UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS

Facultad de Educación Social y Desarrollo Humano

Escuela de Educación Social

Trabajo de Grado para optar por el título de Licenciado (a)

en

Investigación Criminal y Seguridad

Modalidad

Tesis

Estrategias de prevención enfocadas a la disminución del Ciberdelito en el corregimiento de San Carlos

Presentado por:

Poveda De La Cruz, Jacqueline Johana 2-745-78

Asesora:

Mitzila Acosta Herrera

Panamá, 2022

DEDICATORIA

Con mucho amor y cariño dedico este trabajo a mis amados padres Jacqueline y Virgilio; ellos han sido un soporte fundamental a lo largo de mi vida y con sus sabios consejos me han guiado hasta alcanzar tan anhelada meta.

De igual manera a mis familiares que con su alegría y dinamismo me alentaron en los momentos de flaqueza y me animaron a continuar hasta finalizar mi formación profesional.

Jacqueline

AGRADECIMIENTO

A Dios, por permitirme vivir una etapa más, llena de ilusiones y metas que darán origen a mi camino profesional; por darme las fuerzas y la motivación espiritual necesaria para seguir adelante sin importar los obstáculos que se me puedan presentar; por brindarme la oportunidad de demostrarme que, si puedo, aunque el recorrido sea complicado.

A el cuerpo de docentes y compañeros de la Lic. Investigación Criminal y Seguridad quienes me han acompañado desde el inicio de esta carrera incrementando mis conocimientos y brindándome su apoyo para mi crecimiento profesional.

Jacqueline

RESUMEN

La investigación que se desarrolla en las siguientes páginas trata sobre el análisis de las estrategias preventivas para la disminución del Ciberdelito y sus modalidades en el ciberespacio, teniendo en cuenta la problemática que el delito supone para la población del corregimiento de San Carlos en la provincia de Panamá Oeste.

En esta, se presenta un enfoque mixto en el que se logra medir algunas variables mediante datos numéricos, así como también, se describen las características propias del problema. Se desarrolla un diseño no experimental porque se trata de un fenómeno ya existente el cual se busca estudiar con más profundidad.

Además, se expone un tipo de investigación descriptivo y explicativo, debido a que se reseña el fenómeno y se analizan las estrategias para disminuirlo; tomando para ello el estudio exhaustivo de la muestra seleccionada e implementando los instrumentos de recolección de datos que plasman la opinión y expectativa de los residentes y autoridades del área.

Finalmente, se comprueba la importancia de las estrategias de prevención como herramienta fundamental para el control y disminución en el desarrollo del ciberdelito dentro del corregimiento estudiado.

Palabras claves: análisis, Ciberdelito, ciberespacio, disminución, estrategias, preventivas, problemática.

ABSTRACT

The research that is developed in the following pages deals with the analysis of preventive strategies for the reduction of Cybercrime and its modalities in cyberspace, taking into account the problems that crime supposes for the population of the town of San Carlos in the province of West Panama.

This presents a mixed approach in which it is possible to measure some variables through numerical data, as well as describing the characteristics of the problem. A non-experimental design is developed because it is an existing phenomenon which is sought to be studied in more depth.

In addition, a type of descriptive and explanatory design research is exposed, due to the fact that the phenomenon is reviewed and the strategies to reduce it are analyzed; taking for it the exhaustive study of the selected sample, and with the implementation of the data collection instruments that reflect the opinion and expectations of the residents and authorities of the area.

Finally, the importance of prevention strategies is verified as a fundamental tool for the control and reduction in the development of cybercrime within the studied corregimiento.

Keywords: analysis, cybercrime, cyberspace, reduction, strategies, preventive, problematic.

CONTENIDO GENERAL

INTRODUCCIÓN

El constante y desenfrenado mundo de la tecnología utilizado para la comunicación ha evolucionado con el objetivo principal de servir al ser humano. Sin embargo, de esta misma manera los ciberdelincuentes han aprovechado este espacio para disponer en él, sus fechorías con el afán de conseguir lo ajeno y apropiarse de eso. Dada la importancia de este tema, se presenta un estudio en el que se detallan aspectos importantes y relevantes del problema tomando como punto de investigación su incidencia en el corregimiento de San Carlos.

Este trabajo lo desarrollo en cuatro capítulos a saber: En el Capítulo I se abordó los aspectos teóricos que sustentan el planteamiento del problema, presento un breve repaso de las investigaciones o estudios dirigidos al ciberdelito, así como la situación actual justificada y dispuesta a ser resuelta mediante los objetivos y las hipótesis planteadas.

En el Capítulo II se introduce al tema mediante los diferentes conceptos que dan origen al ciberdelito, siendo este el Internet. Además, se reseñan otros aspectos que son piezas fundamentales al momento del estudio del ciberdelito, desde una perspectiva criminológica hasta el entorno en el que se desarrolla (el ciberespacio) teniendo en cuenta las características de su estructura para una mayor comprensión del tema.

Finalmente, en los Capítulos III y IV se detalla el proceso considerado como el más importante de la investigación, debido a que en él se desarrolla la recolección de información mediante la disponibilidad y cooperación de la muestra seleccionada, que posteriormente al ser analizada, brinda las respuestas al estudio exhaustivo realizado sobre las estrategias de prevención para la disminución del ciberdelito.

CAPÍTULO I

CAPÍTULO I: ASPECTOS GENERALES DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

La creación del Internet implicó considerablemente la aparición de nuevos paradigmas en el despliegue de la delincuencia a través de la manipulación de los medios tecnológicos.

Gómez (2010) sustenta que el Internet es un medio virtual bastante fresco; es quizás por este motivo que en la actualidad aún no se cuenta con parámetros bien establecidos que ayuden a mitigar las situaciones fraudulentas que en él se cometen. Además, de complicar su comprensión por ser una vía amplia con escasez de su propia estructura, debido a que este tema se hace cada vez más extenso y su evolución es imparable.

Saín (2015) afirma:

> **La vinculación entre tecnología y delito no comenzó con el desarrollo de las computadoras. Con el surgimiento del teléfono durante el siglo XIX se interceptaban comunicaciones para la transmisión de información de información falsa con fines económicos. Ya con la irrupción del teléfono, durante la década del 60, diferentes programadores informáticos o especialistas en sistemas intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio (p.7).**

Jewkes & Yard (2013) “Ciberdelito es cualquier ilícito penal cometido por medio de (o con asistencia de) sistemas informáticos, redes digitales, Internet y demás TIC” (p.44-45). De acuerdo con los autores, para estar frente a este delito debe existir un claro empleo de los medios o sistemas tecnológicos.

Fratti (2018a):

> **Elimina el elemento definitivo de una ciberdelincuencia, su característica de medios electrónicos, tecnológicos o de comunicaciones, por el hecho de fiscalizar una actuación común. Sin embargo, esto únicamente puede realizarse en aquellos actuares que constituyen un delito, sin la componenda de su particularidad digital (p.6).**

El cibercrimen o ciberdelito, es entonces, un fenómeno realizado mediante el Internet en donde se vulneran los datos o la información de los usuarios a través de las determinadas acciones ilegales que pueden desplegarse por este medio (Barrido, 2017).

Morales (2017a) expresa que:

> **El uso y manipulación fraudulenta de los computadores para destruir programas o datos así como el acceso y uso indebido de información que afecte la privacidad son considerados como medios relacionados con el procesamiento electrónico de datos con el que se puede dar la posibilidad de obtener un gran provecho económico así como también causar considerables daños materiales o morales, tomando en consideración la basta cantidad de datos o información que los sistemas informáticos os pueden ofrecer sobre actividades bancarias, financieras, tributarias y personales (p.109).**

Las acciones ilícitas pueden ser cometidas de diferentes maneras, debido a que cuando son realizadas a través de la red estas pueden tomar diferentes direcciones, afectando la autenticidad de las personas. Es conocidos por todos que, con los sistemas informáticos, se puede vulnerar la identidad de los menores mediante imágenes o videos que responden a la pornografía infantil (Barrido, 2018).

Por ende, los ciberdelincuentes se acogen a sus habilidades y capacidades para distraer cualquier tipo de investigación que pueda entorpecer la comisión de sus

hechos delictivos; desarrollan softwares actualizados que les sirven de escudos protectores ante las autoridades, logrando desviar la dirección investigativa que se esté llevando para dar con su paradero.

De acuerdo con Rinaldi (2017) una de las ventajas de la utilización de la red es el acercamiento que proporciona, puesto que al momento de ingresar estamos a solo un clic de acceder a la información de cualquier usuario. De esta manera, es como los delincuentes estudian a sus víctimas y luego las ultrajan.

Morales (2017b):

> **El peligro real de la humanidad radica en la posibilidad de que individuos o grupos sin escrúpulos aspiren al poder que la información puede conferirles, sea utilizada en la satisfacción de sus propios intereses en franca violación a los derechos y libertades individuales en evidente daño a los individuos de una sociedad (p.109).**

Como bien lo expresa Morales, la formación de los ciberdelincuentes representa una amenaza para la sociedad, debido a que estos se valen del poder informativo y los medios tecnológicos para cometer sus fechorías.

Mencionado lo anterior, Rayón (2014) afirma que:

> **Para hacer frente a esta forma de delincuencia se precisa realizar un enfoque supranacional, con unidades policiales de investigación especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo e, igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de conductas (p.212).**

Según la doctrina mayoritaria no existiría una clasificación autónoma de delitos informáticos. Esta categoría, o quizás, mejor, la de criminalidad o delincuencia informáticas, no expone al bien jurídico protegido (la integridad, el patrimonio) en común que los ciudadanos puedan perder; más bien, esta se ocupa de las

repercusiones o faltas que se pueden originar con la exhibición social que las personas proporcionan en las redes sin medir el efecto que pueda causar (Díaz, 2010).

Para Gustavo Saín (2015b):

> **Fue justamente durante esa época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial (p.8).**

Reafirmando lo expresado por Saín, la necesidad de analizar y crear normativas en todos los temas relativos a una conducta delictiva desde lo evolutivo y cambiante ciberespacio se hace necesario y es allí donde surgen los diferentes estudios a nivel mundial para contrarrestar la Cibercriminalidad.

De acuerdo con el análisis de Temperini (2013a) en uno de los estudios sobre los delitos informáticos (Symantec Corporation, informe de Norton sobre delitos informáticos para el año 2012) en el que, mediante entrevistas realizadas, se establece un cálculo en el aumento de delitos informáticos que afectaban a los consumidores.

La relevancia de los delitos cibernéticos es considerablemente impresionante por su contribución en la criminología del ciberespacio. Para la comunidad de Cybersecurity Ventures estamos frente a una modalidad que en estimación futura doblegará las cifras actuales, teniendo un costoso impacto económico mundial (INTERPOL, Noticias y acontecimientos, 2021a).

> **Los ataques también aceleraron el establecimiento de la Cooperativa de la OTAN. Entre las primeras actividades del Centro de Excelencia de Defensa Cibernética (NATO CCD COE) en Tallin fue encargar un importante estudio sobre la guerra cibernética realizado por un grupo internacional de expertos legales. Los expertos examinaron cómo el derecho internacional rige el uso de la fuerza cibernética por parte de los Estados y el empleo de operaciones cibernéticas durante un conflicto armado. El resultado de Tallin El manual se ha convertido en una guía para los gobiernos de todo el mundo como evalúan la aplicación del derecho internacional en tales situaciones (CCDCOE, 2013, p.23).**

En el año 2014, España evidenció una acumulación de ataques cibernéticos al igual que EE. UU. y Reino Unido; lo exaltante de dichos resultados es que no se expresaron por completo los detalles de los ciberdelincuentes; siendo este un punto interesante para el estudio del modus operandi utilizado estos delincuentes (Gonzáles, 2015).

En la misma dirección, Ruíz Díaz (2016) sustenta el origen del Centro Europeo de Cibercrimen encargado especialmente de los delitos relacionados con ciberterrorismo, en donde se logra obtener una clara visión del desarrollo y los caracteres que este abarca a nivel mundial, con su comisión ilícita desde la afectación económica publica hasta la de algunos asuntos privados. Haciendo mención en su correspondencia de delitos como el fraude, la pornografía infantil, los ataques informáticos, entre otros.

Para marzo de 2014 la República del Perú mediante su congreso nacional establece la Ley 30171, la cual se ocupa de los delitos informáticos y los diferentes aspectos que esta agrupa para las determinadas sanciones ameritadas por las comisiones de las acciones ilícitas ligadas al delito mencionado (Zuluaga, 2015).

El delito informático con mayor pena de prisión en Ecuador es la pornografía con utilización de menores, está a través de los residuos visuales (imágenes o videos) filmados y que pueden ser distribuidos con finalidades comerciales o no; observándose mayormente afectados los infantes por la aparición indirecta de estos actos denigrantes en el que se expone públicamente su intimidad (Asamblea Nacional de la República del Ecuador, 2014).

Según la Asamblea Legislativa de El Salvador (2014), la acción ilícita más perjudicial y mayormente penada es también la pornografía infantil. En donde se expone claramente la condición en la que se puede encontrar la victima (discapacidades físicas o mentales), además, del proceso para la distribución mercantil mediante la reproducción filmológica de imágenes o audios, sin importar su simulación o veracidad.

Ahora bien, el Gobierno de Puerto Rico (2012) establece como delito de mayor pena de prisión la obstrucción de las necesidades básicas proponiendo como ejemplo el sabotaje del gas, la electricidad, las telecomunicaciones, entre otras; utilizadas por el medio público y privado.

Estas penalizaciones, logran establecer un punto de vista más amplio sobre el tema en estudio y demuestra la importancia para los panameños. Es por eso que la situación nacional de este delito en nuestro país es tomada seriamente por las autoridades y se intensifican esfuerzos, para contrarrestar estas modalidades delictivas que aquejan a nuestra sociedad, especialmente a los más vulnerables que son los infantes.

La campaña para concienciación sobre la ciberdelincuencia fue realizada mediante las redes sociales por el despliegue de la situación mundial afectada por la pandemia. En ella se establecieron los aspectos relevantes para el estudio de las diferentes modalidades de la ciberdelincuencia presentadas por los

participantes de este congreso, siendo estos la línea más cercana a la realidad que brinda estos delitos (INTERPOL, Noticias y acontecimientos, 2021b).

> **Afortunadamente el Derecho Penal y el Derecho Procesal Penal han evolucionado para enfrentarse a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los principios vigentes (Concepción, 2014, p.211).**

La investigación criminal carece de los conocimientos actualizados para hacerle frente a la criminalidad desde el ámbito del ciberespacio a nivel mundial. Ahora bien, Panamá no se escapa de esta realidad y es así como las autoridades como el Ministerio Público deben buscar la manera para avanzar en la comprensión del desarrollo de los Ciberdelitos conceptualizados a nivel nacional. Además, estudiar cómo los Delitos Informáticos incrementan su auge con el transcurrir del tiempo y evolucionan en nuestro territorio, para abrir las puertas a un fenómeno preocupante para los ciberna-vegadores y el cuerpo competente del país.

Núñez (2017) sustenta que La Procuraduría de la Nación de Panamá mediante la corrección algunos aspectos del Código Penal con respecto a él Cibercrimen para sancionar las tipologías correspondientes a esta modalidad, establece ámbitos penales más claros y amplios ante la mala utilización de las redes tecnológicas a nivel nacional. Es gracias a ello, que las autoridades competentes como el Ministerio Público logran apegarse a los aspectos normativos legales que éste establece para la protección de la información personal que puede ser saboteada y ultrajada mediante el acceso ilegal de los sistemas informativos.

Afirma Rojas (2016):

> **El Código Penal de la República de Panamá, aprobado mediante Ley 14 del 18 de mayo de 2007, en su Título VIII, sobre los "delitos contra la Seguridad Jurídica de los Medios Electrónicos" regula los delitos contra la seguridad informática. Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas: a) ingresar o utilizar de bases de datos, red o sistemas informáticos; y, b) apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o inferir, interceptar, obstaculizar o impedir la transmisión. Además, determina ciertas conductas como circunstancias agravadas que aumentan la pena de prisión (p.222).**

Las estadísticas de la Policía Nacional y el Ministerio Público en el 2021 dieron a conocer que las denuncias por Ciberdelitos en Panamá aumentaron. De acuerdo con el informe del 2020 se presentaron 415 denuncias y en el primer cuatrimestre del 2021 se registraron 794 denuncias (TVN Noticias, 2021).

Se nota la preocupación nacional en la que las instituciones públicas como el Ministerio Público y la Policía Nacional trabajan en equipo y crean una campaña titulada "El Ciberdelito es Real", en el que se busca concientizar de manera general a los panameños sobre la aparición de modalidades delictivas mediante las redes informáticas, haciendo mención de algunos ejemplos de estos Ciberdelitos o bien, de los Delitos informáticos (Ministerio Público, Departamento de información y Relaciones Públicas, 2021a).

El Ministerio Público en su sección de Estadísticas del Departamento de Información y Relaciones Públicas (2021b) afirma que las denuncias sobre el Ciberdelito repuntan considerablemente en la modalidad de estafas cometidas mediante la utilización de los medios tecnológicos para el desarrollo ilegal de actividades perjudiciales para la ciudadanía en la zona Metropolitana.

De acuerdo con la publicación del periodista Luis Ávila del periódico digital Panamá América; el mayor de la Dirección de Investigación Judicial (DIJ) de la Policía Nacional, Domingo Gallardo expresó que las estafas a través de alquiler de sitios turísticos normalmente suceden en la provincia de Panamá Oeste, donde hay casas campestres o de playa (Panamá América, 2022).

1.1.1 El problema de investigación

Ante esta realidad se hace necesario poder dar respuesta a la siguiente interrogante:

¿Qué estrategias de prevención pueden aplicarse para evitar que las personas sean víctimas del Ciberdelitos y sus modalidades en el corregimiento de San Carlos?

1.2 Justificación

En atención a lo expuesto en el planteamiento, la investigación es importante porque dentro del corregimiento de San Carlos, es necesario que se considere la necesidad de proteger y tutelar a través de la información de las medidas o estrategias preventivas que se debe seguir para no resultar víctima del Ciberdelito.

Es necesario la implementación de las diversas estrategias, ya existentes, por los diferentes medios que han trabajado para la disminución del delito; a su vez aquellas que se escapan para desarrollar mejores mecanismos que, mediante su aplicación por los entes encargados, logre cambiar y disminuir los daños producidos por este tipo de delitos.

Mientras que el Internet ha conectado al ser humano con más información, existe un mal empleo de las redes, pues este mundo se convierte en el hogar de comisiones ilícitas. El mismo permite la ejecución de las actividades iliciticas con mayor facilidad pues, por medio de simples propagandas se vulnera la identidad personal y se logra acceder a su información con fines mal intencionados.

Los ciberdelincuentes buscan la forma de apoderarse de los datos ajenos obteniendo sus víctimas de forma fácil debido a que las personas brindan cooperativamente información personal sin malicia alguna. Son expertos en ganarse la confianza y una vez que han engañado a sus presas, le piden el dinero, lo toman y desaparecen. Pero se puede proteger el bienestar individual y social, armándose de conocimientos sobre las diferentes plataformas que son utilizados para dar origen a delitos en el mundo virtual.

En base a lo anterior, se justifica la necesidad de aprender, conocer y ejecutar las medidas de prevención para la disminución de una modalidad delictiva que crece y/o evoluciona con el entorno y la aparición de plataformas, sitios web y ciberdelincuentes que día a día depuran su modus operandi.

Se considera que, esta investigación aportará y nutrirá a los residentes del corregimiento de San Carlos con información relevante y provechosa para la educación en las medidas preventivas del delito estudiado, obteniendo así comunidades orientadas que actúen como trasmisoras y comunicadoras en las áreas aledañas.

Además, logre brindar una guía de consulta para fines académicos de los futuros profesionales en las grandes ciencias de la criminología y el arduo análisis de modalidades delictivas evolutivas y con constante cambio como lo es el cibercrimen.

1.3 Hipótesis

De acuerdo con Sabino (2014) la hipótesis es un intento de explicación o una respuesta provisional a el fenómeno que establece una delimitación del problema que se está investigando.

Hi: Las estrategias de prevención del Ciberdelito son beneficiosas para la disminución de este fenómeno.

Ho: Las estrategias para medir el ciberdelito nos ayudarán a la disminución de esta conducta.

1.4 Objetivos

Los objetivos representan una guía importante elaborada estratégicamente en una serie de pasos o etapas para conseguir la meta deseada.

1.4.1 Objetico general:

Analizar las estrategias de prevención del Ciberdelito en el corregimiento de San Carlos.

1.4.2 Objetivos específicos:

- Explicar la naturaleza del Ciberdelito en el corregimiento de San Carlos.
- Determinar que tanto conocen los pobladores del corregimiento de San Carlos sobre el Ciberdelito y las estrategias para prevenirlo.
- Describir las estrategias de prevención del ciberdelito existentes en el corregimiento de San Carlos.

CAPÍTULO II

CAPÍTULO II: MARCO TEÓRICO

2.1 El Internet y la Cibercriminalidad

Para poder comprender el Ciberdelito es necesario estudiar el nacimiento y aparición del Internet, que posteriormente abre las puertas a un mundo de modalidades delictivas que usan como vía, los medios tecnológicos. Como lo expresan Van & Vrakend (2012a), al momento de investigar el ciberdelito y las modalidades que este agrupa se hace imprescindible comprender lo que este agrupa desde su aparición en el ciberespacio, su estructura y la configuración que en este se desarrolla. Es importante mirar el Internet como una ventana amplia de nuevos conocimientos que han sido mal empleados para la comisión de fechorías digitales.

2.1.1 Origen y evolución del Internet

Al hablar del Internet debemos estar claros que se trata de un medio completo, Flores (2012a) proporciona algunas situaciones a través de la crónica del Internet que enmarcan la aparición de las redes informáticas dependiendo de las necesidades de la era. Iniciando por el periodo militar desarrollado en los años 70; luego la etapa académica en los años 80 y los primeros de los 90; a mediados de este mismo año la era comercial; para finalizar con la era social del actual siglo.

Cada una de estas etapas solo evidencia que las necesidades básicas como las de comunicación y demás servicios, dan origen a un mundo delictivo que se aprovecha de la carencia de cada época en la historia del Internet. Es así como las grandes organizaciones delictivas han transformado el objetivo principal de las redes para la ejecución y comisión de acciones ilícitas mediante los medios tecnológicos correspondientes a cada etapa como el teléfono, el fax, el celular, el correo, entre otros.

Flores (2012b) en definitiva, la utilización tecnológica mediante el Internet es variante, debido a que, con la aparición de nuevos fines y objetivos, su propósito es modificado por criminales que se aprovechan de la amplia estructura virtual y realizan su cometido, enfocado principalmente en vulnerar una sociedad de la información que cada día es manipulada al antojo de los ciberdelincuentes.

Consecuentemente, Montoya (2014) afirma que los principales usuarios y consumidores del Internet lamentablemente son los criminales que se vuelven expertos en su utilización. Es por ello que, la incertidumbre ante la evolución de este medio establece una preocupación para poder conseguir la manera de contrarrestar a las nuevas actividades criminales, las cuales suponen un auténtico desafío para las autoridades. Cada supuesto avance, frena a las autoridades, debido a que una de las desventajas de la evolución es la privación de nuevos conocimientos y la forma para hacerle frente.

2.1.2 Aspectos del Internet presentes en el desarrollo de delitos

La acción delictiva depende en gran medida de los conocimientos que se tienen sobre los aspectos, conceptos, componentes o características del medio configurado (el Internet), el cual es la vía principal en donde se ultraja y accede la información personal o la identidad de los miembros de la sociedad virtual. Al conocer estos aspectos se logra violar las reglas y parámetro que rigen el ciberespacio, ocasionando una manipulación indebida del medio. Para un ciberdelincuente es primordial el dominio de los aspectos que configuran la red, así como la dirección básica que brinda la misma y la forma en el que la información puede o no cambiar de destinatario.

2.1.2.1 Características

El Internet posee un funcionamiento que puede resultar complejo para aquellos que desconocen los diferentes aspectos que éste abarca, por ende, Van & Vrankend (2012b) proporcionan las siguientes características:

- Conmutación de paquetes: este proceso consiste simplemente en la toma del mensaje en sus diferentes formas (residuos visuales, ilustraciones, texto, etc.) separados en pequeñas fracciones (paquetes) distribuidos en tutas que pueden ser aleatorias; al llegar al destino la información original vuelve a sus estructuras iniciales.

Es importante mencionar, que a diferencia de este sistema a los tradicionales (el teléfono). La comunicación y el envío de mensajes puede ser mediante diferentes formas.

- Addressing and routing: para el transporte de información no se expresa claramente un origen, sin embargo, los mensajes contienen una dirección individual para el traslado del paquete de emisor a receptor.

La ruta es fijada por los “enrutadores” o “routers”, encargados de proporcionar la dirección correcta al mensaje. Su función principal consiste en contrarrestar la aglomeración virtual para que los mensajes sean enviados por diferentes rutas hasta el receptor.

Para ello, no se puede obviar el hecho, de que en muchas ocasiones se pierden los datos en la trasmisión, para ello se reenvía el mensaje en donde se logra solucionar la distorsión y se proporciona un intercambio de información seguro sin importar que la red sea subyacente, fuera inestable o no fiable.

- Protocolo de comunicación: Generalmente, es el encargado de establecer el orden de envíos de los paquetes, brindando un paso directo en el proceso de traslado de información.

Sin embargo, en Internet, este proceso es diferente, debido a las plataformas como Word Wide Web (www), email los cuales están divididos en capas llamadas Layers que se enfocan en proporcionar una estructura para establecer el orden de parámetro utilizados por las otras redes; haciendo de esta forma, un proceso más sencillo.

- Gestor de direcciones IP y nombre de dominio: En este punto, se emplea el siguiente paso en el que se establece una dirección de IP, se predetermina a un solo mensaje desde el origen hasta los dispositivos asignados como destinatarios sin interrupciones, ni errores.

2.1.2.2 Componentes

Según Quevedo (2017) los componentes estructuran la red de forma distribuida en la que los principales son servicios (hots) apoyadas en las redes de área local en los ordenadores, estos componentes son:

- Los routers: Encaminan el mensaje con ayuda del IP asociando las redes con los servicios. De esta forma, se logra obtener una sola vía para que la información pueda ser desplazado con facilidad.

Su función es realizada con algoritmos, puesto que no solo se trata de la ruta, también influye su valor económico que básicamente son el factor más importante para las redes de empresas.

- Redes de acceso: Con la utilización del módem se encarga de transformar la señal análoga de la señal del computador. Anteriormente solo se realizaba este proceso por medio de una red telefónica tradicional.

Actualmente se refleja este avance mediante las redes inalámbricas como 3G, el Wi-fi encargados de anclar a los dispositivos portales como el celular móvil, tabletas, ordenadores permitiendo de esta forma el acceso a Internet.

- Redes de área local: Mejor conocidas como LAN los cuales interconectan los dispositivos al Internet mediante los routers o módem. Cabe destacar que el modem solo proporciona una conexión fisca y el routers desplaza los datos de la LAN al Internet.

- Servidores o Hosts: Enlazan las redes y los servicios para alojar su conexión con el Internet.

2.1.2.3 Aplicaciones y servicios

Bernal (2017) afirma que la disponibilidad en servicios y aplicaciones que brinda la red hace del Internet una plataforma completa utilizada a nivel mundial. Un ejemplo de ello es The World Wide Web, la cual representan la red más conocida por brindar los siguientes servicios:

- World Wide Web (www): para poder gozar de sus servicios necesita utilizar el http mediante el navegador como el Google, el Chrome, entre otros.

Es importante aclara que el Internet no solo es el protocolo “www”; este es el medio que permite conectar dispositivos múltiples y la World Wide Web solo es una aplicación.

- Dominio de internet blindados: En este punto se establece lo que tradicionalmente conocemos como las restricciones en los diferentes servicios. El objetivo del Internet es proporcionar un ingreso seguro a estos servicios mediante el ordenador. Actualmente dicho blindaje es ejecutado a nivel de redes produciendo una separación en los servicios (Internet y Extranet).

- Navegadores (Web Browsers): Con estos se logra recopilar a información o los datos extraviados y borrados mediante los http que tienen su versión de seguridad actualizada quedando en sus siglas HTTPS (Hypertext Transfer Protocol Secure).

- Cookies: Son guardadas por el navegador del dispositivo utilizado, creando un historial de la información visitada en los diferentes sitios web, de esta forma cada vez que se ingrese al mismo sitio, la cookie será leída por el navegador web, sin ser modificada.

- La Internet profunda o Deep Web: Esta representa una plataforma compleja hasta en su acceso, debido a que la protección de estas páginas es más profunda y solo se accede a ella mediante la intranet. Está protegida por cortafuegos o sean solo accesible por la intranet. La Deep web son los datos almacenados en un banco de información que reproducen las páginas web.

2.1.3 La Cibercriminalidad

Luego de exponer los aspectos que presenta el Internet, se procede a tratar en qué medida esas características, componentes, aplicaciones y servicios influyen en el desarrollo de los delitos.

Tal y como se ha planteado, la información digital es proveniente del desarrollo de los diferentes esquemas que engloba el ciberespacio, la red o el internet, de esta forma se logra una telecomunicación virtual instantánea sin importar en qué lugar del mundo te encuentras.

Tejada (2012) afirma que, para la delincuencia tradicional, esto es un gran avance en el que ya no importa el lugar en el que se encuentre su víctima, los criminales pueden tener un acceso inmediato y preciso de su blanco. Ahora bien, esto representa un obstáculo que puede frenar el proceso investigativo y el enjuiciamiento de aquellos ciberdelincuentes que desarrollan la comisión de delitos mediante la vía o medio virtual.

Cabe señalar que, al evolucionar el medio utilizado para el desarrollo delictivo, cambian las modalidades delictivas tradicionales y así se dificulta la manera de contrarrestar el auge que supone el ciberdelito para el mundo y el ámbito jurídico penal. La ciberdelincuencia actual abarca todo el sistema que comprende y estructura a el Internet, por ende, su estudio cada vez es más complejo.

No se puede obviar el hecho de que el internet es un medio que correlaciona las culturas, conocimientos y aspiraciones mundiales, es por eso que frente a esta gran plataforma se abre una puerta a la delincuencia y el crecimiento considerable en la victimología del ciberespacio. Ya no importa la lejanía de la zona que escoge el delincuente, debido a que en menos de un segundo estos ya

controlan y vulneran la información a las que acceden; de esta misma forma y por este medio, distribuyen los datos para la propagación de la información que ahora les pertenece.

Otro aspecto para considerar dentro del despliegue del internet como una red mundialista son los obstáculos que esta establece al momento de penalizar cualquier delito realizado mediante las herramientas tecnológicas, sus autores y el equipo tecnológico utilizado para llevar a cabo el delito.

Todos los factores que se encuentran dentro del gran mundo del internet son considerados como elementos de riesgo. De acuerdo con esto realmente se podría decir que la ciberdelincuencia ha cambiado completamente la criminalidad tradicional. Según Pérez (2016) tanto el Derecho Penal como el Derecho Procesal deben hacer frente a este fenómeno evolutivo que afecta en gran medida a las personas que utilizan el medio virtual para trabajar, comunicarse y compartir.

2.2 Nacimiento y generalidades del Ciberespacio

Sin duda alguna, la evolución y la trasformación en los sistemas de comunicación virtual ha generado una nueva visualización e interpretación del mundo.

El internet se ha convertido en el centro para la distribución de servicios, en donde tenemos acceso a los servicios básicos como la educación, la comercialización, el esparcimiento social y cultural mediante un medio virtual que permite también la compra y venta de los productos imprescindibles para la cotidianidad del ser humano.

Por este motivo, actualmente existen diversas empresas dedicadas únicamente a satisfacer el público cibernético que accede a las plataformas mediante su ordenador para obtener cualquier servicio o mercancía. De esta forma se ha logrado proporcionar una herramienta útil para los emprendimientos impulsando y fortaleciendo la superación personal. Sin embargo, los delincuentes también se benefician de lo que la red puede ofrecerles y con eso desarrollan sus estrategias para acercarse a sus víctimas y extraerle todo lo posible desde la inocencia de los demás usuarios que ven el internet como un medio positivo que les facilita en gran medida la vida.

El ciberespacio ha evolucionado y con el la forma de conceptualizarlo y explicarlo. Debido a las modificaciones que este ha arrojado a lo largo del tiempo, se han creado normativas penales; esto trajo también la aparición de nuevas culturas y grupos dejando atrás a muchas sociedades con poderes políticos que ya carecían de los conocimientos necesarios para hacerle frente a los actuales espacios virtuales que predominan en la comunicación, comercialización, educación y demás aspectos que en épocas pasadas eran desarrolladas solamente de forma presencial, restándole tiempo, pero haciéndose más costoso el proceso para poder obtener algún servicio.

Es así como William Gibson (1948) dio origen a la primera conceptualización de lo que hoy conocemos como ciberespacio con el objetivo de poder establecer la correlación entre las zonas internas y exteriores de los ordenadores. Hoy por hoy, esto es delimitado desde ese momento en el que los participantes (público en general) acceden al medio y se convierte en cibernautas. Es aquí donde se fundamenta la relación de los consumidores con la red, por ende, cada vez que el ciberespacio es abierto para la comunicación, estamos frente a una forma alternativa de acercamiento social (TIC) (Valdés, 2013).

Según los autores Martínez, Leyva & Félix (2014) al momento de acceder a datos tecnológicos y su canje estamos frente a frente navegando en el ciberespacio, puesto que este medio permite la interconexión de personas y su información mediante los dispositivos tecnológicos como las tabletas, los móviles o computadores. Es como tener una sociedad en un mundo que no podemos palpar, pero en donde el usuario se relaciona con el triple de personas que de forma ordinaria no lograría conocer.

Los ciberespacios pueden agruparse por comunidades y no siempre están abiertos al público, esto es lo mágico de este mundo. Cuando se logra comprender la responsabilidad de postear tu información personal o a compartir datos por esta vía, debes saber también que en el momento que se decide abandonar el sitio, lo colgado y distribuido en el perfil no desaparecerá.

Algunas personas piensan que existimos de forma virtual y somos parte de una sociedad escondida en la red; esto pasa porque actualmente la gran mayoría de las actividades que realizamos son compartidas mediante el uso de medios o plataformas virtuales que han creado en la conciencia del ser humano un mundo real y mejor al que ya vivíamos.

Si bien es cierto, la digitalización ha modificado en cierto modo la forma de relacionarse proporcionando un esquema ciber social en el que aquellos individuos poco sociales han experimentado ser parte de un grupo que los comprende y atiende perfectamente sus necesidades. Es aquí donde las redes sociales como plataformas de interrelación en las diferentes comunidades ha generado un entorno placentero del cual es inevitable no ser parte.

Pero no solo las plataformas como las redes sociales solventan esa carencia del mundo real, también las aplicaciones como Amazon han logrado suplir a la sociedad de cualquier mercancía, haciendo de esto un mercado a gran escala

en el que ya no es necesario ni siquiera salir de la comodidad del hogar. Esta aplicación ha modificado tanto a la sociedad que ha producido que las grandes corporaciones dejen de vender presencialmente.

Es esto el motivo del desastroso impacto económico de muchas corporaciones en donde cada uno de sus ingresos ha ido en descenso. Actualmente en EE. UU., no existe la tradicional renta y venta de películas debido a las nuevas aplicaciones que facilitan el entretenimiento para cada miembro de la familia, brindándoles una cartelera impresionante de series, películas, novelas mediante las plataformas digitales como Disney Plus o el afamado “Netflix” que casi todos utilizamos en la actualidad.

2.3 La Ciberdelincuencia y el ciberdelito

La palabra ciberdelito en los últimos años se ha convertido en un concepto de uso común, pero sigue siendo difícil definirla con precisión, porque al igual que el crimen tradicional, la ciberdelincuencia tiene muchas caras y se realiza de distintas formas.

De acuerdo con Ortega (2013) debido a la amplitud del mundo del ciberdelito y todo lo que este agrupa, se hace dificultoso poder establecer los medios para contrarrestar su comisión. El alcance que este fenómeno acarrea evidencia la necesidad constante en la actualización de conocimientos para el manejo de este tema.

Expuesto esto, para nadie es un secreto que durante mucho tiempo ha existido en el mundo un desafío por establecer la conceptualización correcta para abarcar el amplio campo del ciberespacio y las tipologías que este agrupa. Más allá del enfoque claro y el término correcto para el crimen realizado mediante la

vía tecnológica o informática; se debe hacer un estudio pertinente para la denominación de las figuras criminológicas que se encargará de dar origen a las ciber modalidades.

El término de ciberdelito permite conocer aquellas modalidades virtuales realizadas en el ciberespacio, las cuales en gran medida pueden ser iniciadas digitalmente o terminar así; pero también con este concepto se ha logrado agrupar aquellas modalidades realizadas con la utilización de algún medio tecnológico que sirve como instrumento facilitador del delito.

Por otra parte, mundialmente se opta por la utilización del término ciberdelito porque es el vocablo más apegado establecido y estudiado en el Convenio del Consejo de Europa sobre el Cibercrimen realizado el 2001, evento que marcó para toda la historia el uso de este término en lo sucesivo.

Según ATS (2014) es complicado establecer una terminología exacta para el ciberdelito, de debido a ello, existe una profunda confusión para los autores y la sociedad en general que cada día busca ilustrarse sobre el comportamiento y despliegue de esta modalidad virtual.

Ahora bien, debido a dichas circunstancias y confusiones en la terminología correcta, muchos países incluyendo el nuestro, utilizan el término de “delito informático”. La problemática para la conceptualización recae en la contemplación que tiene cada Estado, gobierno o país del mismo, puesto que, para muchos depende del medio que se emplea (plataformas tecnológicas) y en otros lo que importa es el dispositivo utilizado (ordenadores, tabletas, celulares); en otras civilizaciones también varía la tipología que se establece desde el delito tradicional hasta su ejecución por medio virtual y tecnológico.

Según el Convenio de la Ciberdelincuencia (2001) en el artículo 14 establece que para estar frente a un cibercrimen es necesario la participación relevante de los medios informáticos, es por eso que determinan tres perspectivas en las que puede determinarse dicha participación del dispositivo tecnológico, ya sea como: la herramienta sobre la que se produce el delito; el elemento sobre el cual ocurre el hecho, la herramienta utilizada para cometer el delito; por último, como la base de la información extraída.

Cabe destacar que el soporte de la información se encuentra bien estudiado en el art. n°1 del mismo documento, en donde se mencionan los sistemas que también se encuentran presentes. Gracias a toda esa clasificación que agrupa las perspectivas del medio o instrumento, actualmente los países pueden establecer en que caso responde a un delito informático.

Como se evidencia, la ciberdelincuencia es muy amplia y puede ocurrir de muchas maneras. Como dice Kamariah Musa, Ismail, Abd Ghadas, & Md Radzi (2015) podemos llamar ciberdelincuencia a los crímenes, que son perpetrados por el uso de una computadora o a través de las tecnologías de la información y la comunicación, o como comentan otros autores la ciberdelincuencia es usada para referirse a cualquier crimen que involucra computadoras, redes o dispositivos de hardware.

Thomas & Loader (2000, citado por Quevedo 2017) brindan una definición aproximada para conceptualizar las acciones realizadas mediante la utilización de medios tecnológicos y las diferentes redes como la ciberdelincuencia.

La ciberdelincuencia es un área del crimen de rápido crecimiento, dado que el aumento de los delitos informáticos en parte se debe al incremento de los usuarios profesionales en informática (Murashbekov, 2015) y que gracias al internet les han dado la oportunidad de cometer crímenes de manera eficaz y sin

mucho riesgo, tanto los que se denominan como tradicionales como los nuevos tipos de delitos.

La criminalidad desarrollada en los Ciberdelitos expresa los diferentes aspectos realizados por el delincuente en el que se involucra el medio que utiliza, la forma de emplearlo y su capacidad para la adaptación en el medio actual de la sociedad, lo cual le brinda esa confiabilidad y credibilidad para el acercamiento al público virtual.

2.3.1 Clasificación de la Ciberdelincuencia

Dada la amplitud de la definición de ciberdelincuencia como cualquier delito que solo se puede cometer usando computadores, redes de computadores u otras formas de comunicación de la información; la literatura a través de los años han brindado diversas clasificaciones para ayudar a los investigadores, desarrolladores y creadores de la ley a definir el tema de manera más limitada, desarrollando esquemas que vinculen los delitos informáticos con características similares en grupos semejantes a las clasificaciones de los delitos conocidos como tradicionales.

Para Tatarinova, Shakirov, & Tatarinov (2016) la ciberdelincuencia está dividida en: Crímenes contra los derechos personales (el acoso) delitos contra la seguridad financiera-pago electrónico inseguro y delito contra la moralidad de los niños (Acoso escolar).

Así mismo, Trochez (2019a) clasifica en el convenio sobre delito cibernético del (Council of Europe, 2001) y su protocolo adicional la ciberdelincuencia de acuerdo a las conductas legalmente prohibidas que se ajustan a la etiqueta del delito cibernético, y estas son: Los Delitos contra la integridad en general de los

sistemas informáticos y datos; también los relacionados con infracciones de derechos de autor y derechos afines; y lo actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos.

Trochez (2019b) clasifica la ciberdelincuencia en tipo I y tipo II. El primer tipo tiene las siguientes características:

- Generalmente es un evento singular o discreto desde la perspectiva de la víctima.

- A menudo se ve facilitado por la introducción de programas de software criminal como registradores de pulsaciones de teclas, virus, rootkits o caballos de Troya en el sistema informático del usuario.

- Las introducciones pueden, pero no necesariamente, ser facilitadas por vulnerabilidades.

El segundo tipo que incluye actividades como el acoso cibernético, el chantaje, la manipulación del mercado de valores, el espionaje corporativo complejo y la planificación o realización de actividades terroristas en línea tiene las siguientes características:

- Generalmente es facilitado por programas que no se ajustan a la clasificación de la delincuencia. Por ejemplo, las conversaciones pueden tener lugar usando IM (mensajería instantánea) y los clientes o archivos pueden transferirse usando el protocolo FTP.

- Generalmente hay contactos o eventos repetidos desde la perspectiva del usuario.

2.3.2 Métodos de la Ciberdelincuencia

Según Pascual (2013) actualmente existen algunos métodos utilizados para esquivar los parámetros de seguridad en los sistemas tecnológicos. Cabe señalar, que con la evolución de la tecnología y la expansión virtual estos métodos han revolucionado la forma de ver el internet como un medio libre de las acciones ilícitas llevadas a cabo por la ciberdelincuencia.

2.3.2.1 Botnets

El primer método utilizado por la ciberdelincuencia es el Botnets o redes de Bots y su finalidad ayuda a mantener un control que puede ser establecido por el criminal creador de algún malware en donde mediante el spamneo o los ataques al sistema pueden auto protegerse y acceder a cualquier otra red. Con ayuda de este método los ciberdelincuentes crean comunidades dispuestas y encargadas de la opresión mediante la red y evitan ser restringidos con los spams.

2.3.2.2 Spoofing

Este método es utilizado para la suplantación de identidad de las personas. Es así como los ciberdelincuentes consiguen un acercamiento a los demás usuarios de forma fácil y creíble, debido a que las víctimas confían en que se trata de algún familiar, amigo o conocido. Es necesario añadir que existen diferentes tipos de Spoofing, los cuales son:

- IP Spoofing: Esta se ocupa especialmente de la dirección IP que posee cada usuario. El criminal suplanta dicha IP para obtener el acercamiento con el destinatario original de la información y es así como consigue obtener los

datos personales ajenos. También la IP Spoofing permite acceder a las cuentas privadas de servicios o empresas en línea.

- ARP Spoofing: Esta forma alcanza desviar los paquetes en su proceso de traslado, debido a que se intercede entre la red y el dispositivo.

- DNS Spoofing: Cambian los nombres de dominio y la dirección IP mediante su alteración en donde el criminal falsifica la codificación y la manipula a su conveniencia. Estos métodos pueden asociarse con herramientas como el Pharming.

- Web Spoofing: Para desarrollar este método se vulneran los sitios web y todos los datos suministrados por el consumidor del navegador son recogidos e interceptados. Es necesario aclarar que este método es igual al Phishing, puesto que, en el caso de la Web Spoofing se mantiene una comunicación del usuario y la página web, por lo que la víctima no logra percatarse de la situación.

- Mail Spoofing: Este método solo permite una suplantación parcial en las direcciones de email, en donde se logra eludir la seguridad con un reporte de spam.

- GPS Spoofing: El objetivo de este método es conseguir la información fundamental mediante la suplantación de las señales de satélites, proporcionando una ubicación errónea y violando los satélites autorizados. Para la realización de este proceso se altera la ubicación real traspasando la a otro dispositivo o sistema que el criminal desea. Un ejemplo de las aplicaciones utilizadas por este método es aquello que poseen los vehículos con sistema de tripulación automática.

2.3.2.3 Ataques Brute Force

Estos son los ataques por fuerza bruta en dónde se logra vulnerar los sistemas protegidos con contraseñas diseñadas para la protección y la seguridad de la red. Al momento de estar frente a un ataque por fuerza bruta se necesita acceder a un sistema restringido con la intersección en sus algoritmos y la estructura que comprende el mismo.

Para lograr establecer este ataque el criminal se vale de diferentes herramientas qué le permiten acceder a los sistemas mediante la codificación de variables correspondientes a las determinadas contraseñas que el usuario haya podido establecer para la protección de dicho sistema.

2.3.2.4 Ataques JavaScript

Con la nueva modalidad de los sitios web titulada 2.0, se ha logrado abrir puertas a un nuevo ataque desarrollado mediante JavaScript.

Este lenguaje se desarrolla para la creación de aplicaciones utilizadas por el cliente en el cual se puede acceder a los diferentes navegadores web y el usuario alcanza a observar la estructura completa del sitio que visita. Expuesto esto, los ciberdelincuentes ven una vía accesible por este medio en los que desvían a los usuarios a visitar nuevas páginas confines distorsionados e ilícitos.

Lo complicado y riesgoso de este tipo de ataques, es la inseguridad que proyecta la manipulación de los diferentes sitios web, puesto que, muchos de los usuarios piensan estar frente a la página original en la que en su cotidianidad pueden acceder para la obtención de algún dato o información relevante con

fines académicos, entretenimiento, comercialización y/o comunicación. Actualmente, este es uno de los ataques con mayor fuerza debido al daño y la complejidad elevada en la fragilidad de los usuarios que visitan los diferentes navegadores.

2.3.2.5 SQL Injection

La evolución virtual ha traído consigo muchas otras formas de atacar los sistemas, es por eso que la inyección de los códigos SQL es considerada otra forma para interceptar la información de los sistemas.

Mediante este tipo de ataques se ha logrado acceder a las bases de datos de los sistemas que el criminal desea obtener. El modo para poder desarrollar estos ataques es completamente sencillo, debido a que solo se necesita un usuario y la contraseña de acceso que este ha creado.

El desarrollo de la estructura de bases de datos es facilitado por el contenido sencillo que presentan los códigos de SQL. Es por eso que, los criminales logran realizar fácilmente su cometido, puesto que son expertos en el dominio de este lenguaje.

Con este método de ataque se logra acceder a la información de las bases de datos con la facilidad de modificar lo predeterminado de la red, alterando de una u otra forma hasta su acceso por medio de un cambio en el restablecimiento de las contraseñas.

2.3.2.6 Rootkits

Este método, también puede ser considerado un tipo de ataque al sistema, debido a que, con su correcto desarrollo, los ciberdelincuentes pueden crear y asociar aplicaciones para conseguir un acceso directo al sistema, obteniendo también un camuflaje y un ingreso bastante privilegiado al cual no cualquier usuario puede acceder.

2.4 Delitos informáticos: conceptos, prevención y riesgo

De acuerdo con Márquez & Mousalli (2016a) la utilización de la informática a nivel mundia ha sido de mucha importancia frente al desarrollo de la sociedad; debido al acercamiento de cada usuario con los diferentes servicios que la red les ofrece, desde un medio de comunicación, como una forma de educarse e instruirse y como fuente de crecimiento personal y profesional.

Márquez & Mousalli (2016b) afirma que, en la actualidad, el mundo virtual cuenta con muchas plataformas como las bibliotecas virtuales, las videoconferencias o los chats para la comunicación, los foros con carácter académico, los blogs en los que normalmente compartimos nuestra información, entre otros; utilizados como un medio que permite la interacción entre los diferentes usuarios. Todo esto, sin exclusión por la raza, sexo, orientación sexual, cultura, rango social o nivel económico; proporcionando así, una socialización continua en la que el público en general logra crecer en conocimientos interculturales produciendo un mundo que integra a todos los miembros de su entorno.

Cuando se realiza alguna acción contraria a las normativas legales estipuladas por el gobierno de algún país, se podría decir que se está frente a un delito (Tundidor, Nogueira & Medina, 2018). En base a esto, la comisión delictiva es un

proceso en el cual influyen muchos factores como el avance local en diferentes entornos produciendo un origen considerable en el mundo cibernético que también es explotado para la obtención ilícita de datos o para el acceso indebido en sitios que son propiedad de personas ajenas a los delitos concebidos por esa vía.

Torres (2015) afirma que se debe considerar todos aquellos aspectos que pueden quedar ligeramente sueltos en la seguridad o protección de las organizaciones, es por eso que el ámbito empresarial ha sufrido considerables golpes convirtiéndose en una víctima más de los Ciberdelitos.

Con las nuevas ideas para procesar la información se ha logrado incorporar una forma más factible en la que las mismas son procesada sin importar que tipo de datos son. Pero esta modernización no es del todo positiva ya que, permite que muchos ciberdelincuentes accedan a la información de los usuarios y apropiarse de ella para llevar a cabo los mencionados robos de identidad, fraudes o estafas en grandes empresas reconocidas a nivel mundial por sus sistemas de información digital para los servicios de comunicación y el envío de multi contenido para los usuarios que están adscritos y reciben dichos beneficios.

La telecomunicación brinda un enfoque actualizado de la sociedad moderna. En este aspecto Riestra (2016) establece que, compartir los datos por medio de la tecnología puede llegar a ser perjudicial para los usuarios que se exponen en las redes y se vuelven vulnerables ante el desarrollo de modalidades cometidas con el fin de lucrase a costillas de la información extraída mediante los medios por los ciberdelincuentes. Esta información es realmente cotizada, porque en muchas ocasiones estamos hablando de datos confidenciales de las empresas en donde los delincuentes logran ingresar y apropiarse de ella para cobrar por su distribución o protección de los demás clientes.

Ampliando un poco más este punto, Oxman (2013) menciona que la informática es un instrumento fundamental que proporciona muchos beneficios. Entre ellos podemos mencionar la facilidad para adquirir información, la utilidad de diferentes dispositivos tecnológicos portátiles que facilitan las actividades para la comercialización y comunicación del ser humano.

Fuentes, Mazún & Cancino (2018) estudian los delitos informáticos y los establecen como una tipología correspondiente al ciberespacio. Para el desarrollo de esta, se debe ocasionar una acción que cause daños a terceros e involucre la utilización y el empleo de algún dispositivo informático. Ahora bien, esta categoría puede abarcar delitos tradicionales que en consecuencia son realizados por algún medio tecnológico o virtual; generando una conceptualización de la digitalización de las diferentes tipologías del ciberdelito.

En expansión, la Organización para la Cooperación y el Desarrollo Económico (2014) situando a Ruiz en 1996, expresa que el delito informático da respuesta a las acciones ilegales que integran a los datos de la red y la información trasladada por la vía cibernética.

La conceptualización para estos delitos es complicada y compleja porque para muchas normativas estos dan respuesta a los Ciberdelitos, cibercrímenes, terrorismo cibernético, interrupciones telemáticas, estafas u otros delitos que requieren de la tecnología. Es necesario saber cómo enfrentar cada una de estas aristas en las que se está presentando una modalidad evolutiva que no discrimina el tipo de víctimas. La protección puede ser obtenida por medio legal o ilegal para la seguridad interna de los perfiles, cuentas o sitios personales y de corporaciones.

La exposición que obtenemos mediante los medios tecnológicos es perjudicial, pues los delitos informáticos han expuesto diferentes esquemas para violar la privacidad y aumentar el riego de los ataques cibernéticos. Los atentados contra los sistemas informáticos son de gran preocupación para las comunidades del ciberespacio las cuales desarrollan la gran cantidad de sus actividades sin pensar en el riesgo al cual se exponen cada vez que ingresan por medio del navegador.

Ejemplo de las vulneraciones que producen estas modalidades delictivas es la exposición de integridad e identidad personal, ataques la seguridad informática y la protección de datos en general. Esto se puede entender por la sección o la categoría a la que pertenece cada uno, teniendo en cuenta para su división las cualidades o factores que se desarrollen en cada uno.

Es así como cando se habla de delito informático, se toma como punto principal el medio por el cual delinquen sus autores que en este caso se trata del ciberespacio. Esta modalidad también conjunta los daños que se pueden ocasionar en esta vía tecnológica.

La creación de leyes aplicables a la penalización de los delitos informáticos y sus variantes es fundamental. No puede existir una antigua normativa que intente resolver la problemática que estas nuevas modalidades suponen para la sociedad. La naturaleza del delito debe estar bien descrita para su comprensión y el conocimiento del alcance que esta puede tener.

2.4.1 Tipología de los Delitos Informáticos

La variedad agrupada en los delitos informáticos es extensa, pero Lara, Martínez & Viollier (2014a) establecen una categorización amplia y general de la tipología del delito informático, en la que menciona las siguientes:

- El acceso no autorizado: Se detalla a la falta de autorización para el ingreso en los sistemas informáticos en donde se debe contar con un previo permiso que muchas veces es violado por expertos en la estructuración ilícita de contraseñas o codificaciones para obtener el acceso.

- El daño a los datos o programas informáticos: Aquí se produce una alteración en los esquemas cibernéticos de forma ilícita con la que se puede eliminar o desaparecer información.
- El sabotaje informático: Mediante esta se logra distorsionar los sistemas informáticos con restricciones, bloqueos o interferencias de las redes.

- La interceptación no autorizada: Realizados para la vulneración parcial o completa de los dispositivos tecnológicos.

- El espionaje informático: Obtienen los datos mediante la vigilancia exhaustiva para luego propagarla o distribuirla con finalidades de lucro sin importar que sea de carácter público o privado.

Con referencia a esta última tipología, Luna (2018) afirma que el espionaje informático es considerado como una de las modalidades más realizadas en el ciberespacio. Para realizar esta modalidad es importante la parte mal intencionada de una investigación por parte de los autores delictivos para el estudio pertinente de sus víctimas.

Pero esta modalidad en especial también abarca otros campos como lo es el espionaje en el área industrial, dentro de su desarrollo resalta la utilización de los tradicionales equipos como los micrófonos o grabadoras que permiten la recolección de la información. Cabe destacar que, las diferentes modernizaciones han traído consigo la utilización de dispositivos como móviles y ordenadores que mediante aplicaciones se puede adquirir la información deseada por los criminales.

El espionaje puede realizarse de manera industrial, como antes se mencionó, o en ámbito informático. Para ampliar la redacción del primero se pueden mencionar algunas características que se desarrollan en la comisión de esta como lo es la extracción de información sobre proyectos, vulneración del mercadeo empresarial los cuales son normalmente realizados por la competencia empresarial que el organismo en cuestión tiene.

Por otra parte, para el ámbito informático se desarrollan acciones ilícitas con el objetivo de manipular la información personal mediante la red y las diferentes plataformas tecnológicas para poder extorsionar o chantajear a la víctima.

Dentro de este punto Flores (2013) establece otra clasificación que permite observar perspectivas diferentes de los delitos informáticos desde su intelectual autor denominado en la conceptualización informática como hackers, en los que se puede mencionar los siguientes:

- Black hat hackers o bien, los hackers de sombrero negro: Normalmente estos crean virus para quebrantar los medios informáticos con la pérdida de los datos tecnológicos.

- White hat hackers o en español, hackers de sombrero blanco: Son lo opuesto a los antes mencionados, debido a que estos se encargan de salvaguardar la información siguiendo los parámetros de seguridad que puede poseer algún sistema.

- Gray hat hackers o también llamados, los hackers de sombrero gris: Encargados de seguir una estructura ambigua, lo cual puede llegar a debilitar su apoyo en la protección de información.

- Script kiddies: Estos son nuevos en el sistema y por ende carecen de la información necesaria para perjudicar cualquier medio tecnológico.

- Phreaker: Al contrario del script kiddies, son criminales altamente capacitados para atacar los medios telefónicos mediante celulares, móviles, entre otros.

- Newbie: personaje en la ciberdelincuencia que tiene como pasatiempo la búsqueda de indagación en los temas de la informática para la comisión de los hechos delictivos.

- Lammers: Improvisan en la comisión delictiva de los Ciberdelitos, debido a que no cuentan con la capacidad para programar cautelosamente cada punto antes de ejecutar alguna acción ilícita.

Esta clasificación evidencia el porcentaje sobre los ciberdelincuentes agrupados en la categoría de hackers en donde cada uno proporciona una forma distinta de operación para cometer sus fechorías.

Aclarado esto, se prosigue con la clasificación de los tipos de delitos informáticos según Lara, Martínez & Viollier (2014b):

- Crakeo: Se delimita por perjudicar los sistemas para la seguridad informática. En esta sección aparece la figura de cracker, la cual responde al especialista en la incentivación mal intencionada para las transacciones económicas ilícitas. Estos individuos suelen alterar y complicar el debido desarrollo de los sistemas tecnológicos.

Los crackers no son hackers, es por lo que el primero no respeta ni cumple lo estipulado por el otro. Estos acostumbran a quebrantar la ley de forma superior sin importar las consecuencias. Los crackers responden a un comportamiento un tanto diferente en el que solo se guían por las normativas establecidas por ellos mismos.

- Cibergrafitti/Defacements: para Assis (2010) el defacements es el "daño producido de manera intencional en una página web" (p. 56).

Por otra parte, el ciber grafiti responde al cambio de información que estructura las diferentes páginas web. Para ello el delincuente se sirve de contenido obsceno para producir presión en sus víctimas.

- Fraude nigeriano.

> **El fraude nigeriano es conocido como el fraude de pago por adelantado, por lo general consiste en un mensaje de correo electrónico falso de un extranjero que necesita ayuda para retirar una determinada cantidad de su país y ofrece al destinatario un porcentaje del dinero por ayudarle en la transferencia. A pesar de que este correo no es muy confiable, muchos de los destinatarios han caído y han perdido varios miles de dólares en el proceso, porque los ciberdelincuentes solicitan varios pagos por adelantado para facilitar el trato (Meseguer, 2013, p. 507).**

Aunque este tiene su origen en África, actualmente México también ha sido víctima de esta modalidad peculiar. Este delito es ejecutado con una distribución errónea a los diferentes usuarios de plataformas como el correo electrónico, para hacer depositar dinero a las víctimas haciéndoles creer hasta el final de que se trata de una transacción ilícita.

Los autores de esto delitos son personajes altamente capacitados para la evasión de equivocación en el proceso y su descubrimiento como miembro de las organizaciones que comúnmente desarrollan estos delitos.

- Ingeniería social: Se podría definir como “aquellas estrategias y técnicas que se usan para obtener información de las personas mediante la psicología” (López & Restrepo, 2013, p. 16).

El autor de este delito es conocido como el ingeniero social el cual se ocupa de manipular al perjudicado mediante llamadas telefónicas o texto vía correo en donde logran extraer los datos y realizar su cometido.

- Phishing.: “Consiste en el envío de correos electrónicos a una persona con información falsa, con el fin de que esta persona envíe datos personales al remitente” (Anzit, 2013).

Como bien lo expresa el autor, mediante el phishing los delincuentes recopilan información por medio del engaño a sus víctimas que normalmente utilizan el correo electrónico. Una de las modalidades delictivas con mayor popularidad es el mundo cibernético es esta, debido a que sus autores no descansan hasta lograr que de diez personas a las que les envían información falsa, por lo menos la mitad caiga.

Los phishers son personas altamente capacitadas para la ejecución delictiva mediante a una plataforma en la cual a través del spam puede ser reportado, y finalmente estos logran salir bien librados la mayoría del tiempo.

Para el desarrollo de esta modalidad se ejecutan dos etapas. La primera da origen con la distribución de mensajes falsos mediante el correo a los diferentes destinatarios, en la que se busca extraer la información relevante; y la segunda, luego de contar con los datos los delincuentes transfieren el dinero extraído al exterior de lugar de donde base para la comisión del delito para finalmente se retira la ganancia.

- Keylogging: “Son dispositivos o programas con el que se puede grabar todo lo que el usuario digite mediante el teclado y mandar toda esa información a terceros” (Mollo, 2013, p. 44).

Mediante este medio se logra sabotear a los clientes virtuales y así extraer sus dineros y bienes mediante el software base en dispositivos portátiles como el ordenador o modem que permiten su instalación en otros equipos, desarrollado por esta modalidad de los delitos informáticos.

Esta sección presenta dos perspectivas importantes que ayudan a la comprensión de estas, en la cuales se puede mencionar lo siguiente: los Keylogger hardware, encargados de forma limitada de transmitir la información de la red; y los Keylogger software emergen normalmente como virus que espían las actividades realizadas por las personas mediante su ordenador o dispositivo.

- Robo de identidad: Consiste en “la obtención de datos personales reservados o secretos relativos a la identidad de un individuo” (Flores, 2014a, p. 310).

En este punto, se desarrolla una usurpación de información en donde los más perjudicados son las víctimas porque el mismo extravía su identidad y muchas veces no sabe cómo recuperarla en donde se enfrenta a situaciones que ponen en duda hasta su identificación personal.

Con la información robada, los ciberdelincuentes trafican datos para organizaciones criminales que necesitan perfiles libres de delitos para pasar desapercibidos.

Por otra parte, el “robo, hurto, sustracción o usurpación de identidad, aunque la más conocida es la de robo de identidad” (Flores, 2014b, p. 312). De acuerdo con Flores, la terminología varia pero la conceptualización de cada una de estas palabras toma vida en el momento que los criminales realizan sus fechorías causando un daño terrible en los usuarios a quienes se vulnera su integridad personal.

- Ciberbullying/Ciberacoso: Esta puede ser realizada por el simple hecho de que “cualquier persona con acceso a la tecnología puede participar o estar en riesgo de acoso cibernético” (Paul, K. Smith & Blumberg, 2012a, p. 640).

La modernización ha contribuido a la comisión de delitos como la pornografía infantil en donde directamente se puede afectar la salud mental y emocional de las personas víctimas. Lastimosamente estas modalidades son la parte mala de las redes en la que se llega a despreciar la interrelaciones con objetivos o fines positivos.

Desde el punto de vista de Paul, K. Smith y Blumberg (2012b) “el acoso y la violencia escolares son dos acciones distintas, pero que conjuntamente hacen del niño o adolescente una vida complicada en el colegio” p. 641.

Aclarado las situaciones expuestas por los autores, el acoso escolar responde a la persecución discriminada entre los alumnos; y la violencia escolar contempla una agresión directa que puede ser física, mental o psicológica entre los propios compañeros o las autoridades escolares.

El ciberbullying es el “acoso que se da entre menores mediante insultos, humillaciones, amenazas a través de redes sociales u otros medios de comunicación” (Loredo & Ramírez, 2013a, p. 47).

Además, este tema puede ser tratado como un acoso mediante la red, en donde se desarrollan burlas o mofadas en contra de menores que utilizan sus redes sociales como el Instagram, Facebook, Twitter para compartir información que es recopilada para utilizarla en su contra haciendo referencia muchas veces en su aspecto físico, discapacidad u otros.

> **Una clasificación de ciberacoso es: Provocación incendiaria o flaming (…); Hostigamiento o harassment (…); Denigración o denigration(…); Suplantación de la personalidad o impersonation (…); Difamación y juego sucio, outing and trickery (salida y engaño)(…); Exclusión social o exclusión y ostracismo (…); y el Acoso cibernético o cyberstalking (…) (Bartrina, 2014, p. 390).**

De acuerdo con Bartrina, dicha clasificación es expuesta para que se conozcan las diferentes formas en las que se puede presentar el ciber acoso. En estos casos se debe evaluar cada situación y los factores que propician estas modalidades desde temprana edad.

- Cibergrooming.: Wachs, Wolf & Pan (2012) explican la relación entre el aspecto antes mencionando y esta categoría, en la que ambas son muy cercanas, pero también tienen un desarrollo distinto.

Esta categoría se refiere a la acción de ultrajar a los menores mediante las vías tecnológicas, especialmente por medio del Internet. En ella es necesario que el criminal establezca un vínculo con su presa, para lograr el cometido, es así como mediante empatía y comprensión los menores terminan siendo víctimas del Cibergrooming.

> **Se conoce como el cortejo, o grooming, al proceso de acercamiento entre un acosador o depredador en línea hacia un menor de edad; el perseguidor prepara el encuentro físico entre ambos y tiene por objeto eliminar la resistencia del menor hacia los extraños y hacia contenidos inapropiados para el (Velasco & Hernández, 2012a, p. 13).**

- Sexting: Se refiere “al uso de móviles para mantener charlas de índole sexual, donde voluntariamente se genera contenido que implique una situación erótica o sexual” (Loredo & Ramírez, 2013b, p. 47).

La adquisición de dispositivos tecnológicos por menores de edad ha facilitado el acercamiento de desconocidos con objetivo o fines realmente perturbadores en dónde mediante la utilización de videoconferencias o videollamadas surgen conversaciones de índole sexual entre menores y adultos; o adolescentes contemporáneos.

Los dispositivos tecnológicos como los celulares o computadoras actualmente cuentan con diferentes aplicaciones que permiten el acercamiento virtual sin importar en que parte del mundo te encuentres, es por eso que los gobiernos

tienen la necesidad de estipular claramente la forma en la que se actúa en cada modalidad correspondiente a los Ciberdelitos, debido a que si no se establece con pulcritud las características que debe presentar cada modalidad para ser penada, se puede seguir contribuyendo a la realización y propagación de estas conductas.

Expresándolo con claridad, el sexting responde al sexo por mensajes de textos establecido desde el punto de vista tradicional; sin embargo, la modernización ha permitido que el internet establezca una conectividad más efectiva donde ya se puede ver con quién hablas.

- Pornografía infantil: Para Loredo & Ramírez (2013c) “el problema de la pornografía infantil es quizás el más grave que enfrenta la sociedad; las víctimas quedan marcadas de por vida por daños físicos y/o emocionales” (p. 47).

Es mediante la pornografía infantil como muchos menores son privados en libertades que posteriormente se convierten en desafíos que afectan su crecimiento, debido a que las cicatrices psicológicas llegan a deteriorar el crecimiento personal de aquellos infantes. Es de suma importancia que las autoridades presten atención a estos delitos que no se escapan de los medios tecnológicos, puesto que hoy en día su visualización ante la sociedad es muy diferente.

Actualmente se ha llegado considerar que esos menores participan voluntariamente de las imágenes, videos o audios distribuidos con fines de lucro y es preocupante la inconsciencia con la cual la tecnología ha llevado al ser humano interpretar situaciones tan complicadas y perjudiciales.

A través de la historia del ciberespacio, no se llega a mencionar este tipo de modalidades tan perjudiciales para el bienestar de una parte fundamental de la sociedad, es por eso que en esta investigación se hace referencia a todas las actividades explícitas realizadas por medio de los sistemas informáticos que perjudican de forma directa, debido a que estas siguen siendo una forma de entretenimiento para esa porción de la población con ideas perversas y distorsionadas de lo que está bien, es así como día a día se observa la cantidad de archivos descargados en las páginas de internet que promocionan este contenido.

Brindando una propagación de pornografía infantil a nivel mundial realizada vía internet y dándole pasó a criminales que se aprovechan del contenido multimedia impropio.

- Phreaking: Burgos (2014a) expresa que el phreaking puntalmente se refiere a las intercepciones de llamadas a larga distancia.

El autor de esta modalidad es denominado como phreaker, por sus amplios conocimientos en todo el mundo de las telecomunicaciones a través de las redes telefónicas qué son utilizadas actualmente para los fraudes, las extorsiones y hasta el sabotaje de los mismos medios empleados como herramienta para la ejecución de esta modalidad.

- Hacktivismo: De acuerdo con Burgos (2014b) esta hace relevancia al punto de los caracteres políticos, debido a que uno de sus objetivos es la modificación del pensamiento democrático en donde mediante la creación de las plataformas tecnológicas se permite acceder a los usuarios consumidores de dicho contenido que puede ser utilizado con la manipulación predeterminada sobre la víctima.

Está modalidad agrupada en diferentes actividades entre las que se pueden mencionar la distribución de correos a líderes políticos, la creación de diversas comunidades dedicadas a la democracia y el compromiso patriótico, los sitios web con contenido político. En la cual se enmarca la preocupación eminente de un grupo considerablemente grande y en aumento qué puede contratacar a la sociedad mediante la utilización de los medios o vías tecnológicas.

- Virus: “los virus informáticos son similares a sus homólogos biológicos, ya que son capaces de auto replicarse” (Philco & Rosero, 2014a, p. 46).

Los virus son una herramienta utilizada por ciberdelincuentes, debido a que con estos softwares los mismos pueden llegar a duplicar un usuario y el conocimiento del propietario original. Cuando se ejecuta el acceso de las diferentes plataformas virtuales, los virus logran ocasionar daños considerables a la estructura del sitio o página web en donde se vulnera toda la información con la eliminación de los archivos o programas pertenecientes al mismo.

Los virus pueden entrar fácilmente en el ordenador o dispositivo tecnológico, ya que con tan solo la descarga y la instalación de algún archivo no verificado el virus puede colgarse y expandirse por todo el sistema del equipo informático.

“Existen diferencias entre los virus informáticos, dependiendo del modo en que se instalan y propagan” (Philco & Rosero, 2014b, p. 46-47), por ende, se establecen las siguientes clasificaciones:

- Gusano: Su distribución es automática y no necesita de un código para poder adueñarse de los servicios del sistema de datos de un dispositivo, este puede ser considerado una aplicación maliciosa que se duplica.

- Troyano O caballo de Troya: Pretende colarse en el software para ser visto como un esquema original. Lo preocupante de este virus es que suele ser colado o pasado por contenido multimedia. Un dato curioso de este virus es que puede ser utilizado con los gusanos.

- Bot: También conocido como robot web: Estos suelen obedecer las órdenes del hacker, por ende, son como un ejército de robots manejados por el líder que es su creador, su operación es casi indetectable debido a que muchas veces los usuarios del ordenador los alojan por meses y no sé percatan de su presencia.

2.4.2 Los delitos informáticos desarrollados en empresas

Con referencia a lo anterior expuesto, una de las modalidades más desarrollada en el ámbito cibernético, es el espionaje informático que de acuerdo con Loredo (2013) da origen a diversas características pertenecientes a otros delitos tradicionales, es así como la extorsión de información de carácter privado perteneciente a empresas ha sido un mecanismo aprovechado por los ciberdelincuentes; además de la apropiación indebida de los fondos bancarios y vulneración de la ética profesional de organizaciones. Esto último permite la eliminación, discrepancia, intersección de archivos con carácter privado y público.

Los virus mencionados con anterioridad, son una vía rápida para la distribución indeseada de toda la información perteneciente a empresas internacionales.

Mendieta, Zambrano & Ordoñez (2016) afirman que la gran mayoría de los documentos afectados de los sistemas informáticos mediante la vulneración de

su seguridad es debido al acceso que tienen los ciberdelincuentes a través del despliegue de virus que proporcionan en el sistema.

Según Temperine (2013b) Uno de los grandes miedos para las empresas es la implantación de virus que existe a nivel mundial para la comisión de los ciberdelitos. Está distribución ha logrado infiltrar programas pertenecientes a organismos reconocidos qué resultan víctimas de los hackers y sus procedimientos para la restricción de documentación oficial y archivos privados que muchas veces son extraídos con la finalidad de vendérselos a la competencia.

En esta misma línea Quiroga (2018) afirma que la participación de estas figuras es de gran importancia para las diferentes empresas que se han visto vulneradas por las actividades delictivas. Muchos de los hackers y crackers utilizan estás modalidades a gran escala para conseguir una motivación personal, en alcance supremo de entidades reconocida en determinados países, es por lo que su capacitación intelectual sobre temas informáticos es totalmente suficiente para llevar a cabo cualquier modalidad delictiva que agrupe los delitos informáticos mediante la utilización de vías o medios tecnológicos. De esta manera logran obtener un beneficio no solo en términos económicos, sino también emocional por el sentimiento de satisfacción al cometer el ilícito soñado.

Es necesario mencionar que los programas producidos por las empresas no cuentan con la seguridad suficiente para que los ciberdelincuentes no puedan acceder. Realizando así plagios y clonados del autor predilecto y dejando interpuesto la protección de los archivos que conllevan estás aplicaciones. Los ciberdelitos crecen y las empresas deben buscar la forma de apegarse a las normativas legales y penales que puedan enjuiciar dicha ilicitud.

López (2013) afirma que no todos los delitos informáticos causan el mismo desbalance económico para las empresas, por ende, los dueños de estás desconocen de muchas tipologías concernientes al gran mundo del ciberespacio.

En este apartado se ha mencionado la aparición de las figuras criminales ejecutoras de los ciberdelitos o delitos informáticos, sin embargo, en muchas ocasiones dentro de la misma organización la competencia desleal impulsa a que entre compañeros exista una mala conciencia ética en la que se vulnera la información personal de los demás empleados mediante la extorsión de imágenes o videos que puedan empañar su imagen. Punto en el que indirectamente se logra inquebrantable a transparencia total de la organización desde la parte interna que la conforma.

Es importante mantener una constante realización de las auditorías empresariales pues con esto se logra prevenir problemas futuros y establecer la situación actual en la que se encuentra las organizaciones. Las empresas deben mantener esa idea como una herramienta fundamental para contrarrestar la ignorancia que produce la virtualidad cuando se trata de ser víctima de un ciberdelito sin darte cuenta.

Aunque la imagen de la corporación puede ser dañada con la exhibición antiprofesional de algunos colaboradores de la misma, es necesario que se mantenga un control que permita combatir la comisión de los ataques directos hacia la empresa, brindando un equipo profesional que cuente algunos conocimientos sobre los ciberataques para poder contrarrestar la comisión y el despliegue de estos en las organizaciones.

2.4.3 Sujetos presentes en los Delitos Informáticos

> **Los sujetos que participan en los delitos informáticos son: el sujeto activo, de acuerdo al profesor chileno Mario Garrido Montt, se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal; y el sujeto pasivo que es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo (Manjarrés & Jiménez, 2012, p. 75).**

Cuando hablamos de sujeto activo podríamos referirnos a toda aquella persona que tiene las capacidades de manipular e influenciar gracias a sus bastas habilidades, utilizadas para perjudicar y causar daño a otras personas siendo estas el caso el sujeto pasivo.

Además, se puede considerar un sujeto pasivo como, todo individuo que se ve afectado, es decir, quién es víctima o sufre de alguna mala práctica vista como injusticia nivel delictivo. De acuerdo con el autor podríamos decir que se refiere de igual manera a alguien que debe cumplir una obligación o acatar un resultado sin beneficio alguno, solamente respondiendo a las necesidades del sujeto activo.

Hacer un concepto nuevo sobre los delitos virtuales es fundamental, debido a que en muchos países no está reglamentado, ni existen leyes que protejan a las personas que podrían ser víctimas de estas situaciones; por ende, se entiende que muchas víctimas dejen pasar cualquier tipo de evento delictivo como resultado de no conocer alguna ley que sirva como amparo o refugio con apego jurídico.

De igual forma, no solo a nivel individual se presentan estas situaciones, también colectivamente o en las empresas que se ven vulneradas y son víctimas de este tipo de delitos en los cuales no creen fortuito realizar alguna denuncia o alzar su

voz ante lo sucedido por miedo a exponer su imagen a nivel público en una sociedad que carece seguridad tecnológica. Es así como también se empaña la imagen empresarial para próximos usuarios o inversionistas que deseen verse vinculado con dichas organizaciones.

Por otra parte, todos estos sucesos y elementos son considerados por las mentes criminales, que ven en esta, una oportunidad para realizar cualquier cantidad de delitos respaldados por la poca seguridad y falta de conocimiento que establecen un respaldo insuficiente que se obtiene por parte de las leyes y régimen distribuido en la sociedad.

Es muy fácil luego de hacer un análisis simple darse cuenta de esta situación satisfactoria para los delincuentes, creándose un blanco fácil por dónde cometer delitos y fortalecer estrategias para llevar a cabo dicha situación que al conocer los elementos necesarios se termina facilitando el trabajo.

Ambas razones contribuyen indirectamente en la aparición de los Ciberdelitos; y el perfeccionamiento en la ejecución de este, debido a que la falta de investigaciones pertinentes proporciona seguridad a los criminales en la comisión de estos delitos.

Grosso modo, los sujetos son parte fundamental para la comisión de los ciberdelitos, son los autores predilectos y la parte convaleciente de la situación realizada por el sujeto activo. La falta de normativas o documentación penal para el enjuiciamiento de los autores contribuye a la propagación criminológica de los delitos.

2.5 Origen del Ciberdelito y los acercamientos al tema en Panamá

De acuerdo con Beermann (2018) Panamá inició el tema tecnológico o informático con leyes sobre la información personal.

Así la Ley 11 de 1998 sobre Almacenamiento Tecnológico incorpora reglas o mejores prácticas para el almacenamiento de información en formato digital; su artículo 1, por ejemplo, viene a definir aspectos como Microfilmación, sistema óptico y sistema magnético que no eran más que herramientas tecnológicas del momento para almacenar información en medios digitales.

Esta ley también incorpora al código penal una figura delictiva para quien altere o adultere las “películas, microfichas, discos o certificaciones”, teniendo sobre esta el primer aviso de lo que hoy conoceríamos como delitos informáticos.

De igual forma sucede con el Código Civil incorporando a los “documentos almacenados tecnológicamente” como parte de las pruebas en la materia de contratación.

Por su parte la Ley 43 del 2001 de la Asamblea Nacional en la que se logra establecer un acercamiento considerable a los Ciberdelitos o los Delitos Informáticos, debido a que se menciona aspectos como los documentos y firmas electrónicas, gracias a esta ley también se logra visualizar una normativa para la distribución de dicha información de carácter informático o electrónico. En la misma se menciona los siguientes puntos:

- Definición de los documentos electrónicos como: Toda información plasmada de forma digital.

- Conceptualización de la firma electrónica como: Un medio para establecer el propietario del mensaje trasmitido.

- Aspectos que comprenden el mensaje de datos: Refiriéndose al cuerpo del comunicado o distribuida con la utilización de las plataformas tecnológicas.

- Terminología de los Sistemas de la información como: Todo sistema encargado de generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Esta misma ley, otorga un reconocimiento jurídico de los mensajes de datos e incorpora todo lo relativo a la firma electrónica y a los certificados firmados electrónicamente.

Por otra parte, la Ley 51 de 2008 hace algunas modificaciones en materia de firma electrónica e incorpora la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas, definiendo también aspectos de naturaleza tecnológica como el Almacenamiento tecnológico, comercio electrónico, factura electrónica, internet, nombre de dominio, tecnologías de la información y las comunicaciones, World Wide Web, entre otras.

De igual forma, amplía el concepto que hasta la fecha se tenía de los documentos escritos como todo informe que plasma de forma textual alguna información relevante, haciendo alusión a sus variantes en los diferentes aspectos como profesional, empresarial o para la comercialización.

Por último, esta ley establece un concepto de integridad, ya relacionado a los mensajes de datos y/o documentos electrónicos el cual será de vital importancia cuando veamos específicamente la figura objeto de estudio, es decir, la

interceptación de datos, ya que en muchas ocasiones cuando se intercepta un mensaje, este puede ser alterado antes de que llegue a su destinatario, lo cual eliminaría esta condición de integridad de la cual habla la presente Ley.

Otro tema que guarda relación con nuestro objeto de estudio lo encontramos en el numeral 8 del artículo 23 y el 2 del artículo 55, ambos utilizando el mismo tenor literal al establecer la obligación ya del prestador de servicio y/o del certificador del almacenamiento tecnológico el contar con “sistemas confiables o productos que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.”, mismo que introduce el concepto de Encriptación al cual debemos hacer referencia en apartados posteriores.

La Ley 65 de 2009 crea una entidad denominada Autoridad Nacional de Innovación Gubernamental y se le asignan responsabilidades que agrupaban toda la clasificación y el control de las tecnologías de la información y comunicaciones en materia de carácter público esto a tenor literal del artículo 1 de la citada Ley.

Se puede hacer referencia, entre otros, a la adaptación tecnológica y ofimática que genera el Convenio de Cooperación y Asistencia Técnica Interinstitucional, para la implementación del Sistema Penal Acusatorio en la República de Panamá firmado el 22 de julio de 2010, pieza fundamental para la implementación del Sistema Penal Acusatorio en el Segundo Distrito Judicial para el 2 de septiembre de 2010.

El 26 de septiembre de 2011, mediante Decreto Ejecutivo 709 se crea el equipo nacional de respuesta a incidentes de seguridad de la información de Panamá, entidad encargada de “dar respuesta a incidentes de seguridad sobre los sistemas informáticos y de comunicación del Estado Panameño”, como a tenor

literal establece el artículo 1 del citado Decreto, y que forma parte de una red global de colaboración internacional en temas de ciberdelincuencia.

El Computer Security Incident Response Team por sus siglas en inglés CSIRT, o Equipo de Respuesta a Incidentes de Seguridad Computacional (en español), tiene dentro de sus objetivos “la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá.”12, la misma se encuentra adscrita a la AIG.

El proceso evolutivo en la materia encuentra un nuevo capítulo cuando mediante la Ley 83 de 2012 que regula el uso de medios electrónicos para los trámites gubernamentales que tiene por objetivo la digitalización de los trámites gubernamentales con miras a reducir el tiempo y barreras físicas que representa un trámite en específico.

A raíz de estas iniciativas impulsadas por la AIG se cuenta en Panamá con plataformas tecnológicas de gran importancia para el usuario, dentro de las cuales se pueden mencionar algunas como:

- Panamá Emprende, solicitud y trámite de cambios “en línea” en materia de Avisos de Operaciones, antiguamente Licencias Comerciales.

- Panamá Tramita, plataforma virtual que muestra los requisitos propios de cada trámite, que se realiza de forma física o virtual. A palabras de la propia plataforma, lo que se busca es “la integración de la gran variedad de trámites que las diferentes entidades de gobierno les ofrecen a los ciudadanos”.

- Sistema Electrónico de Inscripción Registral (SIR), que busca permitir a los usuarios la posibilidad de realizar “todos los trámites registrales de manera electrónica, lo que ayudará a mejorar y agilizar los procesos internos, reducir el uso del papel y las largas filas”.

- Otros proyectos que ha manejado la AIG en materia de digitalización y/o interconexión en Panamá se puede mencionar Red Nacional Multiservicio, Instituto de Tecnología e Innovación, Proyecto "Panamá en línea", Red Nacional Internet 2.0 – Internet Para Todos, GEORED, entre otros.

Por último, durante la elaboración de la presente investigación, se aprobó Ley 665 de 2018 en la que habla de la Protección de lo datos personales, que coloca a Panamá en la vanguardia a nivel regional sobre la materia.

Ahora bien, lo antes mencionado no brinda una conceptualización amplia sobre la protección de los datos personales como consecuencia de la reciente aparición de esta ley. Sin embargo, se puede considerar como un avance para la penalización y las regulaciones consecuente y derivada del delito informáticos en Panamá. Abriendo así las puertas a la tipificación de sanciones mediante las autoridades competentes previamente también establecidas.

Mediante esto se refuerza la necesidad de que el autor del hecho ilícito realice alguna acción indebida con respecto a las estipulaciones de la ley, para que las autoridades competentes como lo es el MP puedan iniciar el debido proceso investigativo.

En Panamá existen algunas documentaciones o normativas legales futuras que buscan responder al acercamiento del estudio que llevamos a cabo en esta investigación, por ejemplo, el proyecto de Ley No.558 (2017) que modifica y

adiciona artículos al código penal, relacionados con el cibercrimen, si bien es cierto, el mismo no ha sido establecido como una ley, pero es muestra de las acciones que se tratan de llevar a cabo para la penalización de estos delitos.

El Código Penal de Panamá en el Título VIII de “delitos contra la Seguridad Jurídica de los Medios Electrónicos” establece algunas normativas para la seguridad informática, sin embargo, no es un secreto que existe la necesidad de una actualización en temas de Ciberdelitos, debido a que dicha modalidad va en considerable aumento.

2.6 Estrategias de prevención

De acuerdo con las Naciones Unidas (2011)

> **La prevención del delito se ha convertido en un componente cada vez más importante de muchas estrategias nacionales de seguridad pública. El concepto de prevención se basa en la idea de que el delito y la victimización se ven favorecidos por numerosos factores causales o de fondo, los cuales son resultado de una amplia gama de elementos y circunstancias que influyen en la vida de las personas y las familias a medida que pasa el tiempo, y de los entornos locales, así como situaciones y oportunidades que facilitan la victimización y la delincuencia (p.9-10).**

Con esta definición las Naciones Unidas establecen algunos tipos de prevención del delito, teniendo presente algunos aspectos relevantes agrupados en diferentes perspectivas, en las que se puede mencionar las siguientes.

- La prevención delictiva mediante el apoyo social es importante porque está logra agrupar diferentes actividades colectivas en dónde se fortalecen desde temprana edad los miembros de las familias que puedan estar expuesto a

situaciones complicadas debido a las dificultades que presenta el entorno en el que han crecido estos individuos.

Además, la prevención temprana mediante la socialización es fundamental para el control el desarrollo o propagación de las diferentes modalidades que pueden afectar directa o indirectamente a las familias. Con la preparación de diferentes programas sociales se puede estructurar una división proporcional dependiendo de las edades y la escolaridad de los participantes, para así obtener una mayor captación y distribución de la información que se desea proporcionar para la prevención de los delitos.

También es importante la participación de las entidades académicas que brindan un esparcimiento para los jóvenes quienes es por medio de la educación pueden fortalecer los criterios fundamentales para discernir entre el bien y el mal, evitando así crear más delincuentes jóvenes y desenfrenados.

- La comunidad como núcleo de la prevención delictiva es una herramienta, que bien ejecutada establece el control y la dirección de los miembros de la comunidad. Formando con ello un gran grupo de personas con un objetivo en común y con un esquema de auto seguridad para cada uno.

Es necesario escoger un foco o área específica para realizar estudios que permitan la prevención de la delincuencia; es importante determinar con claridad qué zonas mayormente están afectadas o son las más vulnerables a nivel social por su decadencia, pobreza o estirpe social

Lo más razonable, fácil y lógico para atacar a profundidad este tema, es encontrar zonas a nivel social poco estructuradas, no solo económicamente, sino también académicamente; teniendo, así como consecuencia irregularidades,

falta de oportunidades e inestabilidad familiar siendo estos sujetos blancos fáciles tanto para una campaña de prevención ciudadana o víctimas de uno de estos delitos.

Programas de prevención buscan que el individuo sea beneficiado por el sentimiento de protección y seguridad, que, de la mano con información necesaria, logre estabilizar su día a día en la prevención de estos delitos. Es de vital importancia crear en la comunidad individuos con valores, enseñanzas y actitudes que permitan una convivencia sana y provechosa.

Ahora bien, para que todos estos programas funcionen, no solo necesitamos de la población en general, sino también de que está población sirva de instrumento activo en las campañas propuestas y así lograr que los programas funcionen también formando portavoces de las ideas enseñanzas y propuestas para la sociedad y así capacitar también a los líderes comunitarios como una figura visionaria que enfoque este aprendizaje en la creación de una comunidad responsable, apta y digna.

En esta segunda percepción se logra establecer algunas categorías para la prevención en diferentes situaciones del delito; las cuales motivan el esfuerzo y los riesgos de los delincuentes; aquellas qué desvanecen las ganas y la incitación a la delincuencia; y las que simplemente ayudan a estimular tontas excusas para llevar a cabo los actos delictivos.

Se pueden crear y controlar aquellos medios que impulsan y motivan la comisión delictiva. Disminuyendo las actividades en sitios establecidos con aspectos que puedan contribuir a la delincuencia con la saturación de personas en el mismo local, áreas totalmente oscuras o desprotegidas y lugares que sean utilizados para delinquir por la carencia de sistema de seguridad apropiados.

- La prevención a través de la reinserción social, de esta forma se abre pasó a una medida preventiva para evitar reinserción en la comisión de hechos delictivos por los miembros de la sociedad.

Haciendo un análisis profundo, normalmente aquellas personas que cometen delitos reinciden en la violación de las normativas penales. De esta manera, esas personas se cierran la oportunidad de crecer y llevar una vida alejada de todo lo que vincula la comisión de delitos.

Claramente, si puede existir una reinserción completa que ayude a mejorar la situación en el entorno familiar y social. Estableciendo una vida con oportunidades de trabajo, salud, crecimiento personal con emprendimientos y fortalecimiento educativo que proporcione la satisfacción de las necesidades básicas.

2.6.1 Antecedentes de la prevención

Según Fenelly & Crowe (2013) en 1971 el Dr. C. Ray Jeffery fue el encargado de dar vida a la prevención del delito por medio de estudio del entorno en el que este se desarrolla. Pero no es hasta el estudio de Jane Jacobs (1961, citado en Fenelly & Crowe, 2013) en donde se plantea el delito y su relación con el medio donde es llevado a cabo el cual es expuesto por los autores como un entorno de carácter urbano.

Este estudio dio origen a muchas investigaciones enfocadas en los aspectos cibernéticos el que logra plasmar y conocer el espacio por el cual se llevan a cabo las diferentes modalidades delictivas del espacio tecnológico. Además, se consigue resaltar la figura como el autor o propiciador de la actividad delictiva y el encargado de la mala ejecución de las acciones contrarias a las normativas

penales que responde al término que actualmente conocemos como delincuencia.

2.6.2 Teorías relacionadas

Al momento de explicar el porqué de las acciones delincuenciales, es importante analizar los diferentes aspectos que pueden participar en el desarrollo del delito. Es por lo que Galindo (2014) establece la siguiente clasificación:

- Teoría de los “Ojos en la calle”: en la que Jane Jacobs (1961, citado en Lab, 2014a) afirma que el entorno relativamente tiene que ser un factor que motiva la comisión delictiva. Planteando así por su manera de ver la importancia del espacio en el que una persona crece y aprende a adaptarse sin importar que sea por medio de la comisión de hechos delictivos.

La visualización de esta teoría va enfocada directamente al área urbana y la vigilancia que en él se puede desarrollar. El autor proporciona formas de ver la vigilancia en un entorno urbano como un mecanismo que ayudaría a la comunidad en la protección de sus viviendas y la de los miembros de su hogar (Lab, 2014b).

- La teoría del espacio defendible se acentúa en la necesidad de crear una comunidad en el cual la vigilancia natural sea la base de una convivencia sana, tranquila y segura. Es importante, porque la sensación de seguridad permite que los individuos tengan un desarrollo para convivencia sin miedo, es por este motivo que se crean espacios y estructuras que permitan a los ciudadanos gozar de esa agradable sensación.

Las fortalezas de una comunidad se basan en la unión y la buena convivencia, por ende, es importante que los ciudadanos o individuos que pertenezcan a dicha sociedad se vean envueltos en un ambiente de pertenencia, confianza y respaldo de cada uno de los individuos pertenecientes a dicho grupo social; esto traerá como resultado que los individuos sientan el deseo y la necesidad de proteger su comunidad, espacio o sociedad a la que pertenezcan.

Según lo expuesto por los autores, un ambiente social en el cual la comunidad se encarga de deteriorar o destruir las estructuras en las cuales viven diariamente, trae consigo la decadencia de esta, puesto que al crear un ambiente social en el cual solo se ve la degradación, la falta de innovación y la miseria es ciertamente complicado que las personas salgan a delante con criterios formados para su vida futura.

También, se crea en el individuo una percepción de la pobreza y de poco interés en superación y perseverancia. Esto trae como consecuencia la toma de decisiones erróneas creando en ellos la necesidad de superación a base de delitos por medio de pandillas y situaciones fuera de la ley.

- La teoría de las ventanas rotas, indica que la sociedad al verse sumergida en un entorno de desigualdad y socialmente nefasto los lleva a pensar que no existe ninguna oportunidad de surgir en dicho lugar; atrayendo consigo al aumento de delincuencia, el descontrol y el desorden dentro de la comunidad.

Redondo & Garrido (2013) establecen que dentro de los indicadores medidos en la desorganización social se visualiza como detonante principal de la delincuencia el estrés provocado por las situaciones cotidianas del área en el que recibe la persona. Afirman que realmente la calle es una zona que puede proporcionar la motivación necesaria para delinquir.

He puesto esto se logra establecer algunas teorías de origen criminológico en la prevención del delito situacional:

- La teoría de la elección racional está enfocada por los autores como una aclaración de qué posición ocupa el sentimiento delictivo en la conducta punible antes que una exposición de esta como resultado a la ansiedad producida por el ambiente social en dónde muchas veces no existen beneficios considerables para el crecimiento y superación personal.

- La teoría de las actividades rutinarias es vista como una forma en la que la persona integre en sus actividades cotidianas la necesidad de delinquir. El contacto con el dinero en sitios públicos propicia el crecimiento delictivo del individuo.

- La teoría de la desorganización social la cual se basa en la forma en la que los individuos se desplazan habitualmente en su entorno delictivo. Haciendo de esto una rutina para la estructuración en el comportamiento de la persona.

- La teoría del patrón delictivo: Esta menciona el ambiente repetitivo que motiva el delincuente enfocándose desde el estudio conductual el criminal y las características que este puede arrojar.

Es fundamental contrarrestar esto con incentivos positivos que abarquen toda la comunidad, para que los beneficios también puedan ser distribuidos entre cada miembro de forma equitativa.

2.6.3 Prevención Situacional del Delito (PSD)

La información suministrada anteriormente beneficia la comprensión directa de este punto en la investigación realizada. La prevención situacional del delito abarca aspectos importantes del delincuente y su comisión delictiva.

La criminología juega un papel importante para la aclaración y estructuración de la PSD, debido a que es una alternativa para la comprensión de la conducta realizada por el autor del hecho; de esta manera se dispondrá la forma con la cual se pueden contrarrestar dichas actividades ilícitas.

Uitenbogaard y Ceccato (2014), logran establecer algunas técnicas para el desarrollo de la prevención situacional del delito, en la que se dimensionan las oportunidades sostenidas por las actividades rutinarias en dónde fundamentalmente se puede aumentar el riesgo de reincidencia en los delincuentes. Este segundo aspecto visualizado por la elección racional para finalmente fijar la teoría del patrón delictivo y establecer mediante los movimientos delictivos una forma exacta para la comisión de todos los hechos que el amerite.

La prevención situacional del delito establece de forma específica la delincuencia con su interacción en el entorno y la finalidad de poder reducir y prevenir las actividades delictivas obteniendo así la disminución de los riesgos a los cuales se expone la sociedad en general.

2.6.4 Prevención del Ciberdelito en Panamá

El Ministerio de Relaciones Exteriores la República de Panamá presentó ante las Naciones Unidas la experiencia en la prevención de delito y las acciones de la

Justicia Penal e instó a los países de Latinoamérica a adherirse al convenio de Budapest, para juntos enfrentar con mayor fuerza la ciberdelincuencia y proteger la integridad de los ciudadanos e instituciones estatales.

La Misión permanente de Panamá ante las Naciones Unidas, participó en el 23° Periodo de Sesiones de la Comisión de Prevención de Delito y la Justicia Penal en Viena, Austria, este mes, luego de que la Unión Europea confirmó el acceso al Convenio de Budapest, en marzo último (Ministerio de Relaciones Exteriores, Sección noticias por año, 2014a).

En esta misma línea Fratti (2018b) afirma la aprobación y adaptación del convenio sobre la ciberdelincuencia por Panamá mediante la ley 79 de 2013. Tal y como está establecido el convenio para otros países. Panamá dispone de él sin ninguna complicación debido a que conoce las ventajas y los beneficios adquiridos mediante dicho convenio mundialista conveniente para la ciberdelincuencia.

Debo resaltar que hay otras las leyes aceptadas, que mencionan el tema de la cibercriminalidad, tal es el caso de la Ley sobre Crimen Organizado que reconoció a los delitos contra la seguridad informática como crímenes graves y que forman parte de la delincuencia organizada.

De igual manera se creó la División Especializada en Delitos contra la Propiedad Intelectual y Cibercrimen en la Dirección de Investigación Judicial de la Policía Nacional que tendrá a su cargo la investigación, recolección y aseguramiento de las evidencias digitales en los procesos que involucren no sólo sistemas informáticos, sino aquellas investigaciones de campos vinculadas a cibercrímenes.

Para los trámites relacionados sobre Asistencia Mutua, la Procuraduría General de la Nación, será el punto de contacto a través de la Fiscalía de Asuntos Internacionales y de la Fiscalía Superior Especializada en delitos contra la Propiedad Intelectual y Seguridad Informática (Ministerio de Relaciones Exteriores, Sección noticias por año, 2014b).

Finalmente, en este enunciado, se mencionan competencias de las autoridades panameñas en las que para los trámites referentes al artículo 35 (Red 24/7) del Convenio, se ha señalado a la Dirección de Investigación Judicial de la Policía Nacional, específicamente, a la Oficina de Interpol Panamá, como punto de enlace.

Por otra parte, el Capital Financiero en su sección de Actualidad informa sobre la utilización de esquemas tecnológicos la cual estableció la relación entre autoridades competentes como el Ministerio Público y la Policía Nacional, cómo apoyo de la campaña que estás instituciones llevan a cabo como una medida o estrategia de prevención para contrarrestar y establecer la disminución en la comisión de la modalidad de los ciberdelitos.

Al momento las autoridades han tomado la iniciativa para reducir el número de denuncias correspondientes a las tipologías que abarca los delitos informáticos o cibernéticos; se establece una sensación de tranquilidad y protección de los bienes y la identidad personal, los cuales responden a los aspectos más afectados por la comisión de estos delitos

Esta campaña cuenta con una segunda parte en dónde se establecerá los aspectos correspondientes a la comercialización de mercancías mediante las plataformas tecnológicas las cuales también han afectado las grandes empresas dedicada a brindar estos servicios para los panameños.

2.6.4.1 Medidas de prevención a nivel nacional

Existen muchas medidas de prevención implementadas a nivel nacional para la disminución del ciberdelito, en las cuales se ha brindado información mediante todos los medios de comunicación nacionales, permitiendo el acceso a la información preventiva para el público en general.

Es importante conocer algunas de las recomendaciones generales obtenidas mediante los noticieros, las páginas oficiales de la Policía Nacional, los reportes periodísticos digitales, entre otros; las cuales son:

- Evitar compartir información personal en las diferentes plataformas digitales.
- Se recomienda no realizar transacciones con personas desconocidas y asegurarse que la persona con la que habla es quien dice ser.
- No transfiera dinero sin recibir la mercancía solicitada con anterioridad, revisar bien la plataforma por la cual realiza la compra o recibe el servicio.
- Evitar citarse con alguien en sitios poco seguros.
- Revisar las sugerencias y las referencias realizadas por otras personas, para comprobar que el sitio visitado o el perfil es real.
- Optar por usar Encuentra24, pues mediante esta plataforma existe una identificación mediante las cédulas.
- Conservar las pruebas o los datos de la transacción y su destinatario.
- Recordar que si usted es víctima de alguna modalidad del ciberdelito debe realizar las denuncias pertinentes marcando al número: 507-2988 y al 104.

Cabe destacar, que dichas medidas van dirigidas solo algunas modalidades delictivas como estafas, fraude, robo de identidad, entre otras y las mismas pueden variar dependiendo el país en el que se encuentre.

CAPÍTULO II

CAPÍTULO II: MARCO METODOLÓGICO

3.1 Diseño de investigación y tipo de estudio

Es importante realizar una investigación bien fundamentada. En los siguientes puntos, se logra evidenciar cada aspecto relevante dentro del estudio.

La investigación presenta un enfoque mixto. Se busca medir algunas variables mediante datos numéricos, pero otras se describirán y analizarán para determinar algunas características propias del problema. El enfoque mixto puede ser comprendido como “un proceso que recolecta, analiza y vierte datos cuantitativos y cualitativos, en un mismo estudio” (Tashakkori y Teddlie, 2003, citado en Barrantes, 2014, p.100)

En este sentido, corresponde a un diseño no experimental, debido a que se trata de un fenómeno ya existente el cual se busca estudiar con más profundidad, analizando la importancia de las estrategias para la prevención del Ciberdelito.

Palella & Martins (2010)), definen:

> **El diseño no experimental es el que se realiza sin manipular en forma deliberada ninguna variable. El investigador no sustituye intencionalmente las variables independientes. Se observan los hechos tal y como se presentan en su contexto real y en un tiempo determinado o no, para luego analizarlos. Por lo tanto, en este diseño no se construye una situación especifica si no que se observa las que existen. (pag.87)**

El tipo de estudio es descriptivo, tal y como lo define Sabino (citado por Martínez, 2018) al plantear que esta investigación busca reseñar los diferentes aspectos propios y las cualidades del fenómeno estudiado, mediante el despliegue de su comportamiento durante el desarrollo del estudio; por lo cual

en esta investigación se reseña la naturaleza del ciberdelito y los medios para contrarrestarlo.

Además, es explicativo porque se establece cómo las estrategias de prevención ayudan a disminuir el ciberdelito. Arias (2012), comparte que las investigaciones con fines explicativos miden los efectos que han causado dicha problemática y la comprueba con lo que arroja la hipótesis positiva.

3.2 Población

> **La población es la totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis que integran dicho fenómeno y que debe cuantificarse para un determinado estudio integrando un conjunto N de entidades que participan de una determinada característica, y se le denomina la población por constituir la totalidad del fenómeno adscrito a una investigación (Tamayo, 2012, p. 180).**

Para los fines de este trabajo de investigación, la población en estudio fue la conformada por 8 888 habitantes del corregimiento de San Carlos, entre las edades de 20 a 44 años.

De igual forma, un funcionario de la 19ava Zona Policial ubicada en el corregimiento de San Carlos, especialista en el análisis estadístico de los hechos delictivos presentados a nivel de zona.

3.2.1. Sujetos o muestra

Según Hernández-Sampieri & Mendoza (2018) afirman que la muestra responde a un subconjunto de la población, extraído para la obtención veras de la información que es certificada con el rango de confiabilidad que la misma pueda

brindar. Esta porción tiene el objetivo de representar a la población seleccionada en general para la investigación.

Imagen n°1:

Cálculo del tamaño de la muestra

Fuente: Asesoría Económica & Marketing S.C.

De las 369 personas que representan la muestra de la población entre las edades de 20 a 44 años, solo se logró la participación de 50 residentes de la comunidad del corregimiento de San Carlos a quienes se les aplicó el instrumento para la recolección de datos.

Además, se logró contar con la participación del Subteniente Fulvio Morales, especialista de la 19ava Zona Policial ubicada en el corregimiento cabecera del distrito de San Carlos.

3.2.2. Tipo de muestra estadística

El tipo de muestra presentado en esta investigación es no probabilístico por conveniencia. Este tipo de muestreo responde a una sección de la muestra no probabilística, la misma es tomada teniendo en consideración los aspectos que brindan los participantes para el desarrollo de la investigación. La disponibilidad, la facilidad para el reclutamiento y las consideraciones del investigador describen por completo en que consiste el muestreo escogido (QuestionPro, 2020).

Los 50 participantes y el funcionario de la 19ava Zona Policial, evidencian la muestra no probabilística por convivencia, debido a que para su colaboración se dispuso de su voluntariedad y disponibilidad con la investigación. Cabe destacar, que la misma se logró de forma efectiva, con mayor velocidad y menos representación en los costos valorados.

Por otra parte, la estimación del tiempo para la recolección de los datos fue relativamente corto para lograr una cooperación de los 369 representantes residentes del corregimiento de San Carlos.

3.3 Variables

Una variable hace referencia a una herramienta utilizada para medir indicadores en donde sus resultados pueden proporcionar la susceptibilidad de la investigación. (Hernández, Fernández & Baptista, 2010). En otras palabras, las variables son diferentes elementos que influyen en un objeto o proceso que se investiga.

Variable independiente: Estrategias de prevención.

Definición conceptual:

> **Forma de pensar y practicar la prevención del delito más allá de la pena, que posee efectos sociales y culturales característicos. En tanto forma de pensar, cada estrategia involucra una serie de presupuestos teóricos y políticos, que no sólo articulan una visión acerca de la cuestión más estrecha de cómo prevenir el delito, sino que involucran una serie de perspectivas acerca de un conjunto de problemas más o menos conexos con aquél" (Sozz, 2008, citado por Schulman, 2012, p. 4).**

Definición operacional: Mecanismos empleados con la finalidad de contrarrestar las conductas ilícitas que pueden presentarse en modalidades delictivas como el Ciberdelito.

Se va a medir a través de los siguientes criterios:

- Conocimientos que tiene la población sobre las estrategias de prevención.
- Frecuencia con la que se utilizan y se desarrollan.
- Aporte que brindan para la disminución del ciberdelito.

Variable dependiente: Ciberdelito.

Definición conceptual:

Rayon & Gómez (2014) afirman que:

> **Se entiende por "ciberdelito" o "cibercrimen" cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito (p.211).**

Definición Operacional: Los Ciberdelitos son conductas desviadas e ilícitas que ocurren a través de medios informáticos o tecnológicos y ameritan de la intervención de estrategias preventivas que ayuden a limitar sus alcances en el mundo evolutivo en el que vivimos.

Se va a medir a través de los siguientes criterios:

- Evaluación en el acceso a los medios o plataformas tecnológicas.
- La afectación en la seguridad de las personas y sus bienes.

3.4 Instrumentos y técnicas de recolección de datos

Para la recolección de información sobre el tema en estudio, se emplearon las técnicas de encuesta y entrevista, que permitieron la obtención de datos relevantes.

Para Bernal (2018) “La encuesta (...) consiste en tener información de las personas encuestadas mediante cuestionarios diseñados en forma previa para la obtención de información específica”.

El método designado para el primer grupo de estudio es la encuesta. La recolección de los datos se obtuvo por medio escrito con la participación de los 50 participantes residentes del corregimiento de San Carlos, provincia de Panamá Oeste, seleccionados por conveniencia para el desarrollo del instrumento de recolección elaborado de manera controlada y directa. El instrumento utilizado para reunir los datos consiste en cuestionario cerrado para la aplicación de las encuestas, contiene doce (12) interrogantes.

Para el segundo grupo de estudio, se realizó una entrevista a través de un cuestionario abierto de seis (6) interrogantes, directamente al Subteniente Fulvio Morales, funcionario de la 19ava Zona Policial ubicada en San Carlos cabecera. Lanuez & Fernández (2014) definen la entrevista como un medio propicio para la recolección de información personal, mediante el proceso de comunicación entre el investigador y el participante.

3.5 Procedimiento

Para llevar a cabo la investigación, se implementó el siguiente procedimiento, establecido por etapas:

Etapa 1: elaboración o estructuración del estudio científico.
Inicialmente se escoge el tema mediante la investigación de las referencias bibliográficas, tratando así de obtener un estudio que guarde relación y aporte conocimientos a la licenciatura; posterior a eso, se delimita mediante una problemática existente con el fin de encontrar y emplear mecanismos para combatirlo en una determinada zona (corregimiento de San Carlos), teniendo en cuenta el área o porción en la que repercute el fenómeno estudiado. Se plantea el problema investigado y se justifica con la situación preocupante.

Etapa 2: selección, elaboración y validación, de los instrumentos de mediación.
Se elaboró el instrumento y fue validado por jueces expertos, para su respectiva aplicación mediante el desarrollo de las técnicas (encuesta y entrevista) capaces de proporcionar los indicadores. Estos instrumentos evidencian el fenómeno estudiado y su repercusión en la muestra de la población abordada de forma no probabilística por conveniencia dentro de un área determinada (corregimiento de San Carlos, Panamá Oeste).

Etapa 3: Aplicación de instrumentos.
Dando respuestas estrechamente asociadas a las bases de la investigación mediante encuestas ejecutadas con cuestionarios sencillos y preguntas concisas en la población del corregimiento de San Carlos para conocer y logra determinar el estado, situación o conocimiento que presenta la muestra abordada. Además, de la realización de una entrevista al funcionario de la 19ava Zona Policial, quien se considera un medio potencial de información acerca del tema tratado.

Etapa 4: análisis de resultados

Finalmente, se analizarán los resultados con gráficas y tablas con un tipo de estadística descriptiva que evidencien el grado o porcentaje de impacto del estudio.

CAPÍTULO IV: ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

CAPÍTULO IV: ANÁLISIS Y DISCUSIÓN DE RESULTADOS

El análisis e interpretación de los resultados según Hurtado (2010), “Son las técnicas de análisis que se ocupan de relacionar, interpretar y buscar significado a la información expresada en códigos verbales e icónicos” (Hurtado citado por Ramírez, 2013). Luego de aplicar los instrumentos para la recolección de datos, se procede a analizar los resultados arrojados por las encuestas y la entrevista.

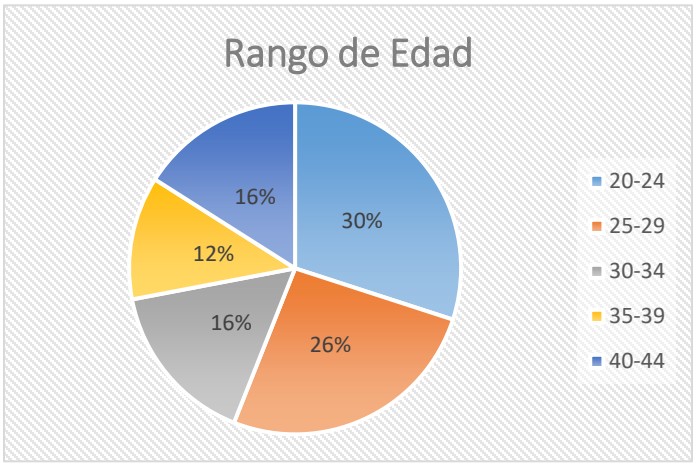
4.1 Resultados obtenidos de la encuesta realizada a los 50 participantes del corregimiento de San Carlos

Para establecer una amplia comprensión de los resultados aportados por la muestra escogida y sus opiniones en la encuesta, se realizaron tablas y gráficos de forma porcentual con los datos.

Tabla n°1. Rango de edad de los encuestados

Grupos de edad	Cantidad	Porcentaje
De 20 a 24 años	15	30%
De 25 a 29 años	13	26%
De 30 a 34 años	8	16%
De 35 a 39 años	6	12%
De 40 a 44 años	8	16%
Total	50	100%

Gráfico n°1. Rango de edad de los encuestados

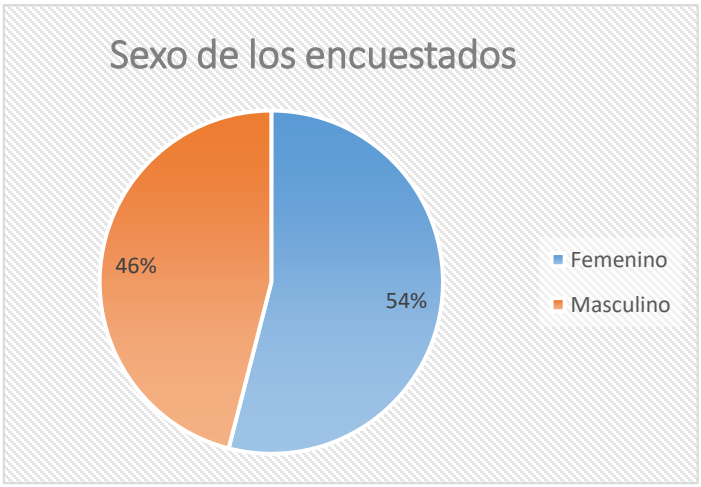


Con respecto a la pregunta sobre la edad de la población encuestada se obtuvo 15 personas entre las edades de 20 a 24 años, 13 entre las edades de 25 a 29 años, 8 entre las edades de 30 a 34 años, 6 entre las edades de 35 a 39 años y 8 entre las edades de 40 a 44 años. Resultando el rango de 20 a 24 años con un 30% como la población con mayor participación en la encuesta y un 12% en el rango de 35 a 39 años con menor aparición.

Tabla n°2. Sexo de los encuestados

Sexo	Cantidad	Porcentaje
Femenino	27	54%
Masculino	23	46%
Total	50	100%

Gráfico n°2. Sexo de los encuestados

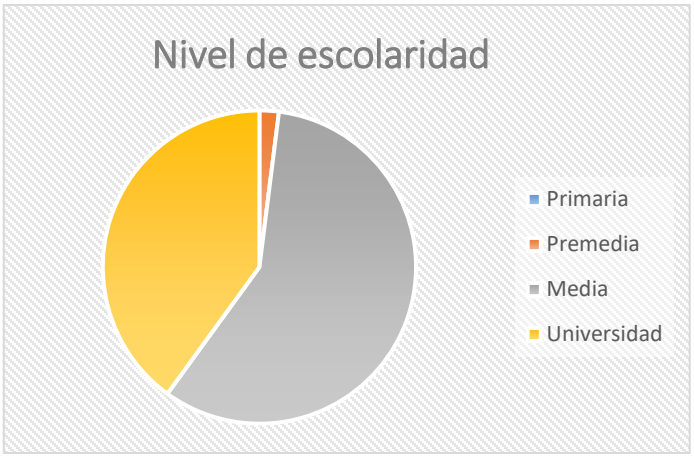


Con respecto a la pregunta sobre el sexo de la población encuestada se obtuvo 27 mujeres y 23 hombres. Resultado una mayor participación del sexo femenino con un 54%.

Tabla n°3. Nivel de escolaridad de los encuestados

Nivel de escolaridad	Cantidad	Porcentaje
Primaria	0	0%
Premedia	1	2%
Media	29	58%
Universidad	20	40%
Total	50	100%

Gráfico n°3. Nivel de escolaridad de los encuestados

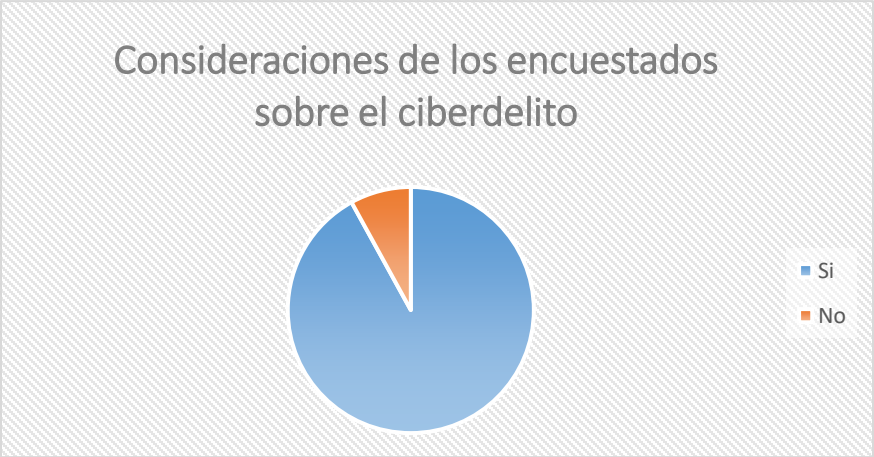


Al analizar el nivel de escolaridad de los encuestados se logró determinar que los 50 participantes se encuentran entre los niveles de Premedia, y universidad y que el 58% cuenta con sus estudios a nivel media, siendo este el porcentaje más alto y colocando al nivel Premedia con un solo participante. Además, se obtiene así, que la mayoría de los participantes son residentes con pertinencias académicas aceptables.

Tabla n°4. Consideraciones de los encuestados sobre el ciberdelito

Opciones	Cantidad	Porcentaje
Si	46	92%
No	4	8%
Total	50	100%

Gráfico n°4. Consideraciones de los encuestados sobre el ciberdelito

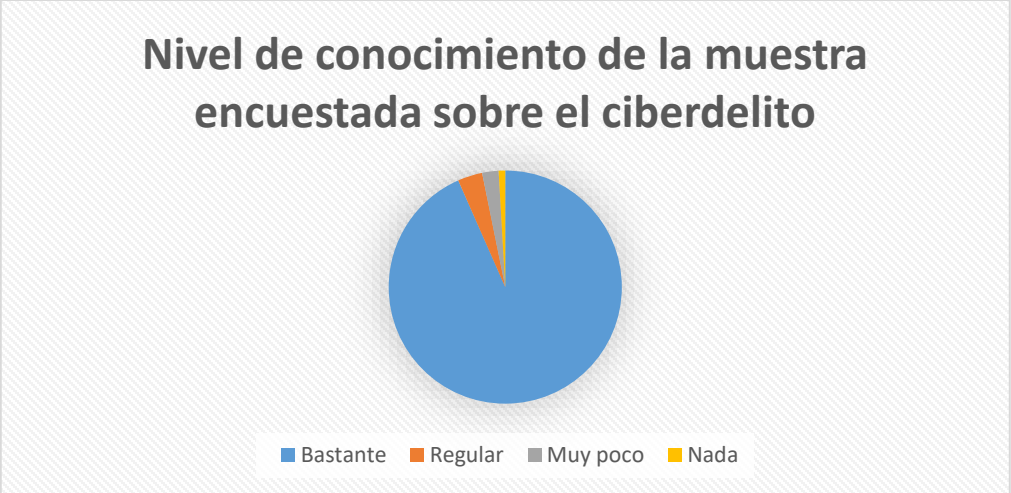


En relación con la interrogante referente al conocimiento o desconocimiento del ciberdelito por los encuestado, se reflejó que el 92% de la muestra seleccionada conoce que es un ciberdelito, mientras que 8% estable el desconocimiento de 4 participantes. Estamos entonces, frente a una población conocedora de la existencia del ciberdelito.

Tabla n°5. Nivel de conocimiento de la muestra encuestada sobre el ciberdelito

Nivel de conocimiento	Cantidad	Porcentaje
Bastante	21	42%
Regular	15	30%
Muy poco	10	20%
Nada	4	8%
Total	50	100%

Gráfica n°5. Nivel de conocimiento de la muestra encuestada sobre el ciberdelito

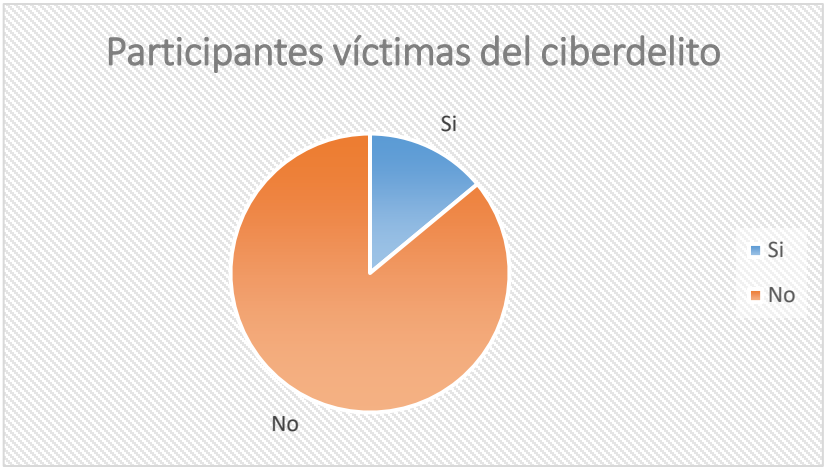


Con relación a la gráfica que antecede sobre el nivel de los conocimientos del ciberdelito, el 42% de los encuestados, respondió que tiene bastantes conocimientos sobre el ciberdelito, lo cual indica que los residentes del corregimiento de San Carlos conocen en gran media sobre el tema.

Tabla n°6. Participantes víctimas del ciberdelito

Opciones	Cantidades	Porcentaje
Si	7	14%
No	43	86%
Total	50	100%

Gráfico n°6. Participantes víctimas del ciberdelito

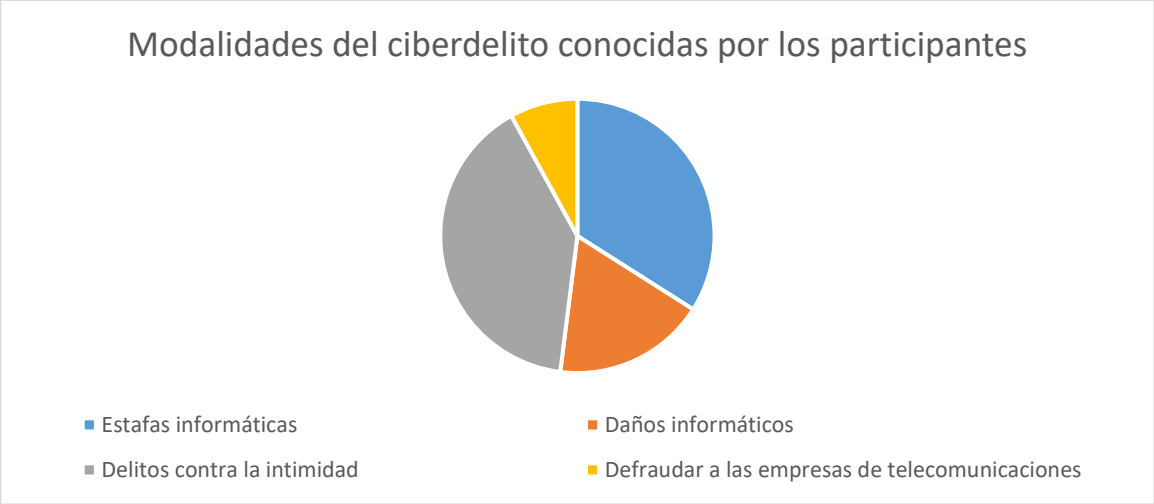


La gráfica anterior en la que se plasman la cantidad de participantes víctimas del ciberdelito arrojó un 86% para la opción “no”.

Tabla n°7. Modalidades del ciberdelito conocidas por los participantes

Modalidades del ciberdelito	Cantidad	Porcentaje
Estafas informáticas	17	34%
Daños informáticos	9	18%
Delitos contra la intimidad	20	40%
Defraudar a las empresas de telecomunicaciones	4	8%
Total	50	100%

Gráfico n°7. Modalidades del ciberdelito conocidas por los participantes

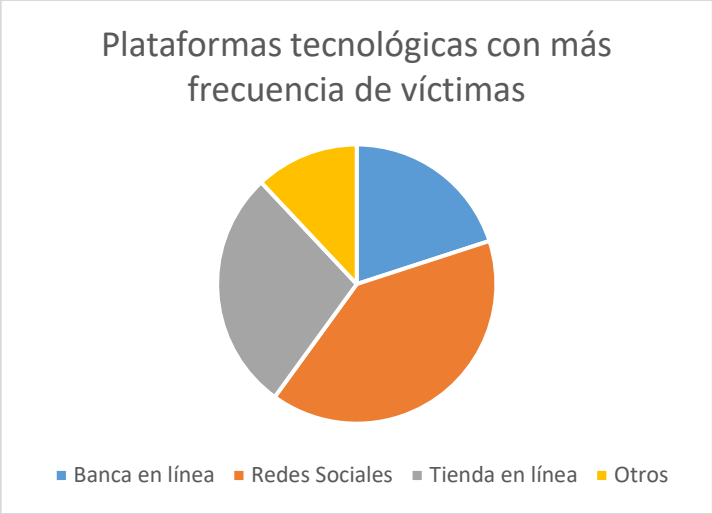


La gráfica anterior demuestra un 40% como porcentaje mayor en el que los participantes respondieron que la modalidad del ciberdelito que más conocen es sobre los Delitos contra la intimidad (robo de datos o imágenes para su filtración); seguida de las Estafas informáticas (suplantación de identidad para robar datos personales, como el phishing o el carding) con un 34%.

Tabla n°8. Plataformas tecnológicas con más frecuencia de víctimas

Plataformas tecnológicas	Cantidad	Porcentaje
Banca en línea	10	20%
Redes Sociales	20	40%
Tiendas en línea	14	28%
Otros	6	12%
Total	50	100%

Gráfica n°8. Plataformas tecnológicas con más frecuencias de víctimas

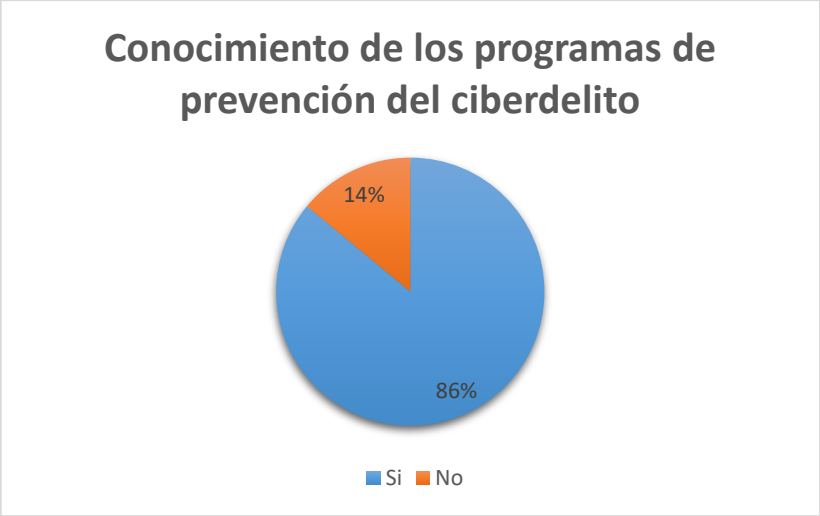


Mediante esta gráfica se refleja las consideraciones de los encuestados sobre cuál es la plataforma tecnológica por la que es más frecuente ser víctima, resultando con un 40% las Redes Sociales (Facebook, Correo, Instagram, WhatsApp), rango bastante alto. Cabe señalar que coloca en segunda posición a las tiendas en línea con un 28%.

Tabla n°9. Conocimiento de los programas de prevención del ciberdelito

Opciones	Cantidad	Porcentaje
Si	43	86%
No	7	14%
Total	50	100%

Gráfico n°9. Conocimiento de los programas de prevención del ciberdelito

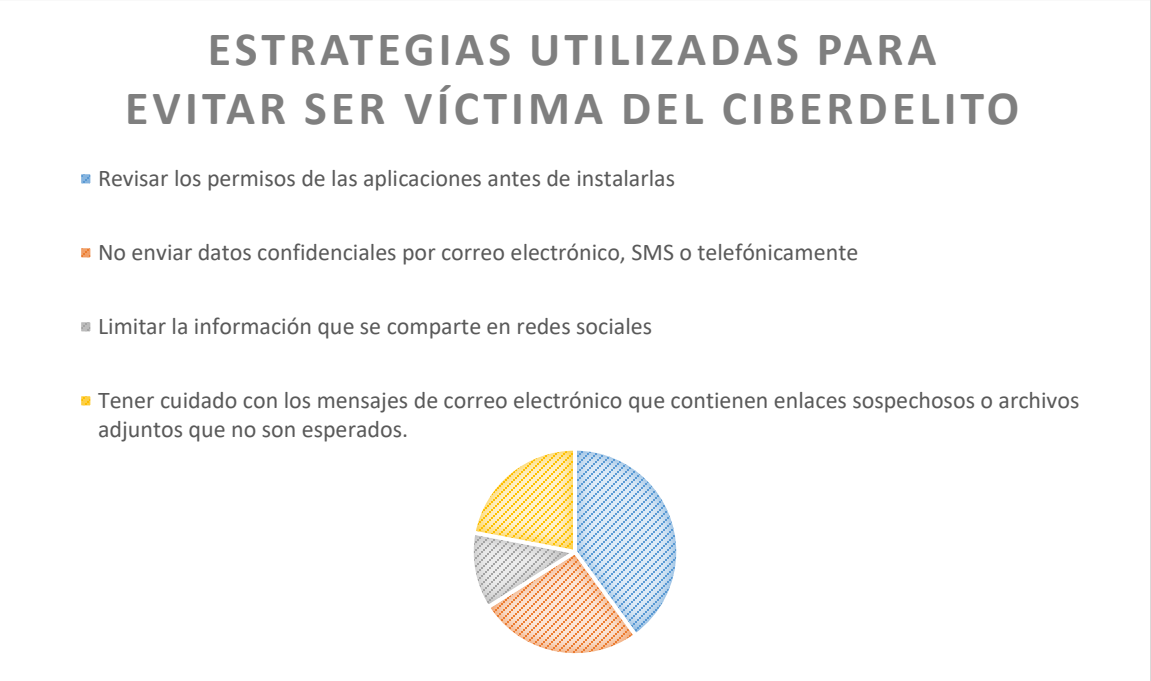


Con relación a los resultados arrojados por la gráfica anterior, el 86% de los participantes respondieron que sí conocen algún programa de prevención del Ciberdelito llevado a cabo en el corregimiento de San Carlos.

Tabla n°10. Estrategias utilizadas para evitar ser víctima del ciberdelito

Estrategias	Cantidad	Porcentaje
Revisar los permisos de las aplicaciones antes de instalarlas.	20	40%
No enviar datos confidenciales por correo electrónico, SMS o telefónicamente.	13	26%
Limitar la información que se comparte en redes sociales.	6	12%
Tener cuidado con los mensajes de correo electrónico que contienen enlaces sospechosos o archivos adjuntos que no son esperados.	11	22%
Total	50	100%

Gráfico n°10. Estrategias utilizadas para evitar ser víctima del ciberdelito

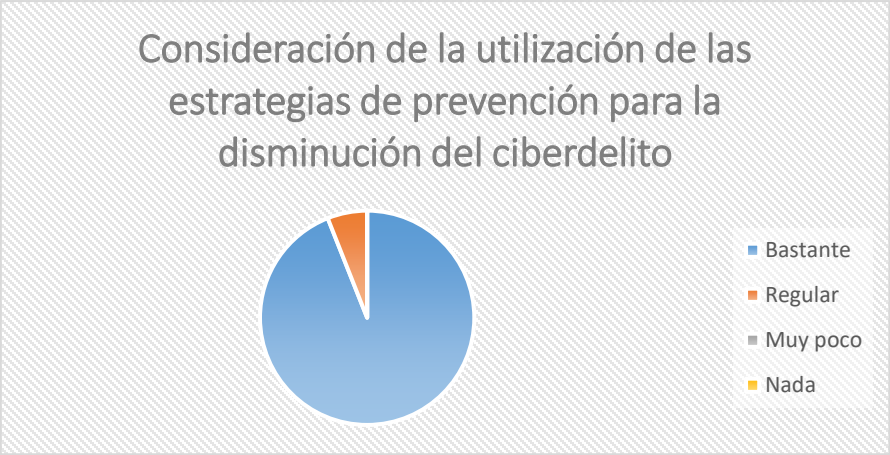


Con referencia al análisis de gráfico anterior, 40% de los participantes respondieron que la estrategia más utilizada para evitar ser víctima del ciberdelito es revisar los permisos de las aplicaciones antes de instalarlas, seguido de no enviar datos confidenciales por correo electrónico, SMS o telefónicamente.

Tabla n°11. Consideración de la utilización de las estrategias de prevención para la disminución del ciberdelito

Opciones	Cantidad	Porcentaje
Bastante	47	94%
Regular	3	6%
Muy poco	0	0%
Nada	0	0%
Total	50	100%

Gráfica n°11. Consideración de la utilización de las estrategias de prevención para la disminución del ciberdelito



Al analizar la medida en la que los participantes consideran que la utilización de las estrategias de prevención puede ayudar a la disminución del ciberdelito, el 94% expresó que realmente estas pueden ser pieza fundamental para contrarrestar el ciberdelito.

Tabla n°12. Consideraciones sobre la importancia de informar a la población sobre las estrategias para la prevención del ciberdelito

Opciones	Cantidad	Porcentaje
Bastante	50	100%
Regular	0	0%
Muy Poco	0	0%
Nada	0	0%
Total	50	100%

Gráfico n°12. Consideraciones sobre la importancia de informar a la población sobre las estrategias para la prevención del ciberdelito

En esta gráfica se aprecia que el 100% de los encuestados, indicó que es bastante necesario informar a la población sobre las estrategias para prevenir el ciberdelito. Lo que resulta ser el reflejo de la preocupación y conciencia de los participantes sobre el tema.

4.2 Resultados de la entrevista realizada a el funcionario de la 19ava Zona Policial

Para establecer una amplia comprensión de los resultados aportados por el especialista en el Análisis estadístico de los hechos delictivos de la zona y sus opiniones en la entrevista, se realizó un cuadro preciso con las interrogantes y los respetivos datos facilitados.

Cuadro n°1. Entrevista realizada al funcionario de la 19ava Zona Policial del corregimiento de San Carlos

Datos generales	Edad:	43 años
	Sexo:	Masculino
	Rango:	Subteniente
	Tiempo de laborar en la institución:	21 años
Preguntas	1. ¿Qué aspectos deben estar presentes para considerar que se está frente a un ciberdelito?	El aspecto más importante indudablemente es que el delito sea realizado mediante la utilización de los medios tecnológicos o el internet, puesto que el delito como tal, tiene su origen en este medio. Normalmente luego se deduce si se está frente a una estafa, extorsión o cualquier modalidad.
	2. ¿A tomado auge el desarrollo del ciberdelito en el corregimiento de San Carlos en los últimos años?	El corregimiento de San Carlos responde a una zona en donde no se registran muy comúnmente los Ciberdelitos; sin embargo, durante el desarrollo de años anteriores se han podido presentar algunas modalidades como las estafas mediante las casas de alquiler del área, los robo de autos de acarreo de mercancía los cuales inician mediante redes como el Facebook o Instagram, en donde postean sus promociones y las personas

		acceden para luego lamentablemente convertirse en una víctima de los Ciberdelitos.
	3. ¿Cuál es la modalidad del ciberdelito que más ha sido denunciada por las personas que han sido víctimas?	Dentro de la zona de San Carlos como corregimiento, no existe una modalidad que lideré; pero si bien es cierto en el año 2021 se presentaron unos casos con la modalidad que ya te mencioné. En un año normalmente se pueden presentar 2 0 3 casos en esta modalidad y dentro de la zona en la que realizas tu investigación, porque en el área de Coronado, Chame si existe un auge considerable por las casas en el área de playa.
	4. ¿Qué estrategias son las más recomendadas para la prevención del ciberdelito en el corregimiento de San Carlos en prevención de este delito? ¿Dichas estrategias pueden aplicarse de forma colectiva?	Con los documentos que nosotros detallamos, logramos hacer un análisis pertinente de la modalidad y la problemática que se desarrolla para que eso pase al Jefe (Comisionado) encargado de la Zona Policial y a su vez esto sea remitido a algún funcionario de alto rango que transmita la información preventiva para ustedes mediante los medios de comunicación, esto como primera estrategia porque de una u otra forma, al realizar ese comunicado se está tomando una buena cantidad de personas para informarlas desde diferentes plataformas. Además, se trata de llegar a la población de San Carlos constantemente con volanteo acerca del tema.
	5. ¿Cuál es su valoración para el desarrollo de la campaña “El Ciberdelito es real” en el corregimiento de San Carlos?	Falta hacer más ruido como se dice, porque si bien es cierto en la 19va Zona Policial el área o sector con más incidencia es el corregimiento de Coronado en

		el distrito de Chame, pero a nivel nacional existen sectores grandes como el distrito de San Miguelito en el que cada día se incrementa más la comisión de los Ciberdelitos Esto se ve reflejado en las denuncias de los primeros meses que es el que normalmente más aparece el ciberdelito.
	6. ¿Qué estrategias puede añadir usted, para la prevención del ciberdelito en el corregimiento de San Carlo?	Tener mucho cuidado al realizar u alquiler de una casa de playa (utilizo este punto como ejemplo porque es lo que más pasa a la altura de zona). Si usted es de la ciudad capital y quiere pasar un fin de semana por el área del corregimiento de San Carlos y ve una casa en las redes sociales muy bonita, cómoda y despampanante; primeramente, debe asegurarse de que ese precio que tiene sea concordante, o sea, las personas deben sacar ese instinto de malicia y lógica. Luego, si es posible antes de hacer algún tipo de transferencia, algún miembro del grupo familiar o de amigos, debe venir a corroborar que en efecto la vivienda se alquila y es la que se muestra en la fotografía. Utilizando estas medidas prevenimos caer en las redes de los delincuentes que están utilizando el internet y las redes para llegar a nosotros tratando de satisfacer alguna necesidad que luego solo deja una pésima experiencia complicada de resolver por el inmenso mundo del ciberdelito.

En análisis de las repuestas brindadas por el Subteniente, se aclara que para estar frente a un ciberdelito es muy importante el origen del delito como tal, debido a que, de acuerdo con los ejemplos de las modalidades denunciadas por las víctimas en el corregimiento de San Carlos según el especialista, son las estafas mediante el alquiler de casas en las playas o los robos de vehículos dedicados al acarreo, en donde claramente se está ante modalidades tradicionales del delito; pero estas iniciaron mediante las diferentes plataformas tecnológicas como las redes sociales (Facebook, Instagram), en donde mediante propagadas de las residencias o el servicio de acarreo, los delincuentes comenten sus fechorías y dan origen al ciberdelito.

Según el especialista, el corregimiento de San Carlos no presenta una aparición considerable de estas modalidades; sin embargo, esos 2 o 3 casos que puedan presentarse son estudiados para posteriormente plantear la problemática y así tomar las medidas pertinentes que puedan contrarrestar el fenómeno.

La prevención mediante las medidas otorgadas por el análisis del Subteniente, reafirma la importancia que tienen las autoridades para la prevención del ciberdelito, si bien es cierto y como lo menciona el funcionario, es necesario explotar más la campaña del “Ciberdelito es Real” a nivel nacional para que los sectores a los que hico mención, también puedan estar más informados y prevenidos.

Las consideraciones del Subteniente refuerzan el pensamiento inicial de esta investigación, debido que, mediante la información de las estrategias de prevención y la aplicación de esta, se logra mantener una disminución considerable del ciberdelito.

CONCLUSIONES

- Dentro del corregimiento de San Carlos el despliegue del ciberdelito es casi inexistente por lo cual su naturaleza responde a una población bastante informada y prevenida sobre el tema. Además, se puede añadir que la presencia de las autoridades y su compromiso con el corregimiento ha servido de apoyo para contrarrestar el desarrollo del delito (ver tablas o gráficas n°4,5,11; y cuadro n°1).

- En cuanto a las estrategias de prevención, estas suponen ser una herramienta fundamental para la disminución del ciberdelito en el corregimiento de San Carlos, a manera que los residentes consideran que la mejor forma de evitar ser víctima de estas modalidades es revisar los permisos de las aplicaciones antes de instalarlas, seguido de no enviar datos confidenciales por correo electrónico, SMS o telefónicamente; lo cual concuerda con las estrategias brindadas por el especialista de la Policía Nacional (ver tabla o gráfica n°10; y cuadro n°1).

- El beneficio otorgado por las estrategias de prevención del ciberdelito es amplio debido a que con ellas se establece un control de alerta ante la utilización de las plataformas tecnológicas; además, se logra crear un estado de conciencia en los residentes del corregimiento de San Carlos quienes también consideran fundamental dotar de los conocimientos necesarios sobre el tema que, en cuestión, se refiere a una modalidad evolutiva y cambiante (ver tabla o gráfico n°12).

- Finalmente, al corroborar la información plasmada en las diferentes plataformas tecnológicas y evitar proporcionar datos personales en las redes sociales; se elude cualquier situación proveniente de los Ciberdelitos; lo cual

comprueba que con la utilización de las estrategias de prevención se logra la disminución en el desarrollo de esta modalidad delictiva.

RECOMENDACIONES

- Si bien es cierto, el corregimiento de San Carlos resultó exento del desarrollo del ciberdelito, debido a la prevención que en esta zona se despliega, se hace necesario ampliar los programas de capacitación sobre el tema para que día a día se instruya a la población de las nuevas modalidades y plataformas utilizadas por los ciberdelincuentes.

- Realizar antes del inicio de cada año, actividades a nivel nacional en donde se refuerce la prevención del ciberdelito. De esta manera se crea conciencia en los residentes capitalinos que son víctimas de las estafas mediante el supuesto alquiler de casas en sectores cercanos a las playas, ríos o lagos del interior.

- Es necesario concienciar a la población más joven (adolescentes), la cual se puede ver expuesta ante las modalidades de extorsión o delitos contra la intimidad, puesto que en este estudio no se tomó en cuenta su participación.

LIMITACIONES

- La investigación no incluyó la muestra en su totalidad debido a el corto tiempo y la falta de disponibilidad de los participantes.

- La carencia de un buen equipo tecnológico que ayudara a la redacción y estructuración del documento con mayor facilidad.

- Manejo de los formatos exigidos para el desarrollo de la investigación.

REFERENCIAS BIBLIOGRÁFICAS E INFOGRAFÍA

Acosta, G.; Benavides, M. & García, N., (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89). Universidad del Zulia, Venezuela. https://www.redalyc.org/articulo.oa?id=29062641023

Aguilar, M., (2015). Cibercrimen y cibervictimización en Europa: Instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Vol. 57 n°1. Revista Criminalidad. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082015000100009

Álvarez, R., (2012). El ciberdelito: la contribución de las estrategias de seguridad por la lucha contra la ciberdelincuencia: armas jurídicas contra el nuevo enemigo. Cuadernos de la Guardia Civil: Revista de seguridad pública, n°46. https://dialnet.unirioja.es/ejemplar/323657

Montoya, W., (2014). INTRODUCCIÓN. Breve Historia de Internet. http://www.unalmend.edu.co/~incominf/W8070 [6-1].htm

Anzit Guerrero, R. (2013). Los delitos informáticos en la era de la revolución científico- tecnológica: Hacking, cracking, phreaking, phishing, scamming. http://www.anzitguerrero.net/admin/pdf/119759803.pdf

Arias, F., (2012). El Proyecto de Investigación. Introducción a la metodología científica. (6ª Edición). Caracas: Editorial Episteme. http://www.formaciondocente.com.mx/06_RinconInvestigacion/01_Documentos/El%20Proyecto%20de%20Investigacion.pdf

ATS, (2014). Ciberdelito conocido como phishing. (2015), Sección 1: El cibersexo como modalidad del ciberdelito.

Barrantes, R., (2014). Investigación, Un camino al conocimiento, Un Enfoque Cualitativo, Cuantitativo y Mixto. San José, Costa Rica, Editorial EUNED. https://www.uned.ac.cr/academica/images/ceced/docs/Investigacion_camino_conocimiento.pdf

Barrio, M., (2017). Ciberdelitos: amenazas criminales del ciberespacio. Madrid: Editorial Reu. p.https://elibro.net/es/ereader/udelas/46673?pague=2

Barrio, M., (2018). Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos. Madrid: Wolters Kluwer España. https://elibro.net/ereader/udelas/56038?page=30

Bartrina, M., (2014). Conductas de ciberacoso en niños y adolescentes. Hay una salida con la educación y la conciencia social. Educar, 50(2), 383-400. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/287060Texto%20del%20art%C3%ADculo-396455-1-10-20150206.pdf

Beermann, K., (2018). La problemática de la interceptación informática en Panamá. http://up-rid.up.ac.pa/1683/1/kurt%20beermann.pdf

Bernal, A., (2017). Ciberespacio, darkweb y ciber policía. Diario La Ley n°2, Sección Ciber derecho. https://noticias.juridicas.com/conocimiento/articulos-doctrinales/11763-ciberespacio-dark-web-y-ciberpolicia/

Bernal, I., (2018). Técnicas Encuesta. http://tecnicaencuesta1.blogspot.com/2018/05/definicion-de-encuesta-se-denomina.html

Campos, P., (2016). Delitos informáticos en México y sus formas de prevención. http://revista.cleu.edu.mx/new/descargas/1604/articulos/Articulo09_Delitos_informaticos_en_Mexico_y_sus_formas_de_prevencion.pdf

CCDCOE, (2013). NATO Coorperative Cyber Defence of Excellence. Tallínn. Manual Process. https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Código Orgánico Integral Penal (COIP). Asamblea Nacional de la República del Ecuador, 2014. (Ecuador, Quito).

Código Penal (CP). Asamblea Legislativa, 2014. (El Salvador, San Salvador).

Código Penal (CP). Ley 146 de julio de 2012. (Puerto Rico, San Juan).

Código Penal (CP). Proyecto de Ley 558 de 2017, que modifica y adiciona artículos al Código Penal, relacionados al Cibercrimen. http://www.asamblea.gob.pa/proyley/2017_P_558.pdf

Concepción, M., (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, XLVII. 209-234. España. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/Dialnet-Cibercrimen-4639646%20(1).pdf

Consejo de Europa. Convenio sobre la Ciberdelincuencia. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa, (2004). Informe sobre la situación del crimen organizado en Europa", Francia, 2005. p.p. 83 a 94. https://www.europol.europa.eu/sites/default/files/documents/es_euorganisedcrimesitrep04-es.pdf

Consejo Nacional para la Innovación Gubernamental. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf

Decreto ejecutivo 101 del 17 de mayo de 2005. Por el cual se prohíbe el acceso a personas menores de edad a sitios web de contenido pornográfico Gaceta Oficial No. 25.311 de 17 de mayo de 2005.

Díaz, A., (2018). El delito informático, su problemática y la cooperación internacional para paradigma de su solución: El Convenio de Budapest. Revista electrónica del Departamento de Derecho de la Universidad de la Rioja, REDUR. https://doi.org/10.18172/redur.4071

El Capital Financiero.com, sección Actualidad, (2021). Impulsan campaña El Ciberdelito es Real para crear conciencia en la ciudadanía. https://elcapitalfinanciero.com/impulsan-campana-el-ciberdelito-es-real-para-crear-conciencia-en-la-ciudadania/

Fratti, S., (2018a). Panamá: Un País con la necesidad de una legislación sobre Cibercrimen. Ipandetec-Instituto Panameño de Derecho y Nuevas

Tecnologías. https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

Fratti, S., (2018b). Panamá: Un País con la necesidad de una legislación sobre Cibercrimen. Ipandetec-Instituto Panameño de Derecho y Nuevas Tecnologías. https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

Flores, F., (2013). Respuesta penal al denominado robo de identidad en las conductas de phishing bancario. Estudios Penales y Criminológicos, 34. www.usc.es/revistas/index.php/epc/article/download/2073/2120

Flores, F., (2014a). Respuesta Penal al denominado Rodo de Identidad en las conductas de Phishing bancario. Estudios Penales y Criminológicos, vol. XXXIV. ISSN 1137-7550: 301-339. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/2073-Texto%20del%20art%C3%ADculo-8397-1-10-20141023.pdf

Flores, F., (2014b). Respuesta Penal al denominado Rodo de Identidad en las conductas de Phishing bancario. Estudios Penales y Criminológicos, vol. XXXIV. ISSN 1137-7550: 301-339. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/2073-Texto%20del%20art%C3%ADculo-8397-1-10-20141023.pdf

Flores, J., (2012a). Tecnologías de Internet-TI: naturaleza y evolución de internet. Pág.3. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html

Flores, J., (2012b). Tecnologías de Internet-TI: naturaleza y evolución de internet. Pág.3. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html

Fuentes, T., Mazún, R. & Cancino, G., (2018). Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. Revista Advance in Engineering and Innovation [AEI], Año 2, No.4, Yucatán, México.

Galindo, J., (2014). La prevención del delito situacional y mediante el diseño ambiental: el caso del Metro de Barcelona.

http://diposit.ub.edu/dspace/bitstream/2445/58430/1/TFG%20S%C3%A1nchezGalindo%28MMartin%29.pdf

Gómez, A., (2010). El delito informático su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR). https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/0

Gonzáles, M., (2015). España es el tercer país, tras EE. UU. y Reino Unido, el país que sufre más ciberataques". El País, 5 de febrero. https://elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html

Hernández, L., (2010). Aproximación a un concepto de Derecho Penal informático, en DE LA CUESTA ARZAMENDI, José Luis (Dir.), Derecho Penal informático. Editorial Aranzadi, Navarra. https://dialnet.unirioja.es/servlet/articulo?codigo=4848005

Hernández, R., Fernández, C. & Baptista, P., (2010). Metodología de la investigación (6ª Edición). México D.F: McGraw-Hill / Interamericana Editores, S.A. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Hernández-Sampieri, R. & Mendoza, C., (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta, Ciudad de México, México: Editorial Mc Graw Hill Education, Año de edición: 2018, ISBN: 978-1-4562-6096-5, 714 p. https://www.academia.edu/43982331/METODOLOG%C3%8DA_DE_LA_INVESTIGACI%C3%93N_LAS_RUTAS_CUANTITATIVA_CUALITATIVA_Y_MIXTA

IPANDETEC. Cronología de un Proyecto de Ley de Protección de Datos de Carácter Personal en Panamá. http://www.ipandetec.org/blog/cronologia-de-un-proyecto-de-ley-de-proteccion-de-datos-de-caracter-personal-en-panama.html

Instituto Nacional de Estadística y Censo, (2021). Estimación y proyección de la población del distrito de San Carlos, por corregimiento, según sexo y edad. Año 2020. https://www.inec.gob.pa/publicaciones/Default3.aspx?ID_PUBLICACION=556&ID_CATEGORIA=3&ID_SUBCATEGORIA=10

INTERPOL, Noticias y acontecimientos, (2021a). INTERPOL lanza una nueva campaña de concienciación sobre la ciberdelincuencia. https://www.interpol.int/es/Noticias-yacontecimientos/Noticias/2021/Mantener-a-raya-a-losciberdelincuentes-SoloUnClic-puede-marcar-la-diferencia

INTERPOL, Noticias y acontecimientos, (2021b). INTERPOL lanza una nueva campaña de concienciación sobre la ciberdelincuencia. https://www.interpol.int/es/Noticias-yacontecimientos/Noticias/2021/Mantener-a-raya-a-losciberdelincuentes-SoloUnClic-puede-marcar-la-diferencia

Jewkes, Y. & Yard M., (2013). Manual de delitos de internet. Ed.Willian Publishing, Portland USA. file:///C:/Users/PC/Downloads/RoutledgeHandbooks-9781843929338-chapter3.pdf

Kamariah, M., Ismail, N., Abd, A. & Md, M., (2015). Cyber Stalking: Social Issuesof Harassment on Internet. American-Eurasian J. Agric. & Environ. Sci., 15(Tourism & Environment, Social and Management Sciences). http://idosi.org/aejaes/jaes15(tesms)15/2.pdf

Lara, J, Martínez, M. & Viollier, P., (2014a). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, Año 3, No. 1. https://rchdt.uchile.cl/index.php/RCHDT/article/view/32222/34151

Lara, J, Martínez, M. & Viollier, P., (2014b). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, Año 3, No. 1. https://rchdt.uchile.cl/index.php/RCHDT/article/view/32222/34151

Lanuez, M. y Fernández, E. (2014). Metodología de la Investigación Educativa. (CDROM). IPLAC, La Habana, Cuba.: http://revistas.ult.edu.cu/index.php/didascalia/article/view/992

Ley 1 del 1982. Se estableció la división político – administrativa del distrito de San Carlos. 27 de octubre de 1982. Gaceta Oficial No. 20006

Ley 14 de 2007. Por el que se adiciona artículos al Código Penal relacionados al Cibercrimen. 18 de mayo de 2007. Gaceta Oficial No. 25796

Ley 15 de 1994. Derechos de Autor y Derechos Conexos. Capítulo II, Programas de Ordenador. 8 de agosto de 1994. Gaceta Oficial No. 22598

Ley 43 2001. La cual regula lo concerniente a las Firmas y comercio electrónicos. 31 de julio de 2001. Gaceta Oficial No. 24359

Ley 81 de 2019. Sobre Protección de Datos Personales. 26 de marzo de 2019. Gaceta Oficial No. 28743-A

López V., Óscar D., & Restrepo G., W. D., (2013). Análisis y desarrollo de estrategias para la prevención del uso de la Ingeniería Social en la sociedad de la información. Ingenierías USB Med, 4(2), 16–22. Disponible en: https://doi.org/10.21500/20275846.287

Loredo, J. & Ramírez, A., (2013a). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Loredo, J. & Ramírez, A., (2013b). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Loredo, J. & Ramírez, A., (2013c). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Luna, V. (2018). Espionaje informático, robo de identidad e información. Quanti Solutions, 2(1), 6-14. https://www.quanti.com.mx/2018/03/05/espionajeinformatico-robo-identidad-e-informacion/

Martes Financiero La revista Financiera de Panamá, sección Actualidad Empresarial, (2021). Recomendaciones para no ser presa de la ciberdelincuencia. https://www.martesfinanciero.com/actualidad-empresarial/recomendaciones-para-no-ser-presa-de-la-ciberdelincuencia/

Martínez, C., (2018). Investigación descriptiva: definición, tipos y características. https://www.lifeder.com/investigacion-descriptiva

Martínez, L.; Leyva, M. & Félix, L., (2014). Virtualidad, ciberespacio y comunidades virtuales. Ed. Red Durango de Investigadores Educativos, A. C. Pág 48. http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Márquez, Neila y Mousalli, Gloria (2016a). Internet, usos y riesgos. Revista Teuken BidiKay, Año 9, No. 12, Medellín, Colombia, pp 177-191. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/Internet_usos_y_riesgos_Una_vision_desde_la_formac.pdf

Márquez, Neila y Mousalli, Gloria (2016b). Internet, usos y riesgos. Revista Teuken BidiKay, Año 9, No. 12, Medellín, Colombia, pp 177-191. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/Internet_usos_y_riesgos_Una_vision_desde_la_formac.pdf

Ministerio de Relaciones Exteriores, sección de noticias por año, (2014a). Panamá expone a nivel mundial experiencia en prevención de del Cibercrimen. https://mire.gob.pa/panama-expone-a-nivel-mundial-experiencia-en-prevencion-del-cibercrimen/

Ministerio de Relaciones Exteriores, sección de noticias por año, (2014b). Panamá expone a nivel mundial experiencia en prevención de del Cibercrimen. https://mire.gob.pa/panama-expone-a-nivel-mundial-experiencia-en-prevencion-del-cibercrimen/

Ministerio Público, Noticias emitidas por el Departamento de Información y Relaciones Públicas (2021a). ““El Ciberdelito es Real” Ministerio Público y Policía Nacional lanzan campaña de prevención del delito”. https://ministeriopublico.gob.pa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/

Ministerio Público, Noticias emitidas por el Departamento de Información y Relaciones Públicas (2021b). ““El Ciberdelito es Real” Ministerio Público y Policía Nacional lanzan campaña de prevención del delito”. https://ministeriopublico.gob.pa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/

Mollo Mamani, J. L. (junio, 2013). Keylogger. Información, Tecnología y Sociedad, (8). http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100019&script=sci_arttext

Morales, C., (2017a). Delitos informáticos en el Estado de Guerrero. Universidad Autónoma de Guerrero. México. https://es.slideshare.net/PERLA2015/libro-delitos-informaticos-72068879

Morales, C., (2017b). Delitos informáticos en el Estado de Guerrero. Universidad Autónoma de Guerrero. México. https://es.slideshare.net/PERLA2015/libro-delitos-informaticos-72068879

Murashbekov, B., (2015). Methods for Cybrecrime Fighting Improvement in Developed Countries. The Journal of Internet Banking and Commerce, 20(S1), 24-29. https://www.icommercecentral.com/open-access/methods-for-cybercrime-fighting-improvement-in-developed-countries.pdf

Naciones Unidas, (2011). Manual sobre la aplicación eficaz de las Directrices para la prevención del delito. https://www.unodc.org/documents/justice-and-prisonreform/crimeprevention/Handbook_on_the_Crime_Prevention_Guidelines_Spanish.pdf

Núñez, O., (2017). Presentan proyecto de ley que busca penalizar delitos cibernéticos en Panamá. Telemetro.com/Nacionales. http://www.telemetro.com/nacionales/Presentan-Codigo-Penal-relacionados- Cibercrimen_0_1066994305.html

Oficina de las Naciones Unidas contra la Droga y el Crimen (UNODOC), (2013). Estudio exhaustivo sobre el delito cibernético. Nueva York. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014). Recomendación del Consejo de la OCDE relativa a la Cooperación Internacional en el marco de investigaciones y procedimientos en materia de competencia. Aprobada por el Consejo el 16 de septiembre de 2014, México. https://www.oecd.org/daf/competition/Recommendation_Intel%20Cooperation_ES.pdf

Ortega, M., (2013). Ilícitos militares cometidos a través de internet o con ocasión del uso de nuevas tecnologías. Delimitación y problemas procesales y de puerta que plantea. Ponencia presentada en las Jornadas de la Fiscalía Jurídico Militar. Pág. 10. https://www.fiscal.es/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Marcelo%20Ortega%20Gutierrez-Maturana.pdf?idFile=1bf8666f-ba3e-9129-4dec942c381c.

Oxman, Nicolás (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del phishing y el pharming, Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, Año 1, No. 41. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007

Palella Stracuzzi, Santa y Martins Pestana, Filiberto (2010). Metodología de la Investigación Cuantitativa. FEDEUPEL. Caracas

Panamá América, Ávila, L., (2022). Unas 100 denuncias por delitos de estafas de presentan al mes en Panamá. https://www.panamaamerica.com.pa/judicial/una-100-denuncias-por-delitos-de-estafas-se-presentam-al-mes-en-panama-1201054

Pascual, I. (2013). "Ciberdelincuencia Desarrollo y persecución tecnológica". https://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

Paul, S., K. Smith, P., & H. Blumberg, H. (julio, 2012a). Investigating Legal Aspects Of Cyberbullying. Psicothema, 24(4). http://www.redalyc.org/articulo.oa?id=72723959021

Paul, S., K. Smith, P., & H. Blumberg, H. (julio, 2012b). Investigating Legal Aspects Of Cyberbullying. Psicothema, 24(4). http://www.redalyc.org/articulo.oa?id=72723959021

Paz, N. (2015). Contabilidad General. Quinta Edición. McGraw-Hill Interamericana. 2015. http://bibmcgrath.usma.ac.pa/library/index.php?title=227464&lang=%20%20%20%20%20%20&query=@title=Special:GSMSearchPage@process=@autor=DIAZ,%20OSCAR%20@mode=&recnum=5&mode=

Pérez Bes, C., (2016). El Derecho de Internet. Ed. Atelier, Barcelona. https://www.marcialpons.es/libros/el-derecho-de-internet/9788416652075

Question Pro, (2020). Muestreo no probabilístico: definición, tipos y ejemplos. https://www.questionpro.com/blog/es/muestreo-no-probabilistico/#:~:text=El%20muestreo%20no%20probabil%C3%ADstico%20se%20utiliza%20donde%20no,gran%20medida%20de%20la%20experiencia%20de%20los%20investigadores

Quevedo, J., (2017a). Investigación y prueba del ciberdelito. file:///C:/Users/PC/Documents/JQG_TESIS.pdf

Quevedo, J., (2017b). Investigación y prueba del ciberdelito. file:///C:/Users/PC/Documents/JQG_TESIS.pdf

Ramírez, L., (2013). CAPITULO IV. Diagnóstico Situacional, Triangulación y Sistematización. Análisis de Resultados. http://maidalobo.blogspot.com/2013/04/lisette-ramirez-capitulo-iv-dianostico.html?m=1

Rayón, (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Universidad Complutense de Madrid. file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/Dialnet-Cibercrimen-4639646%20(2).pdf

Rayon M. y Gómez J., (2014). Cibercrimen particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677.: file:///C:/Users/Francis%20De%20La%20Cruz/Downloads/Dialnet-Cibercrimen-4639646.pdf

Riestra, E., (2016). Derecho a la intimidad y a la informática. Revista Lus et Praxis, Año 11, No. 26. https://doi.org/10.26439/iusetpraxis1996.n026.3551

Rinaldi, P., (2017). Le VPN. Recuperado en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Rojas-Parra, J., (2016). Análisis de la penalización del cibercrimen en países de habla hispana. Vol. 8. (No. 1), Revista LOGOS CIENCIA & TECNOLOGÍA. [221,222]. ISSN 2145– 549X | ISSN 2422-4200. https://www.redalyc.org/pdf/5177/517754055021.pdf

Ruíz Díaz, J., (2016). Ciber amenazas: ¿el terrorismo del futuro? http://www.ieee.es/Galerias/fichero/doc_opinion/2016/DIEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Sabino, C., (2014). El proceso de investigación. Editorial Episteme, décima edición. Guatemala. https://metodoinvestigacion.files.wordpress.com/2008/02/el-proceso-de-investigacion_carlos-sabino.pdf

Saín, G., (2015a). Cibercrimen: el delito en la sociedad de la información. En Eissa, Sergio (Coord.): Políticas públicas y seguridad ciudadana - Ed. Eudeba - Bs. As. https://es.scribd.com/document/543774629/1-1-Cibercrimen-Sain-Cibercrimen-el-delito-en-la-sociedad-de-la-informacion

Sain, G., (2015b). Cibercrimen: el delito en la sociedad de la información. En Eissa, Sergio (Coord.): Políticas públicas y seguridad ciudadana - Ed. Eudeba - Bs. As. https://es.scribd.com/document/543774629/1-1-Cibercrimen-Sain-Cibercrimen-el-delito-en-la-sociedad-de-la-informacion

Schulman, D., (2012). Psicología Forense y Prevención del Delito. Derecho y Cambio Social, Depósito legal: 2005-5822. https://www.derechoycambiosocial.com/revista026/psicologia_forense.pdf#:~:text=Seg%C3%BAn%20Sozzo%20una%20estrategia%20de%20prevenci%C3%B3n%20del%20delito,de%20problemas%20m%C3%A1s%20o%20menos%20conexos%20con%20aqu%C3%A9l%E2%80%9D

Tamayo, M., (2012). El Proceso de la Investigación Científica. México: Limusa. https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_cient_fica_Mario_Tamayo.pdf

Tatarinova, F., Shakirov, N. & Tatarinov, D., (2016). Criminological Analysis of Determinants of Cybercrime Technologies. International Electronic Journal of Mathematics Education, 11(5). https://www.iejme.com/download/criminological-analysis-of-determinants-of-cybercrime-technologies.pdf

Tejada De La Fuente, E., (2012). Problemas generales de la investigación de la criminalidad informática. Ponencia presentada en el curso menores e internet. http://www.cej.mjusticia.es p.p. 9 a 13.

Temperini, M., (2013a). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://sedici.unlp.edu.ar/bitstream/handle/10915/42145/Documento_completo.pdf?sequence=1&isAllowed=y

Temperini, M., (2013b). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://sedici.unlp.edu.ar/bitstream/handle/10915/42145/Documento_completo.pdf?sequence=1&isAllowed=y

Torres, D., (2015). La información y la comunicación del riesgo de origen tecnológico en la empresa Puerto Moa. Revista Ciencia y Futuro, Año 5, No. 1. http://revista.ismm.edu.cu/index.php/revista_estudiantil/article/view/1031/537

Trochez, I., (2019a). Revisión de la clasificación, categorías, métodos y efectos de la ciberdelincuencia en Colombia en la última década. Tecnología en Sistemas. https://repository.usc.edu.co/bitstream/handle/20.500.12421/4251/REVISI%C3%93N%20DE%20LA%20CLASIFICACI%C3%93N.pdf?sequence=3&isAllowed=y

Trochez, I., (2019b). Revisión de la clasificación, categorías, métodos y efectos de la ciberdelincuencia en Colombia en la última década. Tecnología en Sistemas. https://repository.usc.edu.co/bitstream/handle/20.500.12421/4251/REVISI%C3%93N%20DE%20LA%20CLASIFICACI%C3%93N.pdf?sequence=3&isAllowed=y

Tundidor, L., Nogueira & Medina, A., (2018). Organización de los sistemas informáticos para potenciar en control de la gestión empresarial. Revista Cofín Habana, Año 13, No. 1, Universidad de Matanzas, Cuba. http://scielo.sld.cu/pdf/cofin/v12n1/cofin07118.pdf

TVN Noticias, (2021). Aumentan las denuncias en Panamá por el “Ciberdelito”. https://www.tvn-2.com/nacionales/Aumentan-denuncias-Panama-Ciberdelito_0_5866663342.html

Unicef, (2016). Lanzamiento de la Campaña Nacional para la Prevención del Ciberdelito, “No confíes en Emojis””. https://www.unicef.org/elsalvador/comunicados-prensa/lanzamiento-de-la-campa%C3%B1a-nacional-para-la-prevenci%C3%B3n-del-ciberdelito-no-conf%C3%ADes

Valdés, J., (2013). Ciberespacio y cibersociedad, su relación con las formas de socialización para la apropiación social de las TIC´s. Revista Iberoamericana para la Investigación y el Desarrollo Educativo. http://111.ride.org.mx/index.php/RIDESECUNDARIO/article/viewFile/564/553

Van Eekelen, M. & Vrankend, H., (2012a). They Internet: Historical and Technical Background, en "Cyber Safety: An Introduccion" (Leukfeldt & Stol, coord.). Ed. Eleven International Publishing. La Haya, Holanda.

Van Eekelen, M. & Vrankend, H., (2012b). They Internet: Historical and Technical Background, en "Cyber Safety: An Introduccion" (Leukfeldt & Stol, coord.). Ed. Eleven International Publishing. La Haya, Holanda

Wachs, Wolf & Pan (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. https://www.researchgate.net/publication/232319836_Cybergrooming_Risk_factors_coping_strategies_and_associations_with_cyberbullying

Zuluaga, C., (2015). Códigos estéticos en el pensamiento de Nicolás Gómez Dávila. Discusiones Filosóficas, 16(26), 129-150.doi:10.17151/diil.2015.16.16.9. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-61272015000100009

ANEXOS

ANEXO N°1

CUESTIONARIO DE ENCUESTA

Universidad Especializada de las Américas

Extensión Coclé

Facultad de Educación y Desarrollo Humano

Licenciatura en Investigación Criminal y Seguridad

Encuesta dirigida a los residentes del corregimiento de San Carlos, distrito de San Carlos, provincia de Panamá Oeste.

La investigación realizada, responde a un trabajo de grado que desarrolla el tema de las Estrategias de prevención enfocadas a la disminución del Ciberdelito en el corregimiento de San Carlos.

Objetivo general: Analizar las estrategias de prevención del ciberdelito en el corregimiento de San Carlos.

Nota: Todos los datos recolectados serán utilizados exclusivamente para datos académicos, así como el anonimato de los participantes.

Indicaciones: Marque con una **x** la respuesta con la que usted se considere identificado de acuerdo con su experiencia.

Datos Generales:

Sexo	F	M

Edad	20-24	25-29	30-34	35-39	40-44

Nivel de escolaridad	Primaria	Premedia	Media	Universidad

Preguntas:

1. ¿Sabe usted qué es el ciberdelito?

a) Sí ☐ b) No ☐

2. ¿Qué tanto conoce usted sobre el ciberdelito?

a) Bastante ☐ b) Regular ☐ c) Muy Poco ☐ d) Nada ☐

3. ¿Ha sido usted víctima del ciberdelito?

a) Sí ☐ b) No ☐

4. ¿Qué modalidad de Ciberdelito conoce usted?

a) Estafas informáticas (suplantación de identidad para robar datos personales, como el phising o el carding) ☐

b) Daños informáticos (borrado de bases de datos, interferencias en los sistemas para impedir el normal funcionamiento) ☐

c) Delitos contra la intimidad (robo de datos o imágenes para su filtración) ☐

d) Defraudar a las empresas de telecomunicaciones (al colgarse de la red eléctrica o la conexión a internet de un ☐ o)

5. ¿En qué plataforma tecnológica considera usted, es más frecuente ser víctima del ciberdelito?

a) Banca en Línea ☐

b) Redes Sociales (Facebook, Correo, Instagram, WhatsApp) ☐

c) Tiendas en línea ☐

d) otros ☐

6). ¿Conoce usted algún programa de prevención del Ciberdelito que se lleve a cabo en el corregimiento de San Carlos?

a) Sí ☐ b) No ☐

7). ¿Qué estrategia utiliza usted para evitar ser víctima del ciberdelito?

a) Revisar los permisos de las aplicaciones antes de instalarlas. ☐

b) No enviar datos confidenciales por correo electrónico, SMS o telefónicamente. ☐

c) Limitar la información que se comparte en redes sociales. ☐

d) Tener cuidado con los mensajes de correo electrónico que contienen enlaces sospechosos o archivos adjuntos que no son esperados. ☐

8. ¿En qué medida considera usted, que la utilización de estrategias de prevención podría ayudar a la disminución del Ciberdelito?

a) Bastante ☐ b) Regular ☐ c) Muy Poco ☐ d) Nada ☐

9) ¿En qué medida considera usted que es necesario informar a la población sobre las estrategias para prevenir el Ciberdelito?

a) Bastante ☐ b) Regular ☐ c) Muy Poco ☐ d) Nada ☐

ANEXO N°2

CUESTIONARIO DE ENTREVISTA

Universidad Especializada de las Américas

Extensión Coclé

Facultad de Educación y Desarrollo Humano

Licenciatura en Investigación Criminal y Seguridad

Entrevista dirigida a los miembros de la 19ava Zona Policial de la Subdirección del distrito de San Carlos.

La investigación realizada, responde a un trabajo de grado que desarrolla el tema de las Estrategias de prevención enfocadas a la disminución del Ciberdelito en el corregimiento de San Carlos, que tiene como objetivo analizar las estrategias de prevención del ciberdelito en el corregimiento de San Carlos.

La información que brinde será relevante para la investigación, la misma será tratada con discreción y seriedad.

Datos generales:

Nombre:_____ Edad:_____ Sexo:____.

Rango:_____Tiempo de laborar en la institución:

Preguntas:

1 ¿Qué aspectos deben estar presentes para considerar que se está frente a un ciberdelito?

2 ¿A tomado auge el desarrollo del ciberdelito en el corregimiento de San Carlos en los últimos años?

3 ¿Cuál es la modalidad del ciberdelito que más ha sido denunciada por las personas que han sido víctimas?

4 ¿Qué estrategias son las más recomendadas para la prevención del ciberdelito en el corregimiento de San Carlos En prevención de este delito? ¿Dichas estrategias pueden aplicarse de forma colectiva?

5 ¿Cuál es su valoración para el desarrollo de la campaña "El Ciberdelito es real" en el corregimiento de San Carlos?

6 ¿Qué estrategia puede añadir usted, para la prevención del ciberdelito en el corregimiento de San Carlos?

ANEXOS N°3

NOTA DE PERMISO PARA LA APLICACIÓN DE ENTREVISTA

UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS
Extensión Universitaria de Coclé
El Jagüito, vía Interamericana. Antón.
"Caminando hacia la Excelencia"
Teléfono: 906-0206 Correo electrónico: extension.cocle@udelas.ac.pa

Antón, 26 de noviembre de 2021
EUC-742-2021

Comisionado
Juan Adames
Jefe de la 19ava Zona Policial
E. S. D.

Respetado Comisionado Adames:

Reciba un cordial y atento saludo de parte de la familia udelista, y el deseo de éxitos en sus funciones diarias.

Con la presente deseamos hacer de su conocimiento que la joven **Jacqueline Poveda**, con cédula de identidad personal **2-745-78**, estudiante graduanda de **la Licenciatura en Investigación Criminal y Seguridad**, ha mostrado interés en desarrollar un trabajo de grado titulado: **Estrategias de prevención enfocadas a la disminución del Ciberdelito en el corregimiento de San Carlos,** por lo cual solicitamos el permiso para que pueda recolectar la información pertinente para el desarrollo de su investigación, dentro de la institución que usted dirige.

En tal sentido, la estudiante en mención se compromete a cumplir los requisitos que establezca su institución, los lineamientos académicos y éticos que establece nuestra universidad, así como las normas de seguridad sanitaria que se requiere en estos momentos, bajo el seguimiento y asesoría de la profesora Mitzila Acosta Herrera, docente de trabajo de grado.

Agradecemos todo el apoyo y colaboración que su institución pueda ofrecer a la estudiante en esta última etapa de su formación universitaria.

Cordialmente,

POLICÍA NACIONAL
19va. ZONA DE POLICÍA DE CHAME

Doctorando Daivis Guerra Monterrey
Director Extensión Universitaria de Coclé
daivis.guerra@udelas.ac.pa
Cel. 6923-8458

OFICIO No.
HORA: 09:37 a.m.
RECIBIDO POR:
240-9126

ANEXO N°4

REVISIÓN DE ESPAÑOL

UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS

Evaluación para Trabajo de grado

Facultad de Educación Social y Desarrollo Humano

Panamá, 18 de febrero de 2022.

Señores

COMISIÓN DE TRABAJO DE GRADO

Presente:

El suscrito certifica que él o la estudiante:

Poveda De La Cruz, Jacqueline Johana cédula: 2-745-78

_____, cédula: _____, se le ha revisado el trabajo de grado titulado: Estrategias de prevención enfocadas a la disminución del Ciberdelito en el corregimiento de San Carlos

Doy fe que el trabajo cumple con todas las exigencias de redacción y ortografía del idioma español.

Atentamente,

Rolando A. Camargo V. _____

Profesor(a) de Español

Cédula: 9-118-2266

Registro del Diploma No. 507000

Adjunto: Copia del Diploma.

UNIVERSIDAD DE PANAMA

LA FACULTAD DE

Humanidades

EN VIRTUD DE LA POTESTAD QUE LE CONFIEREN LA LEY Y EL ESTATUTO UNIVERSITARIO,
HACE CONSTAR QUE

Rolando A. Camargo V.

HA TERMINADO LOS ESTUDIOS Y CUMPLIDO CON LOS REQUISITOS
QUE LE HACEN ACREEDOR AL TITULO DE

Licenciado en Humanidades con Especialización en Español

Y EN CONSECUENCIA, SE LE CONCEDE TAL GRADO CON TODOS LOS DERECHOS, HONORES Y PRIVILEGIOS RESPECTIVOS, EN TESTIMONIO DE LO CUAL SE LE EXPIDE ESTE DIPLOMA EN LA CIUDAD DE PANAMA A LOS veintiocho DIAS DEL MES DE Agosto DE MIL NOVECIENTOS noventa y ocho

Secretario General

Diploma 62058

Identificación Personal 9-118-2266

Decano

Rector

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

ÍNDICE DE CUADROS