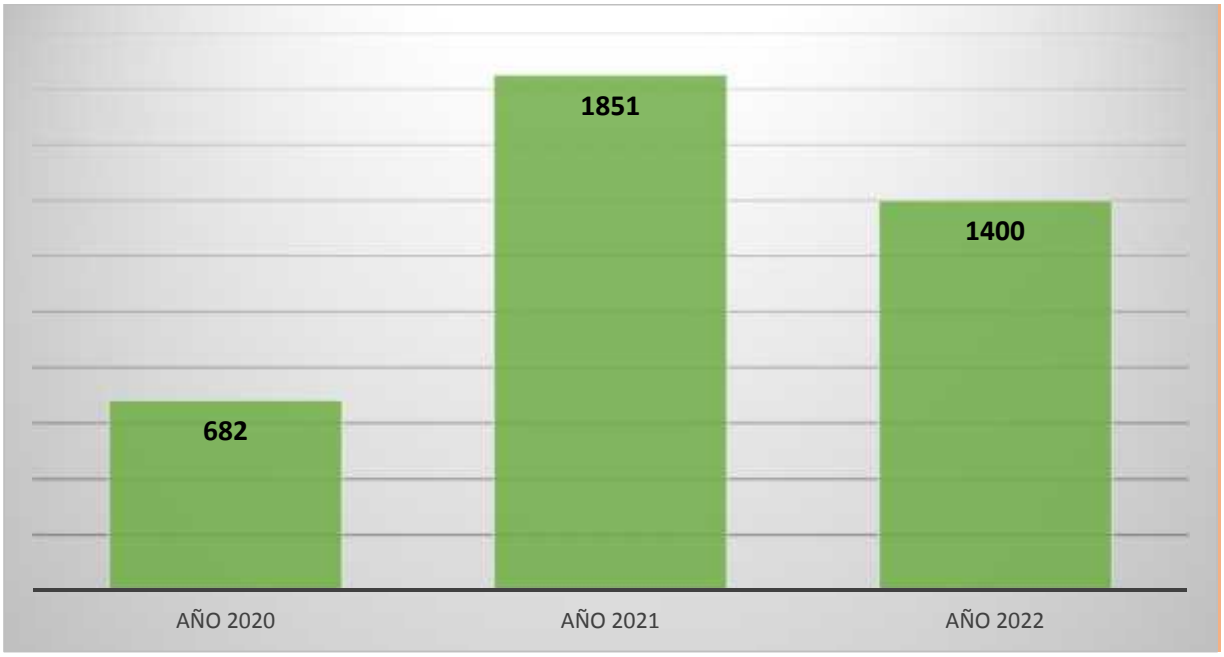
Es importante revisar continuamente el correo electrónico; cuando lleguen correos de instituciones bancarias en donde se tiene una cuenta de ahorros, debemos acercarnos a la sede para verificar la información, no se puede entregar datos personales, contraseñas de la banca virtual, los dígitos o códigos de seguridad de la tarjeta de débito o crédito. Por lo tanto, todo trámite se debe realizar con prudencia y precaución para no ser víctimas de la delincuencia.

6.4. Análisis de Datos Estadísticos.

Para desarrollar este subtema del presente Trabajo de Integración Curricular, se realizó la recopilación de la información más propicia y datos estadísticos de la situación real que enfrenta el Ecuador sobre los delitos informáticos y los ciberataques, luego se procederá a elaborar el respectivo análisis e interpretación de cada uno de los datos encontrados.

6.4.1. Denuncias por Ciberdelitos en el Ecuador año 2020, 2021 y 2022.

Figura No. 6



Fuente: Unidad de Ciberdelitos de la Policía Nacional del Ecuador.
Autora: Lizbeth Sofía Palacios Orellana.

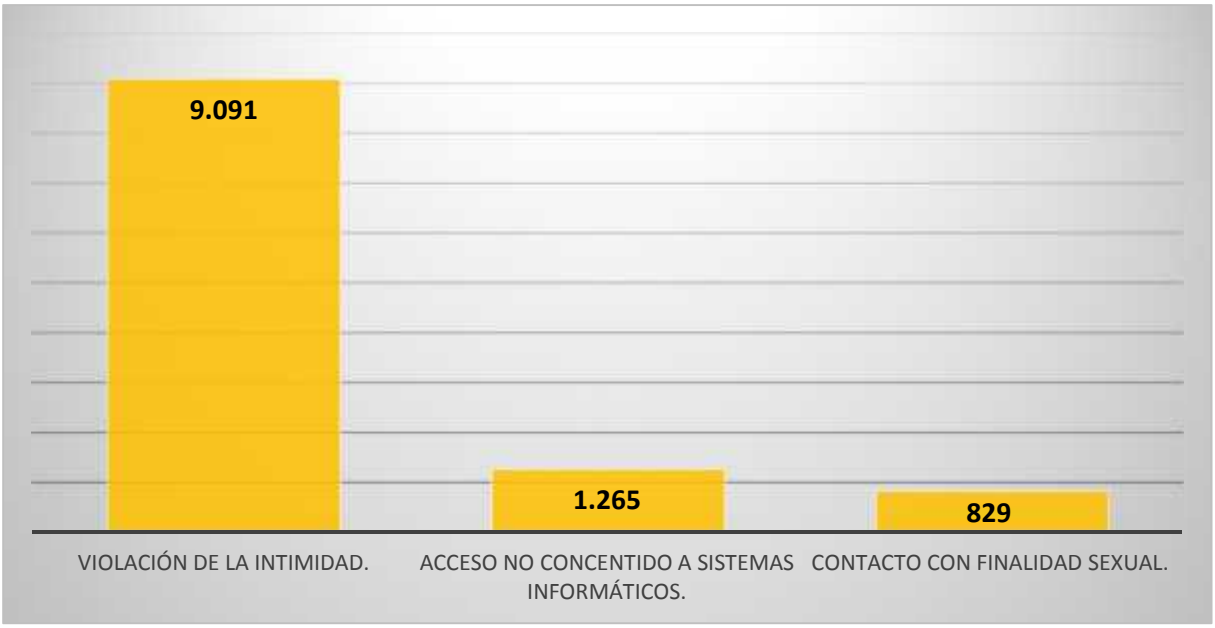
Interpretación y Análisis de la Autora:

De acuerdo a la información proporcionada por la Unidad de Ciberdelitos de la Policía Nacional del Ecuador, los ciberdelitos o delitos informáticos es el acto ilegal que es ejecutado por un ciberdelincuente en el espacio digital a través de las redes informáticas y diversos dispositivos electrónicos. Como podemos observar en la Figura No. 6, en el Ecuador existen múltiples denuncias por ciberdelitos, encontrándose 682 en el año 2020, 1851 en el año 2021 y 1400 en el año 2022. Por lo tanto, en el año 2021 se receptaron un mayor número de ciberdelitos, los mismos que atentan contra la integridad y confidencialidad de los datos y de los sistemas informáticos, violentando los derechos de las personas, empresas, instituciones públicas y privadas e incluso al Estado ecuatoriano, con el fin de dañar, deteriorar, borrar, hacer inaccesibles, suprimir o alterar datos informáticos sin la autorización del propietario.

La Policía Nacional del Ecuador, nos indica que estos datos estadísticos podrían aumentar si las víctimas de los delincuentes informáticos, hicieran sus denuncias ante las autoridades competentes como la Policía y Fiscalía, quienes nos pueden ayudar a encontrar a las personas responsables del cometimiento de estas conductas antijurídicas, contrarrestando de esta forma para que los delitos informáticos no queden en la impunidad.

6.4.2. Delitos Informáticos más cometidos en el Ecuador en el año 2022.

Figura No. 7



Fuente: Unidad de Investigación de Delitos Tecnológicos (UIDT-DNPJ).
Autora: Lizbeth Sofía Palacios Orellana.

Interpretación y Análisis de la Autora:

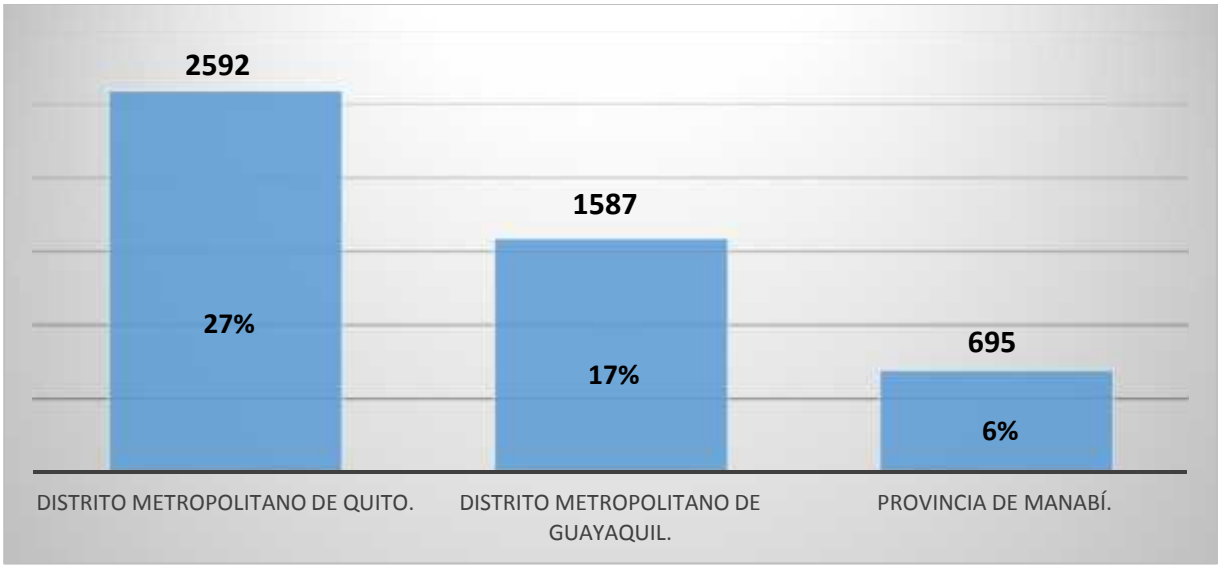
Según la Unidad de Investigación de Delitos Tecnológicos (UIDT-DNPJ), los delitos informáticos más frecuentes en el Ecuador en el año 2022 son: la violación de la intimidad, el mismo que alcanza los 9. 091 casos, este delito implica acceder, grabar, reproducir, difundir o publicar sin el consentimiento de la otra persona datos personales, audios, videos o información contenida en soportes informáticos por cualquier medio digital. Así mismo, tenemos el delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones en el que se ha podido visualizar 1. 265 casos, entendiéndose que este delito ocurre cuando una persona sin autorización de su titular, accede a un sistema informático o se mantiene dentro del mismo en contra de su voluntad. Además, existe otro delito informático que es el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, donde se puede observar 829 casos, ese delito ocurre cuando una persona por medios electrónicos propone concertar un encuentro con una persona menor de dieciocho años, cuya propuesta se basa en el acercamiento con finalidad sexual o erótica.

En consecuencia, los delitos informáticos se encuentran tipificados y sancionados en el Código Orgánico Integral Penal en el Art. 178, 234 y 173. Para evitar el cometimiento de este tipo de delitos, el Estado ecuatoriano, debe concientizar a las personas sobre el correcto uso de las

tecnologías de la información y la comunicación, sobre la ciberseguridad como herramienta para combatir a la ciber delincuencia, logrando que exista la protección adecuada de los datos personales de los usuarios cibernéticos.

6.4.3. Provincias con mayor índice de ciberataques en el Ecuador en el año 2022.

Figura No. 8



Fuente: Policía Nacional del Ecuador.
Autora: Lizbeth Sofía Palacios Orellana.

Interpretación y Análisis de la Autora:

Estos datos estadísticos fueron recogidos por la Policía Nacional, nos demuestran que el 27% de los ciberataques, se concentran en la provincia del Distrito Metropolitano de Quito, con 2592 eventos. En segundo lugar, se puede constatar que el 17% de los ataques cibernéticos se encuentran en el Distrito Metropolitano de Guayaquil, con 1587 casos. En tercer lugar, se puede observar que el 6% de los ciberataques se encuentran en la Provincia de Manabí, donde se reportaron 695 eventos en el Ecuador.

Como podemos observar, los ciberataques son una forma por la que los ciber delincuentes atacan a los usuarios informáticos, comprometiendo los medios tecnológicos de sus víctimas, logrando adquirir los datos personales, con la finalidad de apropiarse de la información confidencial consiguiendo grandes beneficios.

Por lo tanto, es indispensable que las personas, las entidades públicas y privadas, tomen las debidas precauciones, aplicando la Política y Estrategia de Ciberseguridad emitida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como método para combatir la delincuencia informática existente en el Ecuador.

7. Discusión.

7.1. Verificación de los Objetivos.

En el presente subtema, se analiza si se ha dado cumplimiento a cada uno de los objetivos planteados en el Proyecto de Integración Curricular, legalmente aprobado, donde se planteó un objetivo general y cuatro objetivos específicos, a continuación, se procederá a verificar cada uno de ellos:

7.1.1. Verificación del Objetivo General.

En el presente objetivo general que fue aprobado en el Proyecto de Integración Curricular, el mismo que consiste en: **"Realizar un estudio doctrinario, jurídico y comparado de las Estrategias y Políticas de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los delitos informáticos".**

El objetivo general del presente Trabajo de Integración Curricular se verificó de la siguiente manera: El estudio doctrinario se desarrolla en el marco teórico donde fueron analizados los siguientes subtemas: La Ciberseguridad sustentado por el autor Leiva y Barrantes. La Política Pública de acuerdo al jurista Vargas, así como Bañón y Castro. La Política Criminal según el doctrinario Moreno y Albán. Las Ciberamenazas en concordancia con el autor Ruiz, los Ciberataques de acuerdo al criterio de Cubeiro y los Delitos Informáticos de conformidad a la opinión de Téllez, Pérez y Sarzana.

El estudio jurídico con el análisis de la Constitución de la República del Ecuador en el artículo 85 referente a las políticas públicas, el artículo 66 numeral 19, 20, 21 y 26, que hacen mención a los delitos informáticos. En el Código Orgánico Integral Penal, en el artículo 173, 174, 178, 186, 190, 191, 192, 193, 194, 195, 212, 229, 230, 231, 232, 233, 234 y 234.1, en donde se establecen cada una de estas conductas delictivas con sus respectivas sanciones. Así como también, la Política y Estrategia Nacional de Ciberseguridad del Ecuador, propuestas para prevenir y proteger a los usuarios de las ciberamenazas y ciberataques existentes en el espacio digital.

Se verificó el derecho comparado con el análisis de las Políticas y Estrategias de Ciberseguridad de los países de República Dominicana, España, Chile, Costa Rica y Argentina, estableciendo que estos países tienen una mayor capacitación, educación, prevención y cultura de ciberseguridad, en donde el Estado de cada país pone mayor énfasis en proteger los sistemas informáticos, estableciendo un marco legal que garantice la seguridad humana y el bienestar de

los usuarios en el ciberespacio, además, estos países están adheridos al Convenio de Budapest y tienen un Equipo de Respuesta a Incidentes Cibernéticos, logrando con ello mejorar la respuesta a los ataques cibernéticos. En Ecuador existe una Política y Estrategia Nacional de Ciberseguridad, pero no se brinda el conocimiento, educación, aplicación ni ejecución respectiva de la misma, tampoco se encuentra adherido al Convenio de Budapest y no cuenta con un Equipo de Respuesta a Incidentes Cibernéticos.

Además, se constató con la pregunta cinco de la entrevista que dice: ¿Podría usted indicar, en qué consiste la Política y Estrategia Nacional de Ciberseguridad implementada en el Ecuador, para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos?, donde los entrevistados consideran que la Política y Estrategia Nacional de Ciberseguridad, fue realizada por el Estado para construir y fortalecer las capacidades nacionales garantizando el ejercicio de los derechos y libertades de la población.

7.1.2. Verificación de los Objetivos Específicos.

A continuación, analizaremos los objetivos específicos planteados, entre ellos tenemos:

El primer objetivo específico es:

“Establecer las políticas criminales implementadas por el Estado para promover en los usuarios informáticos la capacidad de prevención ante los riesgos existentes con las ciberamenazas y ciberataques”.

El presente objetivo específico se logra verificar al momento de analizar la Política Nacional de Ciberseguridad dictada en el año 2021, mediante Acuerdo Ministerial 006- 2021 y la Estrategia Nacional de Ciberseguridad dictada en el año 2022, por el Ministerio de Telecomunicaciones y de la Sociedad de la Información. Así mismo, se analizó el derecho comparado de las Políticas y Estrategias Nacionales de Ciberseguridad de República Dominicana, España, Chile, Costa Rica y Argentina, para promover en los usuarios informáticos la capacidad de prevención ante los riesgos existentes.

La verificación de este objetivo se podrá constatar con la nueva reforma a la Ley de Seguridad Pública y del Estado del 29 de marzo de 2023, que plantea un capítulo innumerado denominado Consejo Nacional de Política Criminal, que es el encargado de aprobar la política criminal que es el conjunto de respuestas que el Estado adopta, de manera integral e intersectorial, para prevenir y enfrentar la delincuencia y criminalidad.

Por otro lado, se puede verificar con la pregunta número uno de la encuesta, con la siguiente pregunta: De las siguientes líneas de acción, dígnese seleccionar una: ¿Cuál cree usted, que es un aporte a las políticas criminales implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos de ciberamenazas y ciberataques?, donde doce encuestados que representan el 40% seleccionaron la opción crear Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional calificado en el campo de la Informática y el Derecho.

Así mismo, en la entrevista se pudo constatar con la pregunta número uno: Podría indicar usted, ¿Cuáles son las Políticas de Ciberseguridad implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos existentes con las ciberamenazas y ciberataques?, los diez entrevistados indicaron que la Política y la Estrategia Nacional de Ciberseguridad, tiene como objetivo proteger la información de las personas, empresas, entidades públicas y privadas e incluso del Estado, velando por el adecuado ejercicio de los derechos fundamentales de la sociedad.

El segundo objetivo específico es:

“Detectar las formas en las que operan los antisociales al cometer Delitos Informáticos, logrando de esta manera disminuir el índice de personas perjudicadas”.

Se puede verificar con el estudio de los delitos informáticos, tipificados en el Código Orgánico Integral Penal, en el cual se sancionan las conductas ilícitas realizadas por los delincuentes informáticos, a través de las ciberamenazas y ciberataques que se producen en los sistemas tecnológicos.

Además, se puede verificar con la pregunta número dos de la encuesta, cuando se preguntó: Seleccione una opción: ¿Cuál es la forma más común en la que operan los antisociales al cometer los Delitos Informáticos?, donde quince personas que representan el 50% seleccionaron la opción de la creación de perfiles falsos sobre la base de la información consignada en redes sociales.

También, en la entrevista se pudo constatar con la pregunta número dos: ¿Podría usted señalar, cuáles son las formas en las que operan los antisociales para cometer los Delitos Informáticos?, de acuerdo con las respuestas proporcionadas por los entrevistados, nos manifestaron que las formas en las que operan son por medio de la ingeniería social y los delitos informáticos donde

este tipo de delincuentes vulneran la información de otras personas sin su autorización por medio de los dispositivos electrónicos.

Así mismo, la verificación a este objetivo se realiza con los datos estadísticos de los delitos informáticos más cometidos en el Ecuador en el año 2022, donde se observa que el delito de violación a la intimidad alcanza los 9.091 casos, el delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones con 1. 265 casos y el delito de contacto con finalidad sexual con menores de dieciocho años por medios informáticos con 829 casos.

El tercer objetivo específico es:

“Propiciar un mayor conocimiento sobre la Ciberseguridad para proteger y garantizar la correcta utilización de las Tecnologías de Información y Comunicaciones”.

La verificación de este objetivo, se lo realiza con la pregunta número tres de la encuesta, en la que se consultó a los profesionales: Señalar la opción pertinente: ¿En qué nivel de educación estima usted, que sería favorable impartir conocimientos sobre Ciberseguridad, para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?, donde dieciocho personas que equivalen al 60% escogen la opción segundo nivel de educación general básica y bachillerato.

También, en la entrevista se pudo comprobar con la pregunta número tres: ¿En qué nivel de educación, cree usted, que es recomendable propiciar el conocimiento sobre la Ciberseguridad para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?, los entrevistados explican que es pertinente que se imparta una educación sobre ciberseguridad en todos los niveles educativos, empezando desde los primeros años de vida, porque los niños y niñas son nativos informáticos, es decir, que nacieron con la tecnología en sus manos.

El cuarto objetivo específico es:

“Demostrar los adecuados medios informáticos y la protección que el Estado nos brinda a través de la estrategia y política de ciberseguridad.

Este objetivo se verificó con la ayuda de la Política y Estrategia Nacional de Ciberseguridad del Ecuador, emitidas por el Estado, con la finalidad de proteger la información de los usuarios

en el ciberespacio. Actualmente, los delitos informáticos han evolucionado de forma acelerada, ocasionando perjuicios a múltiples personas en sus datos personales, los mismos que son utilizados por los delincuentes informáticos para obtener beneficios, especialmente de carácter económico.

Además, este objetivo tiene relación con la pregunta número cuatro de la encuesta, donde se consultó a los investigados: Escoja la opción pertinente: ¿Según su criterio, qué medio tecnológico es el más adecuado para evitar los perjuicios ocasionados por los Delitos Informáticos?, quince encuestados que representan el 50% seleccionan la opción teléfono celular, como el medio más adecuado que se debe utilizar para realizar las múltiples actividades diarias dentro del ciberespacio.

Con la pregunta número cuatro de la entrevista, se pudo corroborar el presente objetivo específico, se preguntó a los profesionales del Derecho: ¿Podría usted indicar, cuáles son los medios tecnológicos más adecuados y la protección que el Estado brinda a través de la Política y Estrategia de Ciberseguridad?, ellos señalaron que ninguno de los medios tecnológicos son seguros, pueden ser confiables si se coloca en ellos un antivirus efectivo, contraseñas robustas y aplicando la ciberseguridad en los dispositivos electrónicos.

7.2. Contrastación de Hipótesis.

La hipótesis planteada se enfocó en:

“La actualización del conocimiento y correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador”.

La presente hipótesis se relaciona con el tema de las Políticas Públicas, las mismas que son planteadas por el Estado y se encuentran establecidas en la Constitución de la República del Ecuador, en el Art. 86, donde se determinan los mecanismos más adecuados que permiten encontrar soluciones a la proliferación de los delitos informáticos en nuestro país.

Se la puede constar con la pregunta número cinco de la encuesta, donde se preguntó: ¿Cree usted, que la actualización de conocimiento y correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos, servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador?, los encuestados nos indican que es importante que exista una actualización de conocimientos, para ampliar la cultura de ciberseguridad en el manejo de los medios digitales,

permitiendo que cada usuario tenga cuidado en la utilización de la información y las aplicaciones.

Además, se puede verificar la hipótesis con los datos estadísticos obtenidos de las denuncias por Ciberdelitos en el Ecuador, donde se puede evidenciar que en el año 2020 existieron 682, en el año 2021 se receptaron 1851 y en el año 2022 se presentaron 1400. Siendo el año con mayor índice de delitos informáticos el 2021.

7.3. Fundamentación de los Lineamientos Propositivos.

La ciberseguridad es un mecanismo de protección para evitar que los dispositivos, redes y datos de las personas o entidades, sean alterados por las ciberamenazas y ciberataques digitales, que tratan de apropiarse de la información confidencial de los usuarios cibernéticos.

Estas medidas de seguridad digital fueron implementadas por la gran cantidad de delitos informáticos, ocasionados por la dependencia de la sociedad ecuatoriana en el uso de los medios tecnológicos, donde los delincuentes informáticos desarrollaron mecanismos más sofisticados que van evolucionando a la par de la tecnología.

El Estado es el encargado de informar a los ciudadanos sobre el cuidado que deben tener en el uso de la tecnología, de igual forma, el compromiso de las personas en proteger sus datos confidenciales, es decir, debe haber una responsabilidad compartida, por lo tanto, es indispensable que exista una cultura de ciberseguridad.

La Declaración Universal de los Derechos Humanos, nos menciona que todo individuo tiene derecho a la vida, a la libertad y a la seguridad. La Constitución de la República, nos menciona en su Art. 1, que el Ecuador es un Estado constitucional de derechos. En el Art. 10 nos indica que las personas, comunidades, pueblos, nacionalidades y colectivos son titulares y gozarán de los derechos garantizados en la Constitución y en los instrumentos internacionales. Además, el Art. 11 nos hace mención a los principios por los que se rige el ejercicio de los Derechos Humanos. Así mismo, el Art. 417 establece que los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en su Constitución.

Este tema de investigación está vinculado con el derecho a la seguridad humana, en el Art. 393 nos dice que 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, prevenir las formas de violencia, discriminación, la comisión de infracciones y delitos.

Actualmente el aumento de los delitos informáticos en el Ecuador, se encuentran tipificados y reconocidos en el Código Orgánico Integral Penal, que se producen por la poca aplicación, ejecución y conocimiento de la Política y Estrategia Nacional de Ciberseguridad, la misma que es un mecanismo de defensa ante las ciberamenazas y ciberataques.

Es de suma importancia dentro de la presente investigación conocer sobre las Políticas y Estrategias Nacionales de Ciberseguridad de varios países, entre ellos están República Dominicana, España, Chile, Costa Rica y Argentina, con la finalidad de analizar los mecanismos que han sido planteados por los mismos y comparar con las existentes en el Ecuador, logrando con ello establecer las debidas soluciones para mitigar a los delitos informáticos en el ciberespacio.

En el trabajo de campo realizado a través de las encuestas y entrevistas a los profesionales, se pudo observar que el desconocimiento sobre la Política y Estrategia Nacional de Ciberseguridad es muy restringido, por ello, es necesario que el Estado cree Direcciones o Unidades de Prevención contra los Delitos Cibernéticos; así mismo, es indispensable incrementar conocimientos de ciberseguridad en todos los niveles educativos para que los niños, niñas, adolescentes y personas en general puedan identificar y prevenir estas conductas ilícitas, mermando de esta forma el alto índice de delitos informáticos en el Ecuador.

En el estudio de casos y de datos estadísticos, hemos podido evidenciar que los delitos informáticos en Ecuador, están dirigidos a obtener datos confidenciales de las personas sin su consentimiento, transformándose en las víctimas de los delincuentes informáticos.

De toda la información obtenida, se pudo evidenciar que el aumento de los delitos informáticos es ocasionado por la gran dependencia digital de la sociedad, la creciente evolución de la tecnología y su uso generalizado, donde los delincuentes informáticos a través de ciberamenazas y ciberataques cometen el acto delictivo, vulnerando los derechos de las personas involucradas.

El crecimiento exponencial de los delitos informáticos, es ocasionado por la poca información, la falta de concientización y prevención en el uso de los medios electrónicos por parte del Estado, también se presenta por la no aplicación y ejecución de la Política y Estrategia de Ciberseguridad; por tal razón es necesario y urgente que exista una mayor educación y difusión por parte de las autoridades competentes, para propiciar una cultura de ciberseguridad en toda la población ecuatoriana, garantizando la seguridad humana y la confianza digital en el uso de las tecnologías de la información y la comunicación.

8. Conclusiones.

Luego de elaborar el marco teórico, analizar los resultados de campo, el estudio de casos y sintetizar la discusión de los resultados del presente Trabajo de Integración Curricular, se ha llegado a las siguientes conclusiones:

Primera: Los delitos informáticos en el Ecuador, se han presentado a causa de la creciente utilización de los medios tecnológicos por parte de los usuarios cibernéticos, por lo que es necesario que exista mayor prevención por parte del Estado frente a estos actos delictivos.

Segunda: La falta de información respecto a la Política y Estrategia Nacional de Ciberseguridad por parte del Estado y las autoridades competentes sobre la función que deben cumplir las mismas en relación a la prevención de los delitos informáticos.

Tercera: Ecuador no cuenta actualmente con un Plan Nacional coordinado dentro de la educación y la sensibilización en materia de ciberseguridad, así como los planes de estudios escolares y universitarios no proporcionan el apoyo suficiente para contribuir a la creación de una sociedad digital más competente y consciente, hay que tomar en cuenta que los delincuentes informáticos, eligen sus víctimas sin mirar la edad, sexo, raza, estatus, etcétera, por tal razón es necesario incrementar conocimientos de ciberseguridad, a través de una educación que empiece desde los más pequeños, en el hogar, escuela, colegio, universidad y edad adulta, de esta manera poder controlar el aumento de este tipo de delitos.

Cuarta: De acuerdo con la información obtenida del Índice Global de Ciberseguridad, emitido por la Unión Internacional de Telecomunicaciones, nos indica que Ecuador se encuentra en el puesto número 119 de 182, con relación a las amenazas cibernéticas a nivel mundial, por tal razón debemos enfrentar este tipo de amenazas que conllevan al cometimiento de los delitos informáticos, con la aplicación de una cultura de ciberseguridad, que nos permita disminuir la creciente ola de delincuencia producida por los antisociales, que lo único que desean es apropiarse de la información de las personas causando graves daños.

Quinta: De acuerdo al derecho comparado realizado en la investigación con los países de República Dominicana, España, Chile, Costa Rica y Argentina, sobre las Políticas y Estrategias Nacionales de Ciberseguridad, se determinó que es indispensable que Ecuador se adhiera al Convenio de Budapest, para contrarrestar la delincuencia informática, ayudándose de forma compartida con los estados miembros del mismo, a través de la armonización de leyes entre

naciones, ampliando las técnicas de investigación, la cooperación internacional para mitigar y apalear esta clase de delitos.

Sexta: De los resultados obtenidos en la investigación de campo, dentro de las encuestas y entrevistas realizadas, los profesionales indican que la Política y Estrategia Nacional de Ciberseguridad del Ecuador deben ser difundidas a través de los medios digitales existentes en el ciberespacio; así mismo, consideran que es necesario que la ciberseguridad se implemente en la malla curricular de todos los niveles de educación y su aplicación sea en el sector público, privado y en la sociedad en general, propiciando con ello una cultura de ciberseguridad para poder identificar, prevenir y resguardar la información confidencial de los usuarios.

9. Recomendaciones.

Las recomendaciones que se consideran pertinentes presentar son las siguientes:

Primera: El Estado debe crear Direcciones o Unidades de Prevención de Delitos Cibernéticos con personal especializado en el campo de la Informática y el Derecho; con procedimientos preventivos estándar y mecanismos de denuncia eficientes, en cada una de las provincias del Ecuador, con el fin de que la población sea asesorada correctamente en la forma de actuar frente a las ciberamenazas y ciberataques provocados por los delincuentes informáticos, reduciendo así la inseguridad existente en el ciberespacio.

Segunda: El Ministerio de Telecomunicaciones y de la Sociedad de la Información, con la ayuda de la Policía Nacional del Ecuador, deben brindar constantes capacitaciones a la ciudadanía en general sobre ciberseguridad para proteger la confidencialidad de la información, contrarrestando los posibles ataques a los sistemas electrónicos.

Tercera: El Estado a través del Ministerio de Educación, debe incorporar una asignatura de ciberseguridad dentro del plan de estudio y la malla curricular en la Educación General Básica y Bachillerato, de igual forma en la Educación Superior y de Posgrado, logrando desarrollar un conocimiento amplio para identificar y prevenir los delitos informáticos.

Cuarta: El Estado con la ayuda de la Policía Nacional, como institución especializada en el tratamiento de los delitos informáticos, debe propiciar una cultura de ciberseguridad en la población ecuatoriana, para concientizar el uso adecuado de las tecnologías de la información y la comunicación, así como también, los riesgos existentes en el espacio digital.

Quinta: Se debe exigir a la Asamblea Nacional y el Poder Ejecutivo que el Ecuador inicie de forma inmediata la adhesión al Convenio de Budapest sobre la ciberdelincuencia, que constituye el nexo de cooperación internacional más importante entre los países firmantes, para contrarrestar las actividades criminales cometidas a través de los medios informáticos en el ciberespacio.

Sexta: Es necesario que el Estado ecuatoriano establezca una Unidad Especializada de la Fiscalía en la investigación de los Delitos Informáticos en cada provincia de nuestro país, para que exista una correcta indagación de estos actos delincuenciales y una adecuada administración de justicia, contribuyendo a la protección de los derechos humanos de la población en general.

9.1. Lineamientos Propositivos.

El Estado a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información, en vista de la creciente ola de criminalidad informática, ha elaborado la Política y Estrategia Nacional de Ciberseguridad del Ecuador, que son herramientas capaces de brindar seguridad a nivel nacional en el ciberespacio, manteniéndonos en alerta frente a los riesgos informáticos, por lo que es necesario, que las mismas sean difundidas por los distintos medios de comunicación, permitiendo a la ciudadanía poder identificar, detectar, responder o recuperarse de los incidentes cibernéticos que existen en el espacio digital.

El Estado ecuatoriano frente al aumento considerable de la delincuencia informática, tiene la responsabilidad de implementar Direcciones o Unidades de Prevención de Delitos Cibernéticos con profesionales especializados en la rama de la Informática, así como en el Derecho y con ello disminuir las ciberamenazas y ciberataques existentes en nuestro país.

El Estado debe crear una Unidad Especializada en Delitos Informáticos dentro de la Fiscalía de cada provincia del Ecuador, con profesionales especializados para la investigación de estas conductas delictivas, garantizando los derechos de las personas intervinientes en el proceso penal y de esta forma contribuir a la correcta administración de justicia, evitando que los ciberdelitos queden en la impunidad.

Incrementar una asignatura de ciberseguridad en el plan de estudio y la malla curricular de la Educación General Básica, Bachillerato General Unificado, Institutos Técnicos-Tecnológicos, Carreras Universitarias y Posgrado, para que niños, niñas, adolescentes, jóvenes y profesionales, tengan un conocimiento adecuado sobre la ciberseguridad que les permita prevenir y no ser víctimas de los delitos informáticos.

La Policía Nacional especializada debe capacitar permanentemente a la ciudadanía sobre el modus operandi de los antisociales cibernéticos, los delitos informáticos existentes en el Código Orgánicos Integral Penal y sus respectivas sanciones, las ciberamenazas y ciberataques más recurrentes, las recomendaciones que se debemos seguir para cuidar la información personal contenida en los dispositivos electrónicos, con la finalidad de concientizar sobre los riesgos que se producen por el mal uso de los medios tecnológicos.

Para proteger a las entidades financieras de las ciberamenazas y ciberataques que conllevan al cometimiento de los delitos informáticos, es necesario que se utilicen mecanismos de

ciberseguridad para predecir futuros ataques en los sistemas. Aplicar un sistema de seguridad avanzado como es el Managed Detection and Response (MDR), que es capaz de buscar, supervisar, analizar y actuar ante una amenaza cibernética. Implementar un Plan de Seguridad Informática que permita detectar vulnerabilidades y establecer medidas de prevención. Además, elaborar medidas de Seguridad Financiera y guías preventivas para el usuario y los trabajadores de estas entidades, donde se describan las amenazas más comunes, la forma de combatirlos y las recomendaciones para contrarrestar estos actos ilícitos.

El Ecuador debe analizar su Política y Estrategia Nacional de Ciberseguridad y compararla con las existentes en otros países, con el fin de determinar las mejores alternativas que ayuden a minimizar los delitos informáticos, protegiendo la información personal y confidencial de los usuarios cibernéticos.

Es propicio que Ecuador se adhiera al Convenio sobre la ciberdelincuencia, conocido como Convenio de Budapest, procurando el mejoramiento de la cooperación internacional y ayuda jurídica mutua de los países suscriptores en el convenio, aplicando una ley común de carácter supranacional que permita a los gobiernos intercambiar información y pruebas sobre los delitos informáticos cometidos, a fin de unificar los tipos penales y lograr la correlación entre las naciones firmantes.

Implementar en el Ecuador un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT). Un CSIRT que brinde servicios de ciberseguridad para prevenir, detectar, mitigar y responder a incidentes cibernéticos en una comunidad definida. Un CSIRT es una estructura organizativa con procesos establecidos y un catálogo de herramientas tecnológicas que cuentan con un presupuesto, mandatos, servicios, personal especializado, red de contactos, plan de comunicaciones, un marco legal habilitante que le permite actuar, conformando de esta manera la base para la gestión de incidentes cibernéticos en una determinada población.

10. Bibliografía.

(2012). Gob.ec. https://www.ministeriodegobierno.gob.ec/wp-content/uploads/downloads/2012/12/Manual-de-Derechos-Humanos.pdf

¿Qué son los Derechos Humanos? (2014, octubre 13). Defensoría del Pueblo. https://www.dpe.gob.ec/derechos-humanos-y-de-la-naturaleza/

SÁNCHEZ ROMERO, M., (2006). "Derechos Humanos". Constitución Códigos Leyes Reglamentos Convenios Venezolana. Editorial Buchivacoa. Caracas – Venezuela. p. 19

Faúndez, Héctor. 1996, El Sistema Interamericano de Protección de los Derechos Humanos. Aspectos Institucionales y Procesales. Instituto Interamericano de derechos Humanos, pág.28.

Nikken, P. (s. f.). *EL CONCEPTO DE DERECHOS HUMANOS*. Civilisac.org. Recuperado 16 de julio de 2023, de https://www.civilisac.org/civilis/wp-content/uploads/El-concepto-de-derechos-humanos-Pedro-Nikken.pdf

Autoformativo, M. (s. f.). *Acceso a la justicia y derechos humanos en Ecuador*. Cejamericas.org. Recuperado 17 de julio de 2023, de https://cejamericas.org/wp-content/uploads/2020/09/114AccesoalajusticiaeindigenasECUADOR.pdf?fbclid=IwAR0kP6dBgHiNvUKags7ifDadxBXCQkRREF7CL8k6yOhsI91Tv1GZlnez1Z8

Carrera, D. E., Tumipamba, L., & Alejandra, M. (s. f.). *UNIVERSIDAD CENTRAL DEL ECUADOR*. Edu.ec. Recuperado 17 de julio de 2023, de http://www.dspace.uce.edu.ec/bitstream/25000/3048/3/T-UCE-0013-Ab-23.pdf?fbclid=IwAR1shfxOGHveetc5oBVMD-xih591xhQarU9UKANR_OjORx0dfPQbNuemzK0

Derechos humanos de cuarta generación. (s. f.). Wikis.cc. Recuperado 17 de julio de 2023, de https://dhpedia.wikis.cc/wiki/Derechos_humanos_de_cuarta_generaci%C3%B3n

Registro Oficial, 2008-10-20. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. Recuperado de https://zone.lexis.com.ec

United Nations. (2003). *Human Security Now*. Global Equity Initiative.

ALKIRE, Sabina (2003), "A Conceptual Framework for Human Security", Oxford, Centre for Research on Inequality, Human Security and Ethnicity (CRISE), Queen Elizabeth House, University of Oxford.

Coordinador De Seguridad Interna, M. (s. f.). *Ecuador: hacia una seguridad con enfoque integral de buen vivir*. Edu.ec. Recuperado 18 de julio de 2023, de https://repositorio.uasb.edu.ec/bitstream/10644/4125/1/Ministerio%20Coordinador%20Seguridad-Ecuador.pdf

Guía metodológica para la aplicación del enfoque de Seguridad Humana. (s. f.). Instituto Interamericano de Derechos Humanos. Recuperado 18 de julio de 2023, de https://www.iidh.ed.cr/es/component/content/article/guia-metodologica-para-la-aplicacion-del-enfoque-de-seguridad-humana?catid=24&highlight=WyJzZWd1cmlkYWQiLCJzZWd1cmEiLCJzZWd1cm8iLCJodW1hbiIsImh1bWFuYSIsImh1bWFub3MiLCJodW1hbm8iXQ==&Itemid=101

Carpio D. (2013) El delito informático. Editorial Jurídica del Ecuador, Quito Ecuador.

TÈLLEZ, Josè. (2012). Delitos Informáticos y Protección Penal a la Intimidad.

Pérez Luño, A. (1996). Manual de Informática y derecho. Editorial Ariel.

Sarzana, Carlos. Criminalita e Tecnología en Computers Crime; Rassagna Penitenziaria e Criminología. Nos. 1-2 Año 1. Italia. Roma. p. 78

Delitos informáticos o ciberdelitos. (2015, septiembre 2). Gob.ec. https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/

(S. f.). Wordpress.com. Recuperado 18 de julio de 2023, de https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Téllez Valdés, Julio. Derecho Informático. Instituto de Investigaciones Jurídicas. Ed. Mc Graw Hill. Interamericana de México S.A. México. 1997.

Registro Oficial Suplemento, 2014-02-10. CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP. Recuperado de https://zone.lexis.com.ec

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, *3*(4), 161. https://doi.org/10.18294/relais.2015.161-176

The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. (s. f.). Meridianprocess.org. Recuperado 19 de julio de 2023, de https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

En Costa, C., María, A., Coto, B., Alvarado, A., Roberto, F., & Romero, C. (2010). *Ciberseguridad en Costa Rica*. Ucr.ac.cr. http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Ruiz Díaz, J. (2016). Ieee.es. https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Marco, D., Boletín, R., Visitar, E., Web, L., Cabello, E. C., Cubeiro, E., & Documento, C. (s. f.). *Unidades de ciberinteligencia y ciberguerra al servicio de Estados*. Ieee.es. Recuperado 19 de julio de 2023, de https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM10_2021_ENRCUB_Ciberinteligencia.pdf

Vásquez Santamaría, J. E., & Fundación Universitaria Autónoma de las Américas. (2017). Revisión teórica de las políticas públicas para determinar componentes iniciales de un modelo para la planeación de la contratación del departamento de Antioquia. *Estudios de derecho, 72*(162), 77-105. https://doi.org/10.17533/udea.esde.v73n162a04

Moisés Moreno Hernández / Tomo I.pag.64

Gómez, E. A. (s. f.). *MANUAL DE DERECHO PENAL ECUATORIANO*. Wordpress.com. Recuperado 23 de julio de 2023, de

https://estudiantesecuatorianosderecho.files.wordpress.com/2015/07/manual-de-derecho-penal-ecuatoriano-dr-ernesto-alban-gomez.pdf

Registro Oficial Suplemento, 2009-09-28. LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO. Recuperado de https://zone.lexis.com.ec

Registro Oficial Suplemento, 2021-06-23. POLÍTICA NACIONAL DE CIBERSEGURIDAD. Recuperado de https://zone.lexis.com.ec

Vera, S. (2022, agosto 29). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR - Gobierno Electrónico de Ecuador*. Gobierno Electrónico de Ecuador; Gobierno Electrónico - Ecuador. https://www.gobiernoelectronico.gob.ec/estrategia-nacional-de-ciberseguridad-del-ecuador/

Víctima. (2023). Diccionario panhispánico del español jurídico. https://dpej.rae.es/lema/v%C3%ADctima

Manzanera, L. R. (2002). *VICTIMOLOGIA ESTUDIO DE LA VÍCTIMA*. Derechopenalenlared.com. https://www.derechopenalenlared.com/libros/victimologia-estudio-de-la-victima-luis-rodriguez-manzanera.pdf

Cabanelas, G. (Edición 2006). *Diccionario Jurídico Elemental*. http://file:///C:/Users/Ana%20Orellana/Downloads/diccionario%20jur%C3%ADdico%20elemental-Cabanellas%20Guillermo%20(Recuperado).pdf

Registro Oficial Edición Especial, 2018-10-12. REGLAMENTO PARA EL SISTEMA DE PROTECCIÓN A VÍCTIMAS, TESTIGOS. Recuperado de https://zone.lexis.com.ec

De febrero de, 5. (s. f.). *12º Congreso de las*. Unodc.org. Recuperado 30 de julio de 2023, de https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_6/V1050759s.pdf

Rau, M., & Castillo, P. (2008). Prevención de la violencia y el delito mediante el diseño ambiental en Latinoamérica y El Caribe: *Vista de Prevención de la violencia y el delito mediante el diseño ambiental en Latinoamérica y El Caribe: Estrategias*

urbanas de cohesión social e integración ciudadana. https://revistainvi.uchile.cl/index.php/INVI/article/view/62293/66340

Salgado, B. (2019, abril 18). *Delitos informáticos se combaten con la prevención*. Gob.ec. https://www.policia.gob.ec/delitos-informaticos-se-combaten-con-la-prevencion/

Vera, S. (2021, octubre 11). *Recursos de ciberseguridad - Gobierno Electrónico de Ecuador*. Gobierno Electrónico de Ecuador; Gobierno Electrónico - Ecuador. https://www.gobiernoelectronico.gob.ec/recursos-de-ciberseguridad/?fbclid=IwAR06LEPn_GDsMSqBxaIU6cUZ59jShzU2FNViCdJ14yfsoZxVefn_WIwFKo4

POLÍTICA NACIONAL DE CIBERSEGURIDAD. (2017-2022). Gob.cl. Recuperado 30 de julio de 2023, de https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%c3%adtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. (2019). Cni.es. https://www.ccn-cert.cni.es/pdf/documentos-publicos/3809-estrategia-nacional-de-ciberseguridad-2019/file.html

El ámbito mundial, U. C. D. de É. en, El desarrollo económico, P. se H. C. en E. P., del Estado, lo C. H. I. la A. de M. Q. G. la P. de L. A. C. de I., & de la información por parte de las instituciones públicas y privadas., A. C. en G. la S. (s. f.). *Información y la comunicación (TIC) en nuestras actividades económicas y sociales, ha creado*. Gob.do. Recuperado 30 de julio de 2023, de https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

Costa Rica Estrategia Nacional de Ciberseguridad. (2022). Micitt.go.cr. https://www.micitt.go.cr/wp-content/uploads/2022/04/Costa-Rica-ENC-2022-Draft_FINAL_-2-1.pdf

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA. (s. f.). Unodc.org. Recuperado 30 de julio de 2023, de

https://sherloc.unodc.org/cld/uploads/res//treaties/strategies/argentina/arg0002s_html/Estrategia_Nacional_de_Ciberseguridad_de_la_Republica_Argentina.pdf

Tapia, E. (2023, mayo 31). *La banca privada líder en ciberseguridad*. Asobanca. https://asobanca.org.ec/innovacion-y-tecnologia/banca-privada-lider-ciberseguridad-ecuador-asobanca/

Flores-Álava, S., & Mena-Hernández, L., (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. 593 Digital Publisher CEIT, 8(4), 159-173, https://doi.org/10.33386/593dp.2023.4.1652

11. Anexos

11.1. Cuestionario de la Encuesta.

UNIVERSIDAD NACIONAL DE LOJA
FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA
CARRERA DE DERECHO
ENCUESTA DIRIGIDA A PROFESIONALES.

Por motivo que me encuentro realizando mi Trabajo de Integración Curricular titulado: **"ESTUDIO COMPARADO DE LAS ESTRATEGIAS Y POLÍTICAS NACIONALES DE CIBERSEGURIDAD PARA PREVENIR LAS CIBERAMENAZAS Y CIBERATAQUES QUE CONLLEVAN A LOS DELITOS INFORMÁTICOS";** solicito a usted de la manera más comedida contestar el siguiente cuestionario de encuesta, resultados que me permitirán obtener información para la culminación de la presente investigación.

Instrucciones: El problema de esta investigación, es el aumento de los delitos informáticos, ocasionados por la dependencia digital de la sociedad, la creciente sofisticación de la tecnología y su uso generalizado, donde los delincuentes informáticos, a través de ciberamenazas y ciberataques cometen el acto delictivo, vulnerando los derechos de las personas involucradas.

El crecimiento exponencial de estos delitos, es también ocasionado por la poca información, la falta de concientización y prevención en el uso de los medios electrónicos por parte del Estado, por tal razón es necesario y urgente que exista una mayor educación y difusión por parte del mismo, para propiciar una cultura de ciberseguridad en la población ecuatoriana.

CUESTIONARIO

1. **De las siguientes líneas de acción, dígnese seleccionar una: ¿Cuál cree usted, que es un aporte a las políticas criminales implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos de ciberamenazas y ciberataques?**

(….) Crear Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional especializado en el campo de la informática y el Derecho.

(….) Fortalecer la cultura sobre el uso del ciberespacio, mejorando las habilidades y la conciencia de ciberseguridad de las múltiples partes interesadas, a través de capacitaciones técnicas especializadas, de acuerdo con el desarrollo tecnológico acelerado y el panorama de riesgos y amenazas.

(….) Establecer una red de puntos de contacto nacionales, para la educación en ciberseguridad en diferentes sectores, instituciones educativas y agencias gubernamentales.

(….) Incluir contenidos educativos complementarios de ciberseguridad, dirigidos a docentes y estudiantes de educación primaria, secundaria y superior.

(….) Ampliar y formalizar la cooperación con otros organismos nacionales e internacionales de respuesta a incidentes cibernéticos.

2. **Seleccione una opción: ¿Cuál es la forma más común en la que operan los antisociales al cometer los Delitos Informáticos?**

(…..) La creación de perfiles falsos sobre la base de la información consignada en redes sociales.

(…..) Los virus informáticos y malware, que son programas maliciosos que tienden a reproducirse y extenderse dentro del sistema.

(…..) Las Transferencias de recursos de entidades financieras a varias cuentas.

(…..) La Fuga de datos, que consiste en la divulgación o publicación de información confidencial.

3. **Señalar la opción pertinente: ¿En qué nivel de educación estima usted, que sería favorable impartir conocimientos sobre Ciberseguridad, para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?**

(…..) Primer nivel o nivel inicial.

(…..) Segundo nivel de educación general básica y bachillerato.

(…..) Tercer nivel técnico-tecnológico de grado.

(…..) Cuarto nivel o de posgrado.

4. **Escoja la opción pertinente: ¿Según su criterio, qué medio tecnológico es el más adecuado para evitar los perjuicios ocasionados por los Delitos Informáticos?**

(…..) Teléfono Celular.

(…..) Computador Personal.

(…..) Tablet Personal.

(…..) Computador de uso público.

5. **¿Cree usted, que la actualización de conocimiento y correcta aplicación de la Ciberseguridad en el uso de los medios electrónicos, servirá como herramienta para disminuir los Delitos Informáticos en el Ecuador?**

SI ( ) **NO ( )**

¿Por qué?.....
……
……
……

Gracias por su colaboración.

11. 2. Cuestionario de la Entrevista.

UNIVERSIDAD NACIONAL DE LOJA
FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA
CARRERA DE DERECHO
ENTREVISTA DIRIGIDA A PROFESIONALES DEL DERECHO.

1. **Podría indicar usted, ¿Cuáles son las Políticas de Ciberseguridad implementadas por el Estado, para promover en los usuarios informáticos, la capacidad de prevención ante los riesgos existentes con las ciberamenazas y ciberataques?**

2. **¿Podría usted señalar, cuáles son las formas en las que operan los antisociales para cometer los Delitos Informáticos?**

3. **¿En qué nivel de educación, cree usted, que es recomendable propiciar el conocimiento sobre la Ciberseguridad para proteger y garantizar la correcta utilización de las Tecnologías de la Información y la Comunicación?**

4. **¿Podría usted indicar, cuáles son los medios tecnológicos más adecuados y la protección que el Estado brinda a través de la Política y Estrategia de Ciberseguridad?**

5. **¿Podría usted indicar, en qué consiste la Política y Estrategia Nacional de Ciberseguridad implementada en el Ecuador, para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos?**

6. **¿Qué sugerencia daría usted ante la problemática planteada?**

Gracias por su colaboración.

11.3. Certificado de traducción del Resumen.

Mgs. Inés Patricia Torres Ochoa

DIRECTORA ACADÉMICA DEL CENTRO DE ENSEÑANZA DEL IDIOMA INGLÉS GLOBAL QUALITY ENGLISH SCHOOL

CERTIFICATE:

Haber realizado la traducción de español al inglés del resumen del Trabajo de Integración Curricular que se titula "Estudio Comparado de las Estrategias y Políticas Nacionales de Ciberseguridad para prevenir las ciberamenazas y ciberataques que conllevan a los Delitos Informáticos" previo a la obtención del título de Abogada de autoría de la estudiante Lizbeth Sofia Palacios Orellana con CI:1104819485. Se autoriza al interesado hacer uso de la misma para los trámites que crea conveniente. Es todo cuanto puedo certificar en honor a la verdad.

Emitida en Loja, a los 14 días del mes de noviembre de 2023.

Global Quality English
CENTRO DE ENSEÑANZA DEL IDIOMA INGLÉS

Mgs. Inés Patricia Torres Ochoa
1102545850
MAGISTER EN ENSEÑANZA DEL INGLES COMO LENGUA EXTRANJERA
REGISTRO EN LA SENESCYT Número 1031-11-725053